



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Data Protection Policy

Author/Person Responsible	<i>Headteacher and School Business Manager (adopting model policies provided by Judicium)</i>
Date of Ratification	<i>13th of July 2026</i>
Review Group	<i>FGB</i>
Ratification Group	<i>FGB</i>
Review Frequency	<i>Every 2 years</i>
Review Date	<i>By July 2028</i>
Previous Review Amendments/Notes	<i>See below</i>
Chair of Governor's Signature	<i>Oliver Coltman</i>

Version History Log

Version	Description of Change	Date of Release	Policy by
1 - 10	Earlier updates covering initial policy creation, incorporation of the SAR appendix, alignment with UK GDPR, updates to DPO details, formatting improvements, and corrections to wording and grammar. These versions reflect development of the policy from 2018 to 2025 and full details are retained by Judicium in master log.	2018 - 2025	
11	Amendment to Judicium's address	22.04.2025	
12	Added ICO registration number, grammar amendments, and updated process for escalation of concerns.	01.09.2025	
13	Amended confidential references exemption to include references received.	13.09.2025	
14	Updates to "Automated Decision Making", addition of "recognised legitimate interests" lawful basis, and updated complaints procedure in line with amendments under Data (Use and Access) Act 2025. "Fair Processing Conditions" renamed to "Lawful Bases". International transfers section simplified. Data rights wording aligned more closely with UK GDPR.	06.03.2026	



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Policy	Page Number
<u>Data Protection Policy</u>	3
<u>Data Breach Policy</u>	26
<u>Data Retention Policy</u>	33
<u>Bring Your Own Device Policy</u>	42
<u>Cyber Security Policy</u>	44
<u>Freedom of Information Policy and Publication Scheme</u>	47
<u>Home Working Policy</u>	57
<u>Information and Communications Policy</u>	61
<u>Information Security Policy</u>	70
<u>Social Media Policy</u>	76



Data Protection Policy

Introduction

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, governors, volunteers and any other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Staff is defined by employees, governors, trustees and volunteers. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up and including dismissal depending on the seriousness of the breach.

The School is registered with the Information Commissioners Office (ICO) as required, registration reference Z6709487.

Section 1 – Definitions

Personal Data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.
Special Category Data and Data Relating to Criminal Convictions and Offences	Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data. Personal data relating to criminal offences and convictions is included here for the purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.
Data Subject	An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.
Data Controller	The organisation storing and controlling such information (i.e., the School) is referred to as the Data Controller.
Processing	Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using,



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

	disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.
Automated Processing	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Examples of automated processing includes profiling and automated decision making. Automatic decision-making is when a decision is made which is based solely on automated processing (without meaningful human intervention).
Data Protection Impact Assessment (DPIA)	DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Pseudonymised	The process by which personal data is processed in such a way that that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual.

Section 2 – When can the School Process Personal Data?

Data Protection Principles

The School are responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the School must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The School only collect, process and share personal data fairly and lawfully and for specified purposes.

The School must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

Personal Data

The School may only process a data subject's personal data if one of the following lawful bases are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.
- The processing is necessary for a recognised legitimate interest under the UK GDPR (as amended by the Data (Use and Access) Act 2025).

Special Category Data

The School may only process special category data if they are entitled to process personal data (using one of the lawful bases above) **AND** one of the following conditions are met: -



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's (or another person's) vital interests, where the data subject is unable to give consent;
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing is necessary for archiving, statistical or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

Criminal Record Data

Where criminal records data is processed, a lawful condition for processing that data is also identified and documented.

Consent

Where the School relies on consent as a lawful basis for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent is needed in cases of processing special category data and requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their non-special category personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

In cases of processing special category data and explicit consent, the School will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any manner that is incompatible with the legitimate purposes specified.

The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The School will only process personal data when our obligations and duties require us to. We will not collect excessive data and will ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data.

Principle 4: Personal data must be accurate and, where necessary, kept up to date

The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School's Retention Policy for further details about how the School retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to ensure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

- Encryption;
- Pseudonymisation (as outlined above);
- Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Full details on the School's security measures are set out in the School's Information Security Policy.

Sharing Personal Data

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the School shall be clearly defined within written notifications including details and the basis for sharing the data. Further information can be found in the privacy notice.

Transfer of Data Outside the UK

The UK GDPR restricts the transfer of personal data to countries or international organisations outside of the UK to ensure that individuals' data continues to receive an adequate level of protection.

The School will not transfer personal data outside of the UK unless:

- the destination country is covered by a UK adequacy regulation;
- appropriate safeguards are in place, such as a UK International Data Transfer Agreement (IDTA) or an approved set of standard contractual clauses, and enforceable data subject rights and effective legal remedies are available;
- a specific derogation applies under Article 49 UK GDPR (for example, the transfer is necessary for an important reason of public interest).

All staff must comply with the School's guidelines on transferring personal data outside of the UK. For clarity, a "transfer" may occur whenever personal data are sent, accessed, viewed, or otherwise made available from outside the UK.

The School monitors any international transfers with support from the Data Protection Officer (DPO) and maintain records of our transfer assessments alongside a Third-Party Data Sharing Register.

Section 3 – Data Subject's Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the School handle their personal data are set out below:

- To withdraw consent to processing at any time (where consent is relied upon as a condition of processing);
- Receive certain information about the School's processing activities;
- Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1);
- Prevent our use of their personal data for direct marketing purposes;
- Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- Restrict processing in specific circumstances, such as where the accuracy of the data is contested or an objection is being considered
- Challenge processing which has been justified on the basis of legitimate interests or in the public interest;
- Request a copy of an agreement under which personal data is transferred outside of the UK;
- To be informed where decision that has legal or similarly significant effects is made solely by automated means, and to request human intervention, express their point of view, or contest a decision;



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- To raise a concern or make a complaint directly to the School if they believe their personal data has been processed unlawfully or unfairly, or if they are dissatisfied with the School's response to a data protection request. Individuals also have the right to make a complaint to the supervisory authority, which is the Information Commissioner in England and Wales (<https://ico.org.uk/global/contact-us/>); and
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

Direct Marketing

The School are subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must:

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example, by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction. Please refer to the School's Information Security Policy for further details about our security processes);
- Not remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not store personal information on local drives.

Section 4 - Accountability

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The School have taken the following steps to ensure and document UK GDPR compliance:-

Data Protection Officer (DPO)

Please find below details of the School's Data Protection Officer: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (option 1, then option 1 again)

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines. Should staff have any questions about the UK GDPR, the operation of this policy or, if you have any concerns that this policy is not being, or has not been, followed, please contact the School Business Manager in the first instance. Should the matter remain unresolved or require further escalation, please contact the school's DPO.

In particular, you can contact the DPO in the following circumstances:



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- If you are unsure of the lawful basis being relied on by the School to process personal data;
- If you need to rely on consent as a lawful basis for processing (please see below the section on consent for further detail);
- If you need to draft privacy notices or policies;
- If you are unsure about the retention periods for the personal data being processed [and would refer you to the School's Data Retention Policy in the first instance];
- If you are unsure about what security measures need to be put in place to protect personal data;
- If there has been a personal data breach [and would refer you to the procedure set out in the School's Data Breach Policy];
- If you are unsure on what basis to transfer personal data outside the UK;
- If you need any assistance dealing with any rights invoked by a data subject;
- Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
- If you plan to undertake any activities involving automated processing or automated decision making;
- If you need help complying with applicable law when carrying out direct marketing activities;
- If you need help with any contracts, data processing agreements or other areas in relation to sharing personal data with third parties.

Data Subject Complaints

Individuals have the right to make a complaint directly to us if they believe their data protection rights have been breached.

We will acknowledge receipt within 30 days and provide a substantive response without undue delay. If you are not satisfied with our response, you may escalate the matter to the Information Commissioners Office (ICO).

Further information about how the Trust handles data protection complaints can be found at Appendix 3 of this policy, along with a data protection complaints form at Appendix 4. Complaints can be made in writing to the School Office email address: office@christchurchhanham.org.uk

Personal Data Breaches

The UK GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. Please refer to our Data Breach Policy. This is available within this document.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches who is the School Business Manager or the School DPO.

Transparency and Privacy Notices

The School will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The School's privacy notices are tailored to suit the data subject and set out information about how the School use their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.



When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the UK GDPR. Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as “children” under the UK GDPR.

Privacy by Design

The School adopt a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the School conduct DPIAs for any new high-risk technologies or programmes being used by the School which could affect the processing of personal data. The School carries out DPIAs when required by the UK GDPR in the following circumstances:

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; and
- For large scale, systematic monitoring of a publicly accessible area (for example, through the use of CCTV).

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used;
- Details of what types of data are shared;
- Steps taken by the third party and the school in order to protect data;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The School are required to keep full and accurate records of our data processing activities (Records of Processing Activities (ROPA)). These records include:

The name and contact details of the School;

- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the School's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

Training

The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. The school will carry out adequate training with all staff and any urgent updates will be issued in the weekly staff briefing.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Audit

The School, through its Data Protection Officer, regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

Related Policies

Staff should refer to the following policies that are related to this Data Protection Policy:

- Data Breach Policy
- Data Retention Policy
- Bring Your Own Device Policy
- Cyber Security Policy
- Freedom of Information Policy and Publication Scheme
- Information Security Policy
- Social Media Policy

These policies are also designed to protect personal data and can be found within this document and the acceptable use policy can be found on the school website.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

Section 5 – Automated Processing and Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are required to ensure that appropriate safeguards are in place when using automated decision making for significant decisions and the circumstances in which we are permitted to use special category data (sensitive information) in automated decision making are limited.

You will not be subject to automated decision making for significant decisions unless we have a lawful basis for doing so, including a valid condition where required, and appropriate safeguards are in place. Appropriate safeguards include informing the relevant individuals about the automated decision making and their rights to request a human review, express their views, and contest the decision.

The School will carry out a data protection impact assessment before any new automated processing or automated decision-making activities are undertaken.



Appendix 1 – Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the School are undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A data subject has the right to be informed by the School of the following:

1. Confirmation that their personal data is being processed;
2. Access to their personal data;
3. The following 'supplementary information':
 - a. The purposes of processing;
 - b. The categories of personal data concerned;
 - c. The recipients or categories of recipients to whom the data have been or will be disclosed;
 - d. Where possible, the period for which the data will be stored, or the criteria used to determine that period;
 - e. The existence of the data subject's rights to rectification, erasure, restriction, objection and data portability;
 - f. The right to lodge a complaint with the ICO;
 - g. Where the data were not collected directly from the individual, any available information about the source;
 - h. Any automated decision-making, including profiling, and information about the logic involved, as well as the significance and envisaged consequences of such processing; and,
 - i. Where relevant, details of the safeguards applied to data transferred outside the UK.

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, we will have only one month in which to respond to a SAR and even if an extension of the time limit is permitted, the individual must still be informed within that month of the fact that the request will take longer to process and the reasons for the delay. Failure to deal with a SAR within that period could leave us open to the possibility of being fined by the ICO.

All staff must be aware of the potential for receiving a SAR and the importance of dealing with such as request as a matter of urgency.

Anyone within the School may receive a SAR. It does not need to be made to a nominated person or even to a person responsible for dealing with either the data subject or information of that type. It will be equally as valid if sent to anyone within the school.

If you receive a SAR, please contact the School Business Manager. A request for information does not need to mention that it is a SAR provided that it is clear that it is an individual asking for their own personal data. There is no specified wording and it does not have to be on an official form. A SAR does not need to be in writing and can be made verbally, by post, by email or even using social media where relevant.

How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the School process personal data about him or her and, if so



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- for access to that personal data
- and/or certain other supplementary information (listed above).

A valid SAR can be both in writing (by letter, email, WhatsApp text, social media) or verbally (e.g., during a telephone conversation or meeting). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

How to Make a Data Subject Access Request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

If a request is made verbally, we will ensure we follow this up with something in writing to confirm what has been requested and outline the timeframe for dealing with the request.

What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the School Business Manager who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the School must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual. If ever in doubt, please refer the request to the School Business Manager.

Acknowledging the Request

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:

- proof of ID (if needed);
- further clarification about the requested information if it is not clear what information is required;
- if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The School should work with their DPO in order to create the acknowledgment.

Verifying the Identity of a Requester or Requesting Clarification of the Request

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees and current students, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be required to confirm why the request has been made.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

The School shall let the requestor know as soon as possible where more information is needed before responding to the request.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding may be paused when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the school will be unable to comply with the request if they do not receive the additional information.

Requests Made by Third Parties or on Behalf of Children

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Fee For Responding to a SAR

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School may charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received. If the deadline to comply with the request falls on the weekend or public holiday, the deadline will be the next working day.

The circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third-party requester, the written authorisation of the data subject has been received. Where the school may be required to get consent from a pupil, the time period will not start until consent is received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School Closure Periods

The school may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the School will be closed. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the School re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data we process about him or her and the supplementary information listed above.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. Where a request is made by electronic means, and unless the requestor asks otherwise, the School will normally provide the information in a commonly used electronic format (for example, PDF). The format of the response will reflect the method of the request where reasonable and appropriate, unless the requestor specifies another preferred, reasonable and appropriate, format.

The information that the School are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the School is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

How to Locate Information

The personal data the School need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the School may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- safeguarding systems (CPOMS);
- MIS system (Arbor);
- HR system (Every)
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

We will handle data subject rights requests and searches in a manner that is reasonable and proportionate to the nature of the request, the amount of data involved, and the effort required. We will not conduct searches that would impose a disproportionate burden on our operations where this would go beyond what is reasonable to locate personal data.

Protection of Third Parties - Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such



consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard, then the DPO should be consulted.

Other Exemptions to the Right of Subject Access

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School do not have to disclose any confidential references given to, or received from, third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

Legal professional privilege: The School do not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting: The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity, to the extent that disclosure of the information would be likely to prejudice the conduct of the School's business or other activity.

Negotiations: The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

The school can refuse to comply with a request if the request in certain circumstances. These include:

- Where the SAR is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature;
- To avoid obstructing an official or legal inquiry, investigation or procedure;
- To avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- To protect public security;
- To protect national security;
- To protect the rights and freedoms of others.

In the event that you have concerns about supplying the information, you must always refer the matter to the DPO who will make the decision on our behalf.

In the event that we decide not to comply with the SAR, then the data subject must be informed, without undue delay (and in all cases within one month of receipt of the request), of:

- The reasons we are not taking action;
- That they have a right to make a complaint to the ICO or another supervisory authority; and
- That they are entitled to seek to enforce their right through a judicial remedy.

If a request is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision.



Christ Church Hanham CE Primary School

Nurture with love - **Grow** through knowledge and wisdom - **Flourish** in hope

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

Record Keeping

A record of all subject access requests shall be kept by the School Business Manager. The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Appendix 2 – Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

Personal Information

If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Details:

Employment records:

If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility
- ☐ Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

- ☐ Receive the information by post*
- ☐ Receive the information by email
- ☐ Collect the information in person
- ☐ View a copy of the information only
- ☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: office@christchurchhanham.org.uk



Appendix 3 – Data Protection Complaints

Under Data Protection Law, individuals have the right to raise concerns or make complaints about the way their personal data has been handled. This includes concerns about how the School collects, stores, uses, shares, or secures personal data, as well as how the School has responded to a previous data protection related request (for example, a Subject Access Request).

The purpose of this right is to ensure that individuals can easily challenge potential non-compliance, seek clarification or correction, and help the School to continually improve its data protection practices.

This appendix provides guidance for staff on how to handle data protection complaints and for individuals on how to submit one.

Failure to address data protection complaints appropriately can expose the School to enforcement action by the ICO and reputational risk. The School therefore treats all complaints seriously and in accordance with this policy.

What is a Data Protection Complaint?

A data protection complaint is any expression of dissatisfaction from an individual (or their authorised representative) about how the School has processed their personal data or handles a data protection request.

Examples include complaints about:

- Inaccurate, incomplete, or outdated information being held;
- Personal data being used or shared without lawful basis;
- A delay or failure to respond to a Subject Access Request or other data rights request;
- Inappropriate disclosure or loss of personal data;
- Lack of transparency in how data is collected or used;
- Concerns about automated decision-making or profiling; or,
- Any other alleged breach of the UK GDPR or Data Protection Act 2018.

A complaint does not need to reference “data protection” or “UK GDPR” to be valid; any statement indicating concern about how personal data has been handled must be treated as such.

How to Make a Data Protection Complaint

Individuals can make a complaint verbally or in writing (including by email, letter, or online form). To help ensure a full and efficient investigation, complainants are encouraged to use the Data Protection Complaint Form provided below in Appendix 4, providing:

- Their name and contact details;
- A clear description of the concern;
- Any relevant dates, correspondence, or evidence; and,
- The outcome they seek.

Complaints should be directed to the School Office.

Acknowledging and Investigating a Complaint:

The School will acknowledge the complaint within 30 days of receipt. The acknowledgment will confirm that the complaint has been received, outline the next steps, and provide contact details for any questions.

Where clarification or additional evidence is required to investigate the complaint properly, the response timeframe may be paused until sufficient information has been provided. All complaints will be handled confidentially and investigated promptly, fairly, and proportionately.

The School will aim to provide a substantive response as soon as reasonably practicable. The investigation may involve consultation with relevant departments, review of systems or records, and advice from the School DPO.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Outcome of a Complaint

Following investigation, the School will provide a written response setting out:

- The findings of the investigation;
- Any corrective or preventative action the School will take (if appropriate); and,
- The right to escalate the matter to the ICO if the complainant remains dissatisfied.

Complaints Received During School Closure Periods

The School will endeavour to acknowledge and investigate complaints as soon as reasonably practicable. However, during school closure periods, offices and systems may not be routinely monitored, which could delay acknowledgment and investigation. Where a complaint is received during such a period, the School will:

- Record the date of receipt;
- Acknowledgment the complaint as soon as possible; and,
- Provide an update to the complainant once the School reopens.

Complainants who require an urgent response are encouraged to submit their complaint during term time wherever possible.

Record Keeping

The School will maintain a record of all data protection complaints, including:

- The date the complaint was received;
- The complainant's name;
- The nature of the complaint;
- Any key investigative steps taken;
- The outcome and date of response; and,
- Any follow-up actions taken.

Records will be retained in accordance with the School's Records Retention Schedule.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Appendix 4 – Data Protection Complaints Form

The UK GDPR and the Data Protection Act 2018 give you the right to raise a concern or make a complaint about the way the School processes your personal data, handles your request, or otherwise complies with data protection law.

Please complete this form if you wish to raise a complaint and send it to the school office. The School will acknowledge your complaint within 30 calendar days of receipt and will aim to provide you with a full response as soon as reasonably practicable.

Proof of Identity

If your complaint relates to the processing of personal data and we need to verify your identity, we may ask for proof of identity before investigating. Acceptable documents include a copy of your passport, driving licence.

Section 1 – Complainant Details

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

Section 2 – Details of Complaint

Please describe your concern in as much detail as possible. Include dates, names, and copies of any relevant correspondence or documents if available.

Have you previously raised this concern with the School?	☐ Yes ☐ No
If yes, please provide the date and to whom it was reported:	
What outcome are you seeking?	



Christ Church Hanham CE Primary School

Nurture with love - **Grow** through knowledge and wisdom - **Flourish** in hope

Section 3 – Representative (if applicable)

If you are making this complaint on behalf of someone else, please complete the section below.

You must provide proof of your identity and evidence of your authority to act on behalf of the data subject.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	
Relationship to Data Subject	

Proof of Authorisation (enclose one):

☐ Letter of authority ☐ Power of Attorney ☐ Parental responsibility ☐ Other (details): _____

Section 4 – Acknowledgement and Declaration

- ☐ I confirm that the information provided in this form is accurate to the best of my knowledge.
- ☐ I understand that the School may need to contact me to clarify details and may need to verify my identity before investigating.

Signature: _____ Date: _____



Data Breach Policy

Data Breach Policy

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

Definitions

Personal Data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.
Special Category Data	Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions
Personal Data Breach	A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data or special category data transmitted, stored or otherwise processed.
Data Subject	Person to whom the personal data relates.
ICO	The ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.
Data Protection Officer (DPO)	The person we appoint from time to time to lead the development and implementation of our data protection and compliance with the UK GDPR and other applicable.

Responsibility

The School Business Manager has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of the School Business Manager, please contact the Headteacher.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the School Business Manager in the first instance if you have any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being followed. Should the matter remain unresolved, or requires further escalation, please contact our DPO.

The DPO's contact details are set out below: -

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 opt 1, then opt 1

Security and Data Related Policies

We must keep personal data secure against loss or misuse. All staff are required to comply with our information security guidelines and policies. In particular, staff should refer to the following policies that are related to this Data Breach Policy:

- *Security Policy* which sets out the School's guidelines and processes on keeping personal data secure against loss and misuse.
- *Data Protection Policy* which sets out the School's obligations under UK GDPR about how they process personal data.
- *Cyber Security Policy* which sets out the School's obligations and guidelines for cyber security issues.

These policies are also designed to protect personal data and can be found at on the school website or by requesting from the school office.

Data Breach Procedure

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored for example, loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example, sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it;
- Alteration of personal data without permission;
- Loss of availability of personal data.

When does it need to be reported?

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed, the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- Potential or actual discrimination;
- Potential or actual financial loss;
- Potential or actual loss of confidentiality;
- Risk to physical safety or reputation;
- Exposure to identity theft (for example, through the release of non-public identifiers such as passport details);
- The exposure of the private aspect of a person's life becoming known by others.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

- Complete a data breach report form (Appendix 1);
- Email the completed form to the School Business Manager.

Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from the School Business Manager or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The School Business Manager will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording the Breach

On being notified of a suspected personal data breach, the School Business Manager will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so, the school will take steps to:-

- Where possible, contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO where required;
- Notify data subjects affected by the breach if required;
- Notify other appropriate parties to the breach; and
- Take steps to prevent future breaches.

Assessing the Breach

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover, correct or delete data (for example, notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e., the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation, two factor authentication);
- What has happened to the data, e.g., if data has been stolen, could it be used for harmful purposes;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

Containment and Recovery

The School Business Manager with the support of our DPO will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

The School Business Manager with the support of our DPO will identify ways to recover, correct or delete data. This may include contacting the police, e.g., where the breach involves stolen hardware or data.

Depending on the nature of the breach, the School Business Manager with the support of our DPO, will notify the appropriate insurer, as the insurer can provide access to data breach management experts.

Notifying the ICO

The School Business Manager will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (i.e., it is not 72 working hours). If the School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

If the school are unsure whether to report, the presumption should be to report. The school will take into account of the factors set out below:

The potential harm to the rights and freedoms of data subjects

This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include:

- Exposure to identify theft through the release of non-public identifiers, e.g. passport number;
- Information about the private aspects of a persons life becoming known to others, e.g. financial circumstances;

The personal data breach must be reported unless it is unlikely to result in a risk to data subjects' rights and freedoms.

The volume of personal data

There should be a presumption to report to the ICO where:

- A large volume of personal data is concerned; and
- There is a real risk to individuals suffering some harm.

It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances if the loss or the extent of information about each individual.

The sensitivity of data

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.

This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report. The ICO provides two examples:

- theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable;
- breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss) would not be reportable.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the School Business Manager will notify the affected individuals without undue delay including the name and contact details of the DPO and the ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach, including where appropriate, recommendations for mitigating potential adverse effects.

When determining whether it is necessary to notify individuals directly of the breach, the School Business Manager will co-operate with and seek guidance from the DPO, the IC and any other relevant authorities (such as the police).



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example, by making a statement on the School website).

Notifying the Police

The School will already have considered whether to contact the police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act, the school will notify the police and/or relevant law enforcement authorities.

Notifying Other Authorities

The School will need to consider whether other parties need to be notified of the breach. For example:

- The Information Commissioner's Office (ICO);
- Affected data subjects;
- Insurers;
- Parents;
- Third parties (for example, when they are also affected by the breach);
- Local authority;
- The police (for example, if the breach involved theft of equipment or data).

This list is non-exhaustive.

Preventing Future Breaches

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred;
- Assess whether the breach was a result of human error or a systematic issue;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time, and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to the Headteacher or School Business Manager. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

If you have concerns that your personal data has been involved in a data breach, or you have concerns about a suspected breach of any of your data rights, please refer to the School's Data Protection Policy for details of how to submit a data protection complaint.

Staff Awareness and Training

Key to the success of our systems is staff awareness and understanding. We provide regular training to staff:

- At induction;
- When there is any change to the law, regulation or our policy;
- When significant new threats are identified; and
- In the event of an incident affecting our school.

The School will ensure that staff are trained and aware on the need to report data breaches to ensure that they know to detect a data breach and the procedures of reporting them. This policy will be shared with staff.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.



Christ Church Hanham CE Primary School

Nurture with love - **Grow** through knowledge and wisdom - **Flourish** in hope

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Appendix 1 – Data Breach Report Form

If you know or suspect a personal data breach has occurred, please:

- Complete this form; and
- Email or deliver it to The School Business Manager and Headteacher, ensuring that you mark your email as urgent, with the subject 'Data Breach'.

Time is of the essence with data breaches. You must submit this report as soon as know or suspect there has been a data breach. Do not delay to satisfy yourself whether a data breach has definitely happened and do not contact any individuals who may be affected by the data breach. The School Business Manager along with DPO, will investigate the potential breach and take necessary actions.

Name and contact details of person notifying the actual or suspected breach	<i>[Insert name and contact details]</i> <i>If you wish to submit an anonymous report, leave this section blank</i>
Date of actual or suspected breach	<i>[Insert date]</i>
Date of discovery of actual or suspected breach	<i>[Insert date]</i>
Date of this report	<i>[Insert date]</i>
Summary of the facts	<i>[Provide as much information as possible – including the amount, sensitivity and type of data involved]</i>
Cause of the actual or suspected breach	<i>[Provide a detailed account of what happened]</i>
Is the actual or suspected breach ongoing?	Yes ☐ No ☐ Not known ☐
Who is or could be affected by the actual or suspected breach?	<i>[Include details of categories and approximate number of data subjects concerned]</i>
Are you aware of any related or other data breaches?	Yes ☐ No ☐ <i>[If yes, provide more details]</i>



Data Retention Policy

Data Retention Policy

The School has a responsibility to maintain its records and record keeping systems. When doing this, the School will take account of the following factors:

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Accessibility of records and record keeping systems.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the School's current practice, the requirements of current legislation and best practice and guidance. All staff must be familiar with this policy and comply with it. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

Data Protection

This policy sets out how long employment-related and pupil data will normally be held by the School and when that information will be confidentially destroyed in compliance with the terms of the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the School. The School's Data Protection Policy outlines its duties and obligations under the UK GDPR.

Retention Schedule

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule.

The retention schedule refers to all records regardless of the media (e.g., paper, electronic, microfilm, photographic etc) in/on which they are stored. All records will be regularly monitored by the School Business Manager.

Destruction of Records

The schedule is a relatively lengthy document listing the many types of records used by the School and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

Where records have been identified for destruction, they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate wastepaper merchant. All electronic information will be deleted.

The School maintains a database of records which have been destroyed and who authorised their destruction (detailed in Appendix 1). When destroying documents (paper and electronic records), the appropriate staff member should record in this list the following:

- File reference (or other unique identifier);
- File title/description;
- Number of files;
- Name of the authorising officer;



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- Date destroyed or deleted from system; and
- Person(s) who undertook destruction.

Retention of Safeguarding Records

Any allegations made that are found to be malicious must not be part of the personnel records.

For any other allegations made, the School must keep a comprehensive summary of the allegation made, details of how the investigation was looked into and resolved and any decisions reached. This should be kept on the personnel files of the accused.

Any allegations made of sexual abuse should be preserved by the School for the term of an inquiry by the Independent Inquiry into Child Sexual Abuse. All other records (for example, the personnel file of the accused) should be retained until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer. In 2022 the Independent Inquiry into Child Sexual Abuse (IICSA) concluded and published their final report, leaving a recommendation that all records relating to child sexual abuse should be retained for a period of 75 years.

The ICO has not currently produced guidance or frameworks regarding retention as recommended by the inquiry. Until this has been produced, records will still be retained for a prolonged period as recommended initially by IISCA in order to fulfil potential legal duties that a school may have in relation to the inquiry or any further guidance.

Archiving

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the School Business Manager. The appropriate staff member, when archiving documents should record in this list the following information:

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

Files in our archive will be filed away with the destruction date as appropriate.

Transferring Information to Other Media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

Transferring Information to Another School

We retain the pupil's educational record whilst the child remains at the School. Once a pupil leaves the School, the file should be sent to their next school. The responsibility for retention then shifts onto the next school. We retain the file for a year following transfer in case any issues arise as a result of the transfer.

We may delay destruction for a further period where there are special factors such as potential litigation.

Responsibility and Monitoring

The School Business Manager has primary and day-to-day responsibility for implementing this policy. The Data Protection Officer, in conjunction with the School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The Data Protection Officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this policy and are given adequate and regular training on it.

Emails

Emails accounts are not a case management tool in itself. Generally, emails may need to fall under different retention periods (for example, an email regarding a health and safety report will be subject to a different time frame to an email which forms part of a pupil record). It is important to note that the retention period will depend on the content of the email and it is important that staff file those emails in the relevant areas to avoid the data becoming lost.

Pupil Records

All schools with the exception of independent schools, are under a duty to maintain a pupil record for each pupil. If a child changes schools, the responsibility for maintaining the pupil record moves to the next school. We retain the file for a year following transfer in case any issues arise as a result of the transfer.

Retention Schedule

<u>FILE DESCRIPTION</u>	<u>RETENTION PERIOD</u>
Employment Records	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
Job applications and interview records of successful candidates	Added to staff personnel file and retained in line with that record (6 years after employment ceases)
Written particulars of employment, contracts of employment and changes to terms and conditions	Added to staff personnel file and retained in line with that record 6 years after employment ceases.
Right to work documentation including identification documents and immigration checks	Kept separately from personnel file and retained for 2 years after employment ceases. Employer's guide to right to work checks: 21 June 2024
DBS checks and disclosures of criminal records forms	DBS certificates should be destroyed as soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months
Change of personal details notifications	No longer than 6 months after receiving this notification
Emergency contact details	Destroyed on termination
Personnel records	While employment continues and up to six years after employment ceases (Limitation Act 1980)
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Working Time Regulations: - Opt out forms - Records of compliance with WTR	- Two years from the date on which they were entered into - Two years after the relevant period
Disciplinary records	6 years after employment ceases (Limitation Act 1980)
Grievance records	6 years after employment ceases (Limitation Act 1980)
Training	6 years after employment ceases (Limitation Act 1980) or length of time required by the professional body
Staff training where it relates to safeguarding or other child related training	Date of the training plus 40 years (This retention period reflects that the IICSA may wish to see training records as part of an investigation)
Annual appraisal/assessment records	Current year plus 3 years
Professional Development Plans	Life of the plan or plan superseded + 6 years
Allegations of a child protection nature against a member of staff including where the allegation is unfounded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.
Financial and Payroll Records	
Pension records	12 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	6 years from the end of the scheme year in which the event took place
Payroll and wage records	6 years after end of tax year they relate to (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to (Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567))
Statutory Sick Pay	3 years after the end of the tax year they relate to (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Current bank details	Until updated plus 3 years (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Bonus Sheets	Current year plus 3 years (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Time sheets/clock cards/flexitime	Current year plus 3 years (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Pupil Premium Fund records	Date pupil leaves the provision plus 6 years
National Insurance (schedule of payments)	Current year plus 6 years (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Insurance	Current year plus 6 years (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Overtime	Current year plus 3 years (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Annual accounts	Current year plus 6 years



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Loans and grants managed by the School	Date of last payment on loan + 6 years if the loan is under 10,000 or date of last payment on loan + 12 years if the loan is over 10,000
All records relating to the creation and management of budgets	Life of the budget plus 3 years
Invoices, receipts, order books and requisitions, delivery notices	Current financial year plus 6 years
Student Grant applications	Current year plus 3 years
Pupil Premium Fund records	Date pupil leaves the provision or school plus 6 years
School fund documentation (including but not limited to invoices, cheque books, receipts, bank statements etc).	Current year plus 6 years
Free school meals registers (where the register is used as a basis for funding)	Current year plus 6 years
School meal registers and summary sheets	Current year plus 3 years
Agreements and Administration Paperwork	
Collective workforce agreements and past agreements that could affect present employees	Permanently
Trade union agreements	10 years after ceasing to be effective
Strategic Plan or School Development Plans	Life of plan or until plan superseded + 3 years. If major changes are made to the plan then an archive copy of previous plans should be retained
Visitor Signing-in Records	6 years
Newsletters and circulars to staff, parents and pupils	1 year (and the School may decide to archive one copy)
Minutes of Senior Management Team meetings	Date of the meeting plus 3 years or as required
Reports created by the Head Teacher or the Senior Management Team.	Date of the report plus a minimum of 3 years or as required
Records relating to the creation and publication of the school prospectus	Current academic year plus 3 years
Health and Safety Records	
Health and Safety consultations	Permanently
Health and Safety Risk Assessments	Life of the risk assessment plus 3 years
Health and Safety Policy Statements	Life of policy plus 3 years
Any records relating to any reportable death, injury, disease or dangerous occurrence	Date of incident plus 3 years provided that all records relating to the incident are held on personnel file
Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Until the child reaches the age of 21. (Limitations Act 1980)



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Date of last entry in the accident book + 3 years but if there is possibility of negligence allegation then date of incident + 15 years or date of settlement + 6 years. (Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980)
Fire precaution log books	Current year plus 6 years
Medical records and details of: - - control of lead at work - employees exposed to asbestos dust - records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record (Control of Substances Hazardous to Health Regulations (COSHH); Control of Asbestos at Work Regulations)
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made
Temporary and Casual Workers	
Records relating to hours worked and payments made to workers	3 years
Governing Body Documents	
Instruments of government	For the life of the School. Consult local archives before disposal
Meetings schedule	Current year
Minutes – principal set (signed)	Date of meeting + 10 years
Agendas – principal copy	Where possible the agenda should be stored with the principal set of the minutes
Agendas – additional copies	Date of meeting
Policy documents created and administered by the governing body	Until replaced
Register of attendance at full governing board meetings	Date of last meeting in the book plus 6 years
Annual Reports created under the requirements of the Education (Governors Annual Reports) (England) (Amendment) Regulations 2002	Date of report plus 10 years
Records relating to complaints made to and investigated by the governing body or head teacher	Major complaints: current year plus 6 years. If negligence involved: current year plus 15 years. If child protection or safeguarding issues are involved then: current year plus 40 years. If the complaint relates to child sexual abuse, then indefinitely. (Based on recommendations left by the IICSA, will be reviewed upon publication of ICO guidance)
Correspondence sent and received by the governing body or head teacher	General correspondence should be retained for current year plus 3 years
Records relating to the terms of office of serving governors, including evidence of appointment	Date appointment ceases plus 6 years except where there have been allegations concerning children. In this case retain for 25 years.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Register of business interests	Date appointment ceases plus 10 years (Companies Act 2006)
Records relating to the training required and received by governors	Date appointment ceases plus 6 years
Records relating to the appointment of a clerk to the governing body	Date on which clerk appointment ceases plus 6 years
Governor personnel files	Date appointment ceases plus 6 years
Pupil Records	
Details of whether admission is successful/unsuccessful	1 year from the date of admission/non-admission (School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels)
Proof of address supplied by parents as part of the admissions process	Current year plus 1 year (School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels)
Admissions register	Entries to be preserved for six years from date of entry (Working together to improve school attendance, Section, 36, 2024 Statutory guidance)
Pupil Record, including non-child protection safeguarding records.	Primary – Whilst the child attends the School (The Education (Pupil Information) (England) Regulations 2005, The Pupil Information (Wales) Regulations 2011) Secondary – until the child reaches the age of 25 (Limitation Act 1980, Section 2)
Attendance Registers	Six years from the date of entry (Working together to improve school attendance, Section 36, 2024 Statutory guidance)
Correspondence relating to any absence (authorised or unauthorised)	Current academic year plus 2 years (Education Act 1996, Section 7)
Special Educational Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Primary school - whilst the child attends the school. Secondary - Date of birth of the pupil plus 31 years (Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan). (Children and Family's Act 2014; Special Educational Needs and Disability Act 2001)
Child protection information (to be held in a separate file).	DOB of the child plus 25 years then review. If aspects of the record relate to child sexual abuse, then these records should be retained indefinitely. (Based on recommendations left by the IICSA, will be reviewed upon publication of ICO guidance)
Exam results (pupil copy)	This information should be added to the pupil file and retained in line with that record.
Examination results (school's copy)	Current year plus 6 years
Allegations of sexual abuse	If the complaint relates to child sexual abuse, then indefinitely. (Based on recommendations left by the IICSA, will be reviewed upon publication of ICO guidance)
Records relating to any allegation of a child protection nature against a member of staff	Until the accused normal retirement age or 10 years from the date of the allegation (whichever is the longer) (Retention period informed by the guidance of KCSIE)



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Consents relating to school activities as part of UK GDPR compliance (for example, consent to be sent circulars or mailings)	Evidence of consent will be retained whilst the pupil attends the school, or until withdrawn, whichever the shorter.
Pupil's work	Where possible, returned to pupil at the end of the academic year (provided the School have their own internal policy to this effect). Otherwise, the work should be retained for the current year plus 1 year
Mark books	Current year plus 1 year
Schemes of work	Current year plus 1 year
Timetable	Current year plus 1 year
Class record books	Current year plus 1 year
Record of homework set	Current year plus 1 year
Photographs of pupils	For the time the child is at the School and for a short while after. Please note select images may also be kept for longer (for example to illustrate history of the school)
Parental consent forms for school trips where there has been no major incident	End of the trip or end of the academic year (subject to a risk assessment carried out by the School)
Parental permission slips for school trips where there has been a major incident	Date of birth of the pupil involved in the incident plus 25 years. Permission slips for all the pupils on the trip should be retained to demonstrate the rules had been followed for all pupils
Other Records	
Privacy notices	Until replaced plus 6 years
Inventories of furniture and equipment	Current year plus 6 years
All records relating to the maintenance of the School carried out by contractors or employees of the school	Whilst the building belongs to the school
Records relating to the letting of school premises	Current financial year plus 6 years
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	Current year plus 6 years then review
Referral forms	While the referral is current
Contact data sheets	Current year then review, if contact is no longer active then destroy



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Appendix 1 - Data Destruction Log

File Reference Number	Description of Record/Document	Number/Detail of Documents Included	Details of Action Carried Out and Date Destroyed	Name of Staff Member and Date
<i>Example: Staff2016</i>	<i>Job description, CV, contract, qualifications and certifications</i>	<i>5 ex-staff members</i>	<i>Shred-It – Data Destruction certificate: ShredIt 2701</i>	<i>John Smith – 01/01/01</i>



Bring Your Own Device Policy

The School has implemented this policy to protect the School and all parties when using ICT and media devices. Staff are able to use devices at work and outside of work for work related activities provided the terms of this policy are met. The School reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below. This policy is intended to protect the security and integrity of the School's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. This policy is not designed to offer protection for the device itself. The safety of the user's own device is the responsibility of the user.

Mobile devices within the context of this policy includes any mobile phone, tablet, laptop, MP3/iPod or other device which is capable of connecting with the internet or mobile networks or taking image or sound recordings.

This guidance is in addition to the School's Acceptable Use Policy (separate policy).

Acceptable Use

The School embrace the use of new and mobile technologies and acknowledge they are a valuable resource in the classroom having educational purpose.

However, by accessing the School's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing so (including ensuring adequate security of that personal information).

All employees must agree to the following terms and conditions in order to be able to connect their devices to the company network:

- All staff who wish to use their own devices to access the School's network must sign and return the statement at the conclusion of this policy.
- All internet access via the network is logged and as set out in the Acceptable Use policy, employees are blocked from accessing certain websites whilst connected to the School network.
- The use of camera, microphone and/or video capabilities are prohibited whilst in School unless this has been approved by the Headteacher. If approved, any pictures, videos or sound recordings can only be used for School purposes and cannot be posted or uploaded to any website or system outside of the School network.
- If approved to use personal device, you should upload any pictures, video or sound recordings to our school network and delete from personal devices.
- You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.
- WhatsApp must not be used on personal devices for School related communication. Members of staff are able to use WhatsApp on their own devices for personal communication. However, staff should not communicate internally with other staff members for School business using their personal WhatsApp accounts, sharing School related information which could include categories of personal data.

Non-acceptable Use

- Any apps or software which are downloaded onto the user's device whilst using the School's own network is done at the users risk and not with the approval of the School.
- Devices may not be used at any time to:
 - Store or transmit illicit materials;
 - Store or transmit proprietary information belonging to the School;
 - Harass others;
 - Act in any way against the School's Acceptable Use policy and other safeguarding and data related policies.
- Technical support is not provided by the School on the user's own devices.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- Storing school data on personal devices is not allowed. This includes forwarding school emails to your personal email address.

Devices and Support

- Smartphones including iPhones and Android phones are allowed;
 - Tablets including iPad and Android are allowed;
 - Devices must be presented to IT for proper job provisioning and configuration of standard apps such as browsers, office productivity software and security tools, before they can access the network.
- In order to prevent unauthorised access, devices must be password/pin/fingerprint protected using the features of the device and a strong password is required to access the School network.

Security

- When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example, through password protection and cloud back up), keeping information confidential (for example, by ensuring access to emails or sensitive information is password protected) and maintaining that information.
- The School does not accept responsibility for any loss or damage to the user's device when used on the School's premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).
- If information is particularly sensitive then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device).
- In the event of any loss or theft of personal data/device, this must be reported immediately as a data breach in accordance with the School's Data Breach policy.
- The School may require access to a device when investigating policy breaches (for example, to investigate cyber bullying).
- Staff are not permitted to share access details to the School's network or Wi-Fi password with anyone else.

Disclaimer

- The School will not monitor the content of the user's own device but will monitor any traffic over the School system to prevent threats to the School's network.
- The School reserves the right to disconnect devices or disable services without notification.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the School's policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The School reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

I confirm that I have read, understood and will comply with the terms of the Bring Your Own Device Policy when using my mobile device to access the School network.

Signed:

Date:

Print Name:



Cyber Security Policy

Introduction

Cyber security has been identified as a risk for the School and every employee needs to contribute to ensure data security.

The School has invested in technical cyber security measures but we also need our employees to be vigilant and to act to protect the School IT systems.

The School Business Manager is responsible for cyber security within the School.

If you are an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies, namely our Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy (separate document), Home Working Policy and Electronic Information and Communications Policy (all found within this document).

Purpose and Scope

The purpose of this document is to establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as to set out an action plan should the School fall victim to cyber-crime. This policy is relevant to all staff.

What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet including hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- Cost – The global cost of all forms of online crime is estimated to be in excess of £300 billion. We may be fined up to £17.5 million or 4% of the total worldwide annual turnover if we fail to protect our data.
- Confidentiality and data protection - Protecting individuals' confidential information and all forms of personal data is one of the most essential requirements our school. The risk to confidential information and personal data is the biggest of all threats from cyber-crime.
- Potential for regulatory breach – We have various regulatory duties which we could unintentionally breach through falling victim to cyber-crime or a cyber-attack. Loss of personal data can lead to claims for damages by the individuals concerned and/or significant fines from the Information Commissioners Office (ICO).
- Reputational damage – A cyber security incident can have a major impact on our reputation, particularly if it involves the loss of confidential information, personal data and/or is reported in the media. Protecting our reputation is of utmost importance.
- Business interruption – Some forms of cyber-attack could render key systems (for instance servers including email servers, cloud computing services or our website) unavailable. This would have a major impact on delivering lessons and delivering our services. It may be necessary in such cases to invoke our Business Continuity Plan. The School Business Manager is responsible for making that decision and communicating with IT.
- Structural and financial instability – The financial losses flowing from online crime may cause or contribute to financial difficulty.

Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for the School to take preventative measures and for staff to follow the guidance within this policy.

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

The School have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff.

Technology Solutions

The School have implemented the following technical measures to protect against cyber-crime:

- firewalls;
- anti-virus software;
- anti-spam software;
- auto or real-time updates on our systems and applications;
- URL filtering;
- secure data backup;
- encryption;
- deleting or disabling unused/unnecessary user accounts;
- deleting or disabling unused/unnecessary software;
- using strong passwords; and
- disabling auto-run features.

Controls and Guidance for Staff

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.
- Technology solutions in isolation cannot protect us adequately, so our systems and controls extend to cover the human element of cyber-crime/cyber security risk.
- All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the School or any third parties with whom we share data.
- It may be appropriate in some instances to limit the number of people involved or who have access to information on a matter to ensure the security of the data involved. This can be part achieved through IT security measures. We may implement other controls that are more practical in nature, e.g.:
 - Physically ringfencing the individuals or teams working on a matter;
 - Taking steps to ensure our system for opening, distributing and/or scanning incoming correspondence (by post, email or otherwise) does not allow or inadvertent sharing of confidential information;
 - Getting a signed confidentiality agreement from each staff member;
 - Disposing of confidential documents securely;
 - Having a clear desk policy;
 - Discouraging staff from reading confidential papers or discussing sensitive matters in public.
 - Due diligence – we may conduct due diligence on the cyber security controls and cyber-crime prevention measures that other parties with whom we share information.
 - All staff must ensure you are familiar with the risks presented by cyber-crime and cyber security attacks or failures and take appropriate action to mitigate the risks by taking a sensible approach, e.g. not forwarding chain letters or inappropriate/spam emails to others. We will help you by continually raising awareness of those risks and providing training where necessary.
 - Report any concerns you may have.

Passwords

- Choose strong passwords (the School's IT team will stipulate the requirements upon setting a password).
- keep passwords secret;
- never reuse a password;
- never allow any other person to access the school's systems using your login details;
- not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the School IT systems;



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to the School Business Manager as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy;
- only access work systems using computers or phones that the School owns. Staff may only connect personal devices to the visitor Wi-Fi provided;
- not install software onto your School computer or phone. All software requests should be made to the School Business Manager; and
- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School equipment and/or networks.

The School considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against the School or using the School's systems;
- accessing inappropriate, adult or illegal content within School premises or using School equipment;
- excessive personal use of School's IT systems during working hours;
- removing data or equipment from School premises or systems without permission, or in circumstances prohibited by this policy;
- using School equipment in a way prohibited by this policy;
- circumventing technical cyber security measures implemented by the School's IT team; and
- failing to report a mistake or cyber security breach.

Cyber-Crime Incident Management Plan

The incident management plan consists of four main stages:

- (i) *Containment and recovery*: To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost. We will notify our insurers as soon as reasonably practicable of any circumstances that may give rise to claim under relevant insurance policies. We will also assess whether it is necessary to invoke our business continuity plan.
- (ii) *Assessment of the ongoing risk*: To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed and any consequences of the breach/attack identified.
- (iii) *Notification*: To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.
- (iv) *Evaluation and response*: To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber security incident involves a personal data breach, the School will invoke their Data Breach Policy rather than follow out the process above.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Freedom of Information Policy and Publication Scheme

Introduction

The Freedom of Information Act 2000 gives individuals the right to access official information from public bodies. Under the Act, any person has a legal right to ask for access to information held by the school. They are entitled to be told whether the school holds the information and to receive a copy, subject to certain exemptions. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information. Full details on how requests can be made are set out in section 1 of this policy.

Public authorities should be clear and proactive about the information they will make public. For this reason, a publication scheme is available and can be found at section 2 of this policy.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. This policy should be used in conjunction with the School's Data Protection Policy.

Section 1 – Freedom of Information Requests

Requests under Freedom of Information should be made to the School Office who will pass onto the School Business Manager. However, the request can be addressed to anyone in the School. All staff need to be aware of the process for dealing with requests. If staff receive a FOI request in their inbox, it should be instantly forwarded to the School Business Manager.

Requests for information that are not data protection or environmental information requests will be covered by the Freedom of Information Act.

Data protection enquiries (or Subject Access Requests/SARs) are requests where the enquirer asks to see what personal information the school holds about the enquirer. If the enquiry is a data protection request, the School's Data Protection Policy should be followed.

Environmental Information Regulations enquiries are those which relate to air, water, land, natural sites, built environment, flora and fauna, health and any decisions and activities affecting any of these. These could, therefore, include enquiries about recycling, phone masts, school playing fields, car parking etc. If the enquiry is about environmental information, follow the guidance on the Department for Environment, Food and Rural Affairs (DEFRA) website.

Freedom of Information requests *must* be made in writing (including email) and should include the enquirer's name, correspondence address (email addresses are allowed) and state what information they require. There must be enough information in the request to be able to identify and locate the information. If this information is covered by one of the other pieces of legislation (as referred to above), they will be dealt with under the relevant policy/procedure related to that request.

If the request is ambiguous and/or the School require further information in order to deal with your request, the School will request this further information directly from the individual making the request. Please note that the School do not have to deal with the request until the further information is received. Therefore, the time limit starts from the date that the School receives all information required in order to deal with the request.

The requester does not have to mention the Act, nor do they have to say why they want the information. There is a duty to respond to all requests, telling the enquirer whether or not the information is held and supplying any information that is held, except where exemptions apply. There is a time limit of 20 school days (i.e., excluding school holidays) for responding to the request.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Information

Provided all requirements are met for a valid request to be made, the School will provide the information that it holds (unless an exemption applies).

Holding information means information relating to the business of the school:

- That the school has created; or
- That the school has received from another body or person; or
- Held by another body on the school's behalf.

Information means both hard copy and digital information, including email.

If the information is held by another public authority (for example, the Local Authority), check whether they hold the information and if so, transfer the request to them. If this applies, the School will notify the enquirer that they do not hold the information and to whom they have transferred the request. The School will continue to answer any parts of the enquiry in respect of information it does hold.

When the School does not hold the information, it has *no duty to create or acquire it* just to answer the enquiry; although a reasonable search will be made before confirming whether the School has the information requested.

If the information requested is already in the public domain, for instance, through the Publication Scheme or on the School's website, the School will direct the enquirer to the information and explain how to access it.

The requester has the right to be told if the information requested is held by the School (subject to any of the exemptions). This obligation is known as the school's *duty to confirm or deny* that it holds the information. However, the school does not have to confirm or deny if:

- The exemption is an absolute exemption; or
- In the case of qualified exemptions, confirming or denying would itself disclose exempted information.

Vexatious Requests

There is no obligation on the School to comply with vexatious requests. A vexatious request is one which is designed to cause inconvenience, harassment or expense rather than to obtain information and would require a substantial diversion of resources or would otherwise undermine the work of the school. However, this does not provide an excuse for bad records management.

In addition, the School do not have to comply with repeated identical or substantially similar requests from the same applicant unless a reasonable interval has elapsed between requests.

Fees

The School may charge the requester a fee for providing the requested information. This will be dependent on whether the staffing costs in complying with the request exceeds the threshold. The threshold is currently £450 with staff costs calculated at a fixed rate of £25 per hour (therefore 18 hours' work is required before the threshold is reached).

If a request would cost less than the threshold, then the school can only charge for the cost of informing the applicant whether the information is held and communicating the information to the applicant (e.g., photocopying, printing and postage costs).

When calculating costs/threshold, the School can take account of the staff costs/time in determining whether the information is held by the School, locating and retrieving the information and extracting the information from other documents. The School will not take account of the costs involved with considering whether information is exempt under the Act.

If a request would cost more than the appropriate limit (£450), the school can turn the request down, answer and charge a fee or answer and waive the fee.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

If the School are going to charge, they will send the enquirer a fees notice. The School do not have to comply with the request until the fee has been paid. More details on fees can be found on the Information Commissioner's Office (ICO) website.

If planning to turn down a request for cost reasons or charge a high fee, you should contact the applicant in advance to discuss whether they would prefer the scope of the request to be modified so that, for example, it would cost less than the appropriate limit.

Where two or more requests are made to the School by different people who appear to be acting together or as part of a campaign, the estimated cost of complying with any of the requests may be taken to be the estimated total cost of complying with them all.

Time Limits

Compliance with a request must be prompt and within the time limit of 20 school days (this does not include the school holidays or weekends) or 60 working days if this is shorter. 'School' days is defined by the ICO as any day on which there is a session, and the pupils are in attendance. Failure to comply could result in a complaint by the requester to the ICO. The response time starts counting as the first day from the next working day after the request is received (so if a request was received on Monday 6th October the time limit would start from the next working day, the 7th October). Where the School has asked the enquirer for more information to enable it to answer, the 20 school days start time begins when this further information has been received.

If some information is exempt this will be detailed in the School's response.

If a qualified exemption applies and the School need more time to consider the public interest test, the School will reply in 20 school days stating that an exemption applies but include an estimate of the date by which a decision on the public interest test will be made. This should be within a "reasonable" time.

Where the School has notified the enquirer that a charge is to be made, the time period stops until payment is received.

Third Party Data

Consultation of third parties may be required if their interests could be affected by release of the information requested and any such consultation may influence the decision.

Consultation will be necessary where:

- Disclosure of information may affect the legal rights of a third party, such as the right to have certain information treated in confidence or rights under Article 8 of the European Convention on Human Rights;
- The views of the third party may assist the School to determine if information is exempt from disclosure; or
- The views of the third party may assist the School to determine the public interest test.

Personal information requested by third parties is also exempt under this policy where release of that information would breach the Data Protection Act. If a request is made for a document (e.g., Governing Body minutes) which contains personal information whose release to a third party would breach the Data Protection Act, the document may be issued by blanking out the relevant personal information as set out in the redaction procedure.

Exemptions

The presumption of the Freedom of Information Act is that the School will disclose information unless the Act provides a specific reason to withhold it. The Act recognises the need to preserve confidentiality and protect sensitive material in certain circumstances.

The School may refuse all/part of a request, if one of the following applies:

- 1) There is an exemption to disclosure within the Act;



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- 2) The information sought is not held;
- 3) The request is considered vexatious or repeated; or
- 4) The cost of compliance exceeds the threshold.

A series of exemptions are set out in the Act which allow the withholding of information in relation to an enquiry. Some are specialised in their application (such as national security) and would not usually be relevant to schools.

There are two general categories of exemptions:

- 1) **Absolute:** where there is no requirement to confirm or deny that the information is held, disclose the information or consider the public interest; and
- 2) **Qualified:** where, even if an exemption applies, there is a duty to consider the public interest in disclosing information.

Absolute Exemptions

There are eight absolute exemptions set out in the Act. However, the following are the only absolute exemptions which will apply to the School:

- Information accessible to the enquirer by other means (for example, by way of the School's Publication Scheme);
- National Security/Court Records;
- Personal information (i.e., information which would be covered by the Data Protection Act);
- Information provided in confidence.

If an absolute exemption exists, it means that disclosure is not required by the Act. However, a decision could be taken to ignore the exemption and release the information taking into account all the facts of the case if it is felt necessary to do so.

Qualified Exemptions

If one of the below exemptions apply (i.e., a qualified disclosure), there is also a duty to consider the public interest in confirming or denying that the information exists and in disclosing information.

The qualified exemptions under the Act which would be applicable to the School are:

- Information requested is intended for future publication (and it is reasonable in all the circumstances for the requester to wait until such time that the information is actually published);
- Reasons of national security;
- Government/international relations;
- Release of the information is likely to prejudice any actual or potential legal action or formal investigation involving the School;
- Law enforcement (i.e., if disclosure would prejudice the prevention or detection of crime, the prosecution of offenders or the administration of justice);
- Release of the information would prejudice the ability of the School to carry out an effective audit of its accounts, resources and functions;
- For health and safety purposes;
- Information requested is environmental information;
- Information requested is subject to legal professional privilege; and
- For *commercial interest* reasons.

Where the potential exemption is a qualified exemption, the School will consider the public interest test to identify if the public interest in applying the exemption outweighs the public interest in disclosing it. In all cases, before writing to the enquirer, the person given responsibility by the School for dealing with the request will need to ensure that the case has been properly considered and that the reasons for refusal or public interest test refusal, are sound.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Refusal

If it is decided to refuse a request, the School will send a refusals notice, which must contain:

- The fact that the responsible person cannot provide the information asked for;
- Which exemption(s) apply;
- Why the exemption(s) apply to this enquiry (if it is not self-evident);
- Reasons for refusal; and
- The School's complaints procedure.

For monitoring purposes and in case of an appeal against a decision not to release the information or an investigation by the Information Commissioner, the responsible person must keep a record of all enquiries where all or part of the requested information is withheld, and exemptions are claimed. The record must include the reasons for the decision to withhold the information.

The School will get advice from their Data Protection Officer (DPO) prior to withholding data under an exemption or refusing the request in its entirety.

Section 2 – Freedom of Information Publication Scheme

This publication scheme follows a model approved by the Information Commissioners Office.

This scheme is not a list of individual publications but rather a description of the classes of types of information that we are committed to publishing. This list is not an exhaustive list of all of the types of information that we publish. We try to proactively publish as much information as we can where the information would have a wider public interest.

This scheme does not include information that we consider to be sensitive, such as personal information, information prevented from disclosure by law or information about security matters.

Classes of Information

There are six classes of information that we hold:

- Who we are and what we do
- What we spend and how we spend it
- What our priorities are and how we are doing
- How we make decisions
- Our policies and procedures
- The services we offer

Making Information Available

Information will generally be made available on the school website. Where it is not possible to include this information on the school website, the school will indicate how information can be obtained by other means and provide it by those means. This may be detailed in response to a request or within the scheme itself. This will usually be by way of a paper copy.

In some exceptional circumstances, some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where we are legally required to translate any information, we shall do so.

Charges for Information Published Under This Scheme

The school may charge individuals for information published under this scheme. The purpose of this scheme is to make the maximum amount of information readily available at the minimum inconvenience and cost to the public. Charges made by the school for routinely published material will be justified and transparent and kept to a minimum.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Material which is published and accessed on the website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by law.

Charges will be made to cover:

- Photocopying;
- Postage and packaging; and
- The costs directly incurred as a result of viewing information.

Single copies of information requested which are covered by the publication scheme will be provided free unless otherwise stated within the scheme. If the request involved a large amount of photocopying, printing or postage, then this may be at a cost. If this is the case we will let you know as well as let you know the cost before fulfilling your request.

How to Request Information

If you require a paper version of any of the documents within the scheme, please contact the school using the contact details below.

Telephone: 01454 867145

Email: office@christchurchhanham.org.uk

Address: Christ Church Hanham CE Primary School, Memorial Road, Hanham, Bristol, BS15 3LA

Please mark all correspondence *Publication Scheme Request* in order to help us process your request quickly. If the information you are looking for isn't available via the scheme, you can still contact the school to ask if we have this information.

The Publication Scheme

Who We Are and What We Do	Description
Information relating to the Governing Body	Information contained in official governing body documents including the governor's annual report:- • Who is who • Basis of governors appointment • The manner in which the governing body is constituted • Category of the school • A statement on progress in implementing the action plan drawn up following an inspection • Agreed minutes from governors board and committee meetings • A financial statement – including gifts made to the school and amounts paid to the governors for expenses • Information about the implementation of the governing body's policy on pupils with special educational needs and any changes to the policy during the last year • A description of arrangements for the admission of pupils with disabilities, including details of the steps to prevent disabled students being treated less favourably than other pupils, details of existing facilities to assist access to the school by pupils with disabilities, the accessibility plan covering future policies for increasing access by those with disabilities to the school • A statement of policy on whole staff development identifying how teacher's professional development impacts on teaching and learning.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

	• Number of pupils on roll and rates of pupils authorised and unauthorised absence • National curriculum assessment results for appropriate key stages with national summary figures • Instruments of government, including the date it takes effect • The term of office of each category of governor if it lasts less than 4 years and the name of anybody entitled to appoint any category of governor.
School prospectus	• The name, address, website and telephone number of the school and the type of school • The name of the school Headteacher • The school's staffing structure • Information about the schools policy on providing for pupils with special educational needs • Statement on the schools aims and values • Information on the school policy on admissions • School term dates, times and attendance • Uniform • Number of pupils on roll and rates of student absence

What We Spend and How We Spend It	Description
Financial statement for the current and previous financial year	Relating to projected and actual income and expenditure, procurement, contracts and financial audit. Includes budget plans, financial statements and financial audit reports.
Details of expenditure	Sets out details of items of expenditure over £5,000 including the cost, name of supplier and information about the transaction.
Procurement and contracts	Details of the procurement and contracts the school has entered into or details relating to the organisation who has carried out this process on the schools behalf (for example the local authority).
Pay policy	A copy of the pay policy that the school uses to govern staff pay.
Allowances	Details of allowances and expenses that can be incurred by staff and governors.
Pupil Premium	How the school uses pupil premium.
Utilities and school running expenditure	Details of the schools overheads and running costs.

What Our Priorities Are and How We Are Doing	Description
Ofsted report	A published report of the outcome of our latest Ofsted inspection.
Performance management Policy	Statement of procedures adopted by the governing body relating to the performance management of staff and the annual report of the Headteacher on the effectiveness of appraisal procedures.
Charging and remissions policies	A statement of the school's policy with respect to charges and remissions for any optional extra or board and lodging for which charges are permitted, for example school publication, music tuition, trips.
Health and Safety Policy and Risk Assessment	Statement of general policy with respect to health and safety at work of employees (and others) and the organisation and arrangements for carrying out the policy.
Staff Conduct, Discipline and Grievance	Statement of procedure for regulating conduct and discipline of school staff and procedures by which staff may seek redress for grievance.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

How We Make Decisions	Description
Admissions Policy/ Decisions (not individual)	This does not include individual decisions. This is a statement of our policy with regards to admissions and how we make decisions regarding admissions.

Our policies and procedures	Description
Home-School Agreement	Written statements of the schools aims and values, the schools responsibilities, the parental responsibilities the schools expectations of its pupils for example homework arrangements.
Curriculum Policy	Statement on following the national curriculum subjects, including any syllabus used by the school.
Complaints Policy	Statement of procedures for dealing with complaints.
Equality and Diversity Policy	Statement on ensuring that the school follows and promotes equality and diversity.
Child protection and safeguarding policy	Statement of policy for safeguarding and promoting welfare of pupils at the school.
Relationships and Sex Education Policy	Statement of policy with regard to sex and relationship education.
Inclusion Policy	Information about the school's policy on providing for pupils with special educational needs.
Behaviour Policy	Statement of general principles on behaviour and discipline and of measures taken by the Headteacher to prevent bullying.
Collective Worship	Statement of arrangements for the required daily act of collective worship.

Lists and Registers	Description
Curriculum Circulars and Statutory instruments	Any statutory instruments, departmental circulars and administrative memoranda sent by the Department of Education to the Headteacher or governing body relating to the curriculum.
Asset Register	A record of major physical assets owned by the school (e.g., computers, furniture, equipment). This is available on request.
Disclosure Log (FOI Requests) (Appendix 1)	A summary of FOI requests received and how the school responded. Includes date, topic of request and summary of response.
Any information you are currently legally required to hold in publicly available registers	Including staffing structure (names/roles of senior leadership) and governors.

Internal Review

The requester has the right to ask for an internal review if they are dissatisfied with the handling of a request.

Internal review requests should be made within 40 working days of the initial response. This deadline should be communicated to the requester in that response. We are not obliged to provide a review if it is requested after more than 40 working days.

Requests for internal review must make clear why they are dissatisfied with the original decision, detailing why they feel that the School has not complied with Freedom of Information Law.

Complaints and/or Appeals

Any written (including email) expression of dissatisfaction should be handled through the School's existing complaints procedure. Wherever practicable the review should be handled by someone not involved in the original decision.

The Governing Body should set and publish a target time for determining complaints and information on the success rate in meeting the target. The school should maintain records of all complaints and their outcome.



Christ Church Hanham CE Primary School

Nurture with love - **Grow** through knowledge and wisdom - **Flourish** in hope

If the outcome is that the School's original decision or action is upheld, then the applicant can appeal to the Information Commissioner.

The appeal can be made via their website or in writing to:

Customer Contact
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Appendix 1: FOI Disclosure Log

Request number/ID	Date of Request	Summary of Request	Date of Response	Summary of Response	Exemptions Applied (if any)	Link to information (if applicable)
<i>Example: FOI2025/01</i>	<i>01/01/2025</i>	<i>Number of exclusions in 2023/24 by year group</i>	<i>20/01/2025</i>	<i>Provided figures broken down by year</i>	<i>None</i>	<i>N/A</i>



Home Working Policy

Scope and Definitions

This policy applies to all staff who work from home and/or use or access School systems or information from home or while working remotely. This includes individuals who are given access to the School networks and School data (including governors, students, visitors, volunteers, contractors and third parties). It applies to information in all formats, including paper records and electronic data.

Remote working means working off the School site. This includes working while connected to the School's networks. A mobile device is defined as a portable device which can be used to store or process information. Examples include but are not limited to laptops, tablets, USB sticks, removable disc drives and smartphones.

This policy does not envisage home, or remote, working from outside the UK, as this would involve significant legal and practical issues, affecting both you and the School. If you wish to work from a location outside of the UK, you must obtain prior permission from the Headteacher.

Homeworking may be requested by staff working in office based roles with the exception of teachers, teaching assistants and premises staff, as these roles can only be undertaken in the workplace.

This policy does not form part of any contract of employment and the School may amend it at any time.

Awareness of Risk

Working from home presents both significant risks and benefits.

Staff may have remote access to information held on secure School servers but without the physical protections available in School. Without the network protections provided by firewalls and access controls, there are much greater risks of unauthorised access to data as well as a risk of loss or destruction of data. There are also greater risks posed by information "in transit" (i.e., moving data between office and home).

The risks posed by working from home can be summarised under three headings:

- **Reputational**: the loss of trust or damage to the School's relationship with its community;
- **Personal**: unauthorised loss of or access to data could expose staff or students to identity theft, fraud or significant distress; and
- **Monetary**: regulators such as the ICO can impose financial penalties and those damaged as a consequence of a data breach may seek redress through the courts.

Roles and Responsibilities

The decision as to whether to allow partial or full-time homeworking in relation to any given role rests with management. Any member of staff working from home is responsible for ensuring that they work securely and protect both information and School-owned equipment from loss, damage or unauthorised access.

Managers are responsible for supporting staff adherence with this policy. Additional measures may be put in place by management to ensure the rules contained within this policy are adhered to (for example, monitoring or supervision). Failure to comply with this policy may result in disciplinary action.

Key Principles of Homeworking

Staff working from home must ensure that they work in a secure and authorised manner. This can be done by complying with the principles below: -

- To adhere to the principles of the Data Protection Act 2018 and the School's Data Protection Policy in the same way as they would if they were working in School.
- Access to personal data must be controlled. This can be done through physical controls, such as locking the home office for physical data and locking the computer by using strong passwords (a mixture of letters, numbers and special characters).



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- iii. No other members of the household should know or be able to guess your password(s). If passwords are written down (which should be a last case scenario) they must be stored securely (e.g., in a locked drawer or in a secure password protected database). Passwords should never be left on display for others to see.
- iv. Automatic locks should be installed on IT equipment used to process School information that will activate after a period of inactivity (i.e., computers should automatically lock requiring you to sign back in after this period of time).
- v. IT equipment used to process and store School information in the home must be kept in a secure place where it cannot be easily accessed or stolen.
- vi. Portable mobile devices used to process and store School information should be encrypted where possible (or at least password/pin code protected) and should never be left unattended in a public place.
- vii. IT equipment in the home used to process School information should not be used where it can be overseen by unauthorised persons.
- viii. It is the responsibility of each member of staff to ensure that they are working in a safe environment at home. No health and safety risks must be taken when using this equipment.
- ix. Access to certain systems and services by those working from home or remotely may be deliberately restricted or may require additional authentication methods (such as two factor authentication which requires an additional device to verify individuals). Any attempt to bypass these restrictions may lead to disciplinary action.
- x. All personal information and in particular sensitive personal information should be encrypted/password protected before being sent by email where possible. Extra care must be taken when sending emails where auto-complete features are enabled (as this can lead to sending emails to similar/incorrect email addresses). The rules relating the sending of emails are outlined in the School's Acceptable Use Agreement.
- xi. Staff should always use school email addresses when contacting colleagues or students. If telephoning a child or parent at their home, staff should ensure that their caller ID is blocked.
- xii. Any technical problems (including but not limited to, hardware failures and software errors) which may occur on the systems must be reported to the School Business Manager immediately.
- xiii. To adhere to the School's Data Retention Policy and ensure that information held remotely is managed according to the data retention schedule. Data should be securely deleted and destroyed once it is no longer needed.
- xiv. If communicating remotely via video conferencing and social media, staff must adhere to using only those platforms which have been approved by the School and follow the School's guidance on the safe use of video conferencing.
- xv. To be vigilant to phishing emails and unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft.
- xvi. Staff should not access inappropriate websites on School devices or whilst accessing School networks.
- xvii. Staff who have been provided with School-owned IT equipment to work from home must:
 - a. only use the equipment for legitimate work purposes;
 - b. only install software on the equipment if authorised by the School's IT support. Please note that this includes screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins;
 - c. ensure that the equipment is well cared for and secure;
 - d. not allow non-staff members (including family, flatmates and friends) to use the equipment or to share log in passwords or access credentials with them;
 - e. not attempt to plug in memory sticks into the equipment unless encrypted and supplied by the School);
 - f. not collect or distribute illegal material via the internet;
 - g. ensure anti-virus software is regularly updated; and
 - h. to return the equipment securely at the end of the remote working arrangement.
- xviii. Staff who process School data on their own equipment are responsible for the security of the data and the devices generally and must follow the School's Bring Your Own Device Policy and Acceptable Use Policy. In particular:
 - a. Where possible, devices must be encrypted;



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- b. An appropriate passcode/password must be set for all accounts which give access to the device. Passwords must be of a complex nature (a mix of letters, numbers and special characters) and must not be shared with others;
 - c. The device must be configured to automatically lock after a period of inactivity (no more than 15 minutes);
 - d. Devices must remain up to date with security software (such as anti-virus software);
 - e. The theft or loss of a device must be reported to IT services just in the same way as if a School-owned device were lost;
 - f. Any use of privately-owned devices by others (family or friends) must be controlled in such a way as to ensure that they do not have access to School information. This will include school emails, learning platforms and administrative systems such as SIMS;
 - g. Devices must not be left unattended where there is a significant risk to theft;
 - h. The amount of personal data stored on the device should be restricted and the storing of any sensitive data avoided;
 - i. Using open (unsecured) wireless networks should be avoided. Consider configuring your device not to connect automatically to unknown networks;
 - j. If the device needs to be repaired, ensure that the company used is subject to a contractual agreement which guarantees the secure handling of any data stored on the device;
 - k. Appropriate security must be obtained for all School information stored on the device (including back up arrangements) and there must be secure storage for any confidential information;
 - l. Care must be taken with file storage. Any school related work should be stored on the School network area. No school data should be stored on a home computer or on an un-encrypted storage device (such as USB stick);
 - m. The School may require access to a privately owned device when investigating policy breaches (for example, to investigate cyber bullying);
 - n. All data must be removed from privately-owned devices when it is no longer needed or at the request of the School; and
 - o. Devices must be disposed of securely when no longer required.
- xix. Staff are responsible for ensuring the security of School property and all information, files, documents, data etc within their possession, including both paper and electronic material. In particular, physical data (i.e., paper documents, which includes documents printed at home) must be secured and staff must ensure that:
- a. Paper documents are not removed from the School without the prior permission of either the Headteacher or the School Business Manager. When such permission is given, reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. In particular the information is not to be transported in see-through bags or other un-secured storage containers;
 - b. Paper documents should not be used in public places and not left unattended in any place where it is at risk (e.g., in car boots, in a luggage rack on public transport);
 - c. Paper documents taken home or printed at home containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed;
 - d. Paper documents are collected from printers as soon as they are produced and not left where they can be casually read;
 - e. The master copy of the data is not to be removed from School premises;
 - f. Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets in the home just as they would be in School;
 - g. Documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them; and
 - h. Paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.
- xx. Any staff member provided with School devices must not do, cause or permit any act or omission which will avoid coverage under the School's insurance policy. If in any doubt as to whether particular acts or omissions will have this effect, the staff member should consult their line manager immediately.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- xxi. All staff must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any School-owned IT equipment or data immediately to the School Business Manager in order that appropriate steps may be taken quickly to protect School data. Failure to do so immediately may seriously compromise School security. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Appendix A – Homeworking Guidance Handout for Staff

Disclaimer:

- Staff are expected to use School owned and privately owned devices in an ethical manner at all times and adhere to the School's policy as outlined above.
- The School reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.
- The School reserves the right to disconnect devices or disable services or access to services without notification.

I confirm that I have read, understood and will comply with the terms of this Home Working Policy.

Signed.....
Date.....
Print Name.....



Information and Communications Policy

Introduction

The School's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service. However, it also brings with it certain risks, some of which may involve potential legal and financial liabilities for both us and you, e.g:

- inadvertently entering into contracts or commitments on behalf of us;
- introducing viruses into our systems;
- breaching copyright or licensing rights;
- breaching data protection rights;
- breaching confidentiality and security;
- defamation; and/or
- bullying, harassment and discriminatory conduct.

This policy aims to guard against those risks. It is therefore important that all staff read the policy carefully and ensure that they use the internet, email and other communication systems in accordance with it. If you are unsure whether something you are about to do complies with this policy, you should seek advice from your line manager.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the School who are required to familiarise themselves and comply with its contents. The School reserves the right to amend its content at any time.

This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards. We expect our computer and communications systems and equipment to be used in an effective and professional manner and encourage all staff to develop the necessary skills to achieve this. These systems and equipment are provided by us for the purpose of our business, and to assist staff in carrying out their duties effectively.

It is the responsibility of all staff to ensure that these systems and equipment are used for proper business purposes and in a manner that does not compromise us or our staff in any way.

All staff should consider how their reputation and that of the School might be affected by how they communicate and conduct themselves online.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data. Therefore, it is regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the School's Data Protection Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the School's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's disciplinary procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the UK GDPR.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Scope of the Policy

This policy applies to all staff, including employees, workers, temporary and agency workers, interns, volunteers and apprentices, governors, trustees, consultants and other contractors who have access to our computer and other communications systems. It also applies to personal use of our systems and equipment in any way that reasonably allows others to identify any individual as associated us.

This policy applies to the use (or misuse) of computer equipment, e-mail, internet systems, telephones, iPads (and other mobile device tablets), Smart Phones, laptops, Chromebooks, mobile phones and voicemail but it applies equally to the use of fax machines, copiers, scanners, and the like, both in the workplace and from outside (e.g. via remote access).

Prohibited use and breach of this policy

We consider this policy to be extremely important. Any breach of the policy will be dealt with under our disciplinary policy. In certain circumstances, breach of this policy may be considered gross misconduct and may result in immediate termination of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, we may withdraw an individual's internet and/or email access.

Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

- unauthorised use of the internet;
- creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation;
- creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in our equality, diversity and inclusion policies;
- accessing, transmitting or downloading any confidential information about the School and/or any of our staff and/or current, former or prospective pupils or parents, suppliers, contractors or other such third parties, except where authorised in the proper performance of your duties;
- accessing, transmitting or downloading unauthorised software; and
- viewing, accessing, transmitting or downloading any material in breach of copyright.

Equipment Security and Passwords

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and staff are required to select a password that cannot be easily broken. All passwords should be considered complex.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the School Business Manager as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If given access to the School e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Team and/or School Business Manager may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Logging off prevents another member of staff or a pupil accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of the School Business Manager.

On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. The School reserves the right to require employees to hand over all School data held in computer useable format.

Members of staff who have been issued with a laptop, iPad (or other mobile device tablet), Smart Phone or any other device (i.e., USB stick) must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the device is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g., ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers. If staff take devices off-site they should follow the Home Working Policy.

Systems Use and Data Security

You should not delete, destroy or modify any of the School's existing systems, programs, information or data which could have the effect of harming or exposing to risk of harm the School, its staff, students, or any other party.

You are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the School Business Manager, who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

You must not connect any personal computer, mobile phone, laptop, tablet, USB storage device or other device to our systems or network without express prior permission from the School Business Manager. Any permitted equipment must have up-to-date anti-virus software installed on it and we may inspect such equipment in order to verify this.

All members of staff need to inform the School Business Manager before sharing any data with any third parties so the School can carry out a Data Protection Impact Assessment (DPIA).

Where consent is given, all files and data should always be virus checked before they are downloaded onto the School's systems. If in doubt, the employee should seek advice from the School Business Manager or a member of the Senior Leadership Team.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- Audio and video streaming;
- Instant messaging;
- Chat rooms;
- Social networking sites; and
- Web mail (such as Hotmail or Yahoo).

No device or equipment should be attached to our systems without the prior approval of the School Business Manager or Senior Leadership Team. This includes but is not limited to, any Smart Phone or telephone, iPad, laptop (or other mobile device tablet), USB device, i-pod, digital camera, infra red connection device or any other device.

The School monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as ending in '.exe'). The School Business Manager should be informed immediately if a suspected virus is received. The School reserves the



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The School also reserves the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the School's Systems and guidance under "E-mail etiquette and content" below.

You must inform the School Business Manager immediately if you suspect your computer may have a virus, and you must not use the computer again until informed it is safe to do so.

E-mail Etiquette and Content

E-mail is a vital business tool but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

The School's e-mail facility is intended to promote effective communication within the business on matters relating to the School's business activities and access to the School's e-mail facility is provided for work purposes only.

Staff are strictly prohibited from using the School's email facility for personal emails at any time.

Staff should always consider if e-mail is the appropriate medium for a particular communication. The School encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally as a letter or fax message and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the School's best practice.

Staff must not send messages from another person's email address (unless authorised in the proper performance of their duties), or under an assumed name.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e-mails should be retained on the appropriate file.

Staff should check the recipient(s) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information and amount to a breach of data protection.

All members of staff should remember that e-mails can be the subject of legal action for example, in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the School. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the School in the same way as the contents of letters or faxes.

E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. They may also be disclosed as part of dealing with subject access requests when they arise. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader or themselves, if it found its way into the public domain. The School standard disclaimer should always be used on every e-mail.

Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending or posting messages or material that is offensive, abusive, obscene, discriminatory, racist, sexually suggestive, harassing, derogatory or defamatory messages or which otherwise: -

- May be inconsistent with our equality, diversity inclusion and anti harassment and bullying policies;
- criticise other schools or their staff; or
- state that anyone is incompetent.

This list is not exhaustive.

If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed, bullied or victimized or are offended by material sent to you by a colleague via e-mail, or that you have witnessed, you should inform the Headteacher who will usually seek to resolve the matter informally. You should refer to our Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance. We encourage staff to report such concerns.

If an informal procedure is unsuccessful, you may pursue the matter formally under the School's formal grievance procedure. (Further information is contained in the School's Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.)

General Guidance

Staff must not:

- Send any e-mail, including resending and forwarding, containing sexually explicit, suggestive or otherwise offensive material either internally or externally;
- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward private e-mails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the School;
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals.
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail, the internet or by other means of external communication which are known not to be secure;



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service related issues. Urgent or important messages to family and friends are permitted but must be of a serious nature;

The School recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once and not forward it to any internal or external recipient, other than internally to the data protection officer in order to report a breach of this or another policy. If you believe you may have been bullied, harassed, sexually harassed or victimised, we encourage you to report this. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message and delete the email as soon as possible to minimise any further risk to individuals whose data could be breached. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. The School Business Manager should be informed as soon as reasonably practicable.

Emails—monitoring

We may monitor the email and instant messaging systems or network in the workplace for the following reasons:

1. to determine whether they are communications relevant to the carrying on of our relevant activities;
2. if the individual is absent from work, to check communications for business calls to ensure the smooth running of the School;
3. to record transactions;
4. where we suspect that the individual is sending or receiving messages that are:
5. detrimental to us;
6. in breach of the individual's contract, or this policy;
7. in breach of data protection rights;
8. to monitor staff conduct;
9. to investigate complaints, grievances or criminal offences.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

When monitoring incoming or outgoing emails, we will, unless exceptional circumstances apply:

1. look at the sender or recipient of the email and the subject heading only; and
2. avoid opening emails marked 'Private' or 'Personal'.

We do not, as a matter of policy routinely monitor employees' use of the internet or the content of email messages sent or received. However, we have a right to protect the security of its systems or network, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon it.

To achieve these objectives, we carry out random spot checks on the system which may include accessing individual email messages or checking on specific internet sites searched for and/or accessed by individuals.

We will only intercept (i.e. open) outgoing or incoming emails, received emails, sent emails and draft emails where relevant to the carrying on of our business and where necessary:

- to determine whether the message is relevant to the carrying on of our business;
- to establish the existence of facts;
- to check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, i.e. to detect unauthorised use of the system;
- to check whether staff using the system in the course of their duties are achieving the standards required of them;
- for the purpose of investigating or detecting the unauthorised use of the system;
- for the purpose of preventing or detecting crime; or
- for the effective operation of the telecommunication system.

The content of emails will be examined only in exceptional circumstances, initially by the School Business Manager. The information obtained through monitoring may be shared internally, if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way where the School believes there may have been a breach of the individual's contract or this Policy.

Use of the Internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the School, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if for example, the material is pornographic in nature.

Staff must not access any web page or any files from the School's system (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use School systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

The School's website may be found at <https://www.christchurchhanhamprimaryschool.co.uk>. This website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. Such input should be submitted to the Senior Leadership Team in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

The School should refrain from texting and using systems such as WhatsApp for School related matters using personal phones. The School require staff to use alternative systems to make contact with staff (such as emails).

Internet—monitoring

We may monitor internet usage (including searches made, the IP addresses of sites visited, and the duration and frequency of visits) if we suspect that the individual has been using the internet in breach of the individual's contract or this policy, e.g.:

- by viewing material that is pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us;
- by spending an excessive amount of time viewing websites that are not work-related.

Monitoring may include internet usage at the workplace, internet usage outside the workplace during working hours using our systems or network and internet usage using hand-held or portable electronic devices.

Monitoring will normally be conducted by our *IT team*. The information obtained through monitoring may be shared internally, if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way where the *IT team* believes there may have been a breach of the individual's contract or this Policy.

Personal Use of School Systems

Staff are strictly prohibited from personal use of the School's systems. Staff should be aware that any personal use of the systems may also be monitored (see below) and where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Excessive or inappropriate personal use of the School's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

The School reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

Inappropriate Use of Equipment and Systems

Occasional personal use is permissible provided it is in full compliance with the School's rules, policies and procedures (including this policy, the Equal Opportunities and Diversity Policy, Anti-Harassment Policy, Data Protection Policy, Code of Conduct and Disciplinary Policy and Procedure).

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- (a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- (b) Transmitting a false and/or defamatory statement about any person or organisation;
- (c) Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;
- (d) Transmitting confidential information about the School and any of its staff, students or associated third parties;
- (e) Transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for the School);
- (f) Downloading or disseminating material in breach of copyright;
- (g) Copying, downloading, storing or running any software without the express prior authorisation of either the Headteacher or School Business Manager;
- (h) Engaging in online chat rooms, instant messaging, social networking sites and online gambling;



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- (i) Forwarding electronic chain letters and other materials;
- (j) Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.



Information Security Policy

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the School to achieve this, including to:-

- To protect against potential breaches of confidentiality;
- To ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- To support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- To increase awareness and understanding at the School of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they handle.

Introduction

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Staff are referred to the School's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data and can be found on the school website or by requesting from the school office.

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to laptops, tablets, digital cameras, memory sticks and smartphones.

Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and to comply with the provisions contained within it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

General Principles

All data stored on our IT Systems are to be classified appropriately (including, but not limited to personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the School's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with School Business Manager the appropriate security arrangements for the type of information they access in the course of their work.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

All data stored within our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired and upgraded by Integra IT or by such third party/parties as the Headteacher and School Business Manager may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including but not limited to the security, integrity and confidentiality of that data) lies with the School Business Manager unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the School Business Manager who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Physical Security and Procedures

Paper records and documents containing personal information, sensitive personal information and confidential information shall be positioned in a way to avoid them being viewed by people passing by as far as possible, e.g. through windows. At the end of the working day or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available locked containers shall be used to store paper records when not in use. If you do not feel you have appropriate and/or sufficient storage available to you, you must inform the School Business Manager as soon as possible.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the School Business Manager as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The following measures are taken by the School to ensure physical security of the building/s and storage systems:

- The School carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.
- The School has an intercom system to minimise the risk of unauthorised people from entering the school premises.
- The School close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.
- Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

Computers and IT

The School Business Manager shall be responsible for the following:

- a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;
- b) ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management and reporting the outcome of such reviews to the School's management;



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations and other relevant rules whether now or in the future in force, including but not limited to the UK GDPR and the Computer Misuse Act 1990.

Furthermore, the School Business Manager shall be responsible for the following:

- a) assisting all members of staff in understanding and complying with this policy;
- b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
- c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities and any special security requirements;
- d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];
- e) taking proactive action, where possible, to establish and implement IT security procedures and to raise awareness among members of staff;
- f) monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Responsibilities – Members of Staff

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure. You must immediately inform [POSITION] of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.

Any other technical problems (including but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the School Business Manager immediately.

You are not permitted to install any software of your own without the approval of the School Business Manager. Any software belonging to you must be approved by the School Business Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

Prior to installation of any software onto the IT Systems, you must obtain written permission by the School Business Manager. This permission must clearly state which software you may install and onto which computer(s) or device(s) it may be installed.

Prior to any usage of physical media (e.g., USB memory sticks or disks of any kind) for transferring files, you must make sure to have the physical media virus scanned. Approval from the School Business Manager must be obtained prior to transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to the School Business Manager (this rule shall apply even where the anti-virus software automatically fixes the problem).

Access Security

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teach individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods can only be used if approved by the IT Department.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the School Business Manager as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password you should notify the school office to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary, you may write down passwords provided that you store them securely (e.g., in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g., mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this time period or disable the lock.

All mobile devices provided by the School shall be set to lock, sleep or similar after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Data Security

Personal data sent over the School network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from [POSITION] who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given, all files and data should always be virus checked before they are downloaded onto the School's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided that you follow the [POSITION] requirements and instructions governing this use. All usage of your own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy). The School Business Manager may at any time request the immediate disconnection of any such devices without notice.

Electronic Storage of Data

All portable data and in particular personal data should be stored on encrypted drives using methods recommended by the appointed IT provider.

All data stored electronically on physical media and in particular personal data, should be stored securely in a locked box, drawer, cabinet or similar.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

You should not store any personal data on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the Headteacher. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the School's computer network in order for it to be backed up.

All electronic data must be securely backed up by the end of the each working day and is done by our appointed IT provider.

Homeworking

You should not take confidential or other information home without prior permission of the Headteacher and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

- a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- b) all confidential material that requires disposal is shredded or in the case of electronical material, securely destroyed as soon as any need for its retention has passed.

Communications, Transfers, Internet and Email Use

When using the School's IT Systems, you are subject to and must comply with the School's Electronic Information and Communication Systems Policy.

There are restrictions on international transfers of personal data and transfers to international organisations. Staff may only transfer personal data outside the UK or to any international organisation, with the prior written authorisation of the DPO. You should refer to the Schools Data Protection policy for further information on international transfers.

The School work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the School Business Manager.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the School cannot accept liability for the material accessed or its consequence.

All personal information and in particular sensitive personal information and confidential information should be encrypted before being sent by email or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine. Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

Personal or confidential information should not be removed from the School without prior permission from the Headteacher or the School Business Manager except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

- a) not transported in see-through or other un-secured bags or cases;
- b) not read in public places (e.g., waiting rooms, cafes, trains, etc.); and



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

c) not left unattended or in any place where it is at risk (e.g., in car boots, cafes, etc.)

Reporting Security Breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the School Business Manager. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the School Business Manager shall immediately assess the issue, including but not limited to, the level of risk associated with the issue and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the School Business Manager. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of and with the express permission of the School Business Manager.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the School Business Manager.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Data Breach Policy.



Social Media Policy

Introduction

This policy applies to all School staff regardless of their employment status. It is to be read in conjunction with the School's Electronic Communications Policy. This policy does not form part of the terms and conditions of employee's employment with the School and is not intended to have contractual effect. However, it does set out the School's current practices and required standards of conduct and all staff are required to comply with its contents. Breach of the provisions of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal in accordance with the School's Disciplinary Policy and Procedure.

This Policy may be amended from time to time and staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

In this policy, 'social media' means internet-based applications which allow users to collaborate or interact socially by creating and exchanging content, such as social networks or platforms, community sites, blogs, microblogging sites, wikis, web forums, social bookmarking services and user rating services.

Purpose of This Policy

The School recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media such as Facebook, Twitter, LinkedIn, blogs, Instagram, TikTok, WhatsApp and Wikipedia. However, staff use of social media can pose risks to the School's confidential and proprietary information, its reputation and it can jeopardise our compliance with our legal obligations. To minimise these risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate work-related purposes, all School staff are required to comply with the provisions in this policy.

Social media platforms allow us to build connections and to share ideas and content more broadly and quickly, and the School supports their use. However, improper use of social media may give rise to a breach of your contract and/or the school's policies, and/or the following:

- Bullying, harassment and unlawful discrimination;
- Defamation (i.e., damaging the good reputation of another person or organisation);
- Contempt of court (i.e., interfering with the administration of justice e.g., by revealing someone's identity that had been protected by the courts);
- Breach of data protection laws;
- Misuse of confidential information belonging to the school or to its students/staff/parents/suppliers; and
- Damage to reputation of the user or school or to its students/staff/parents/suppliers.

Who is Covered by This Policy?

This policy covers all individuals working at all levels and grades within the School, including senior managers, officers, governors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as *Staff* in this policy).

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

Scope and Purpose of This Policy

This policy deals with the use of all forms of social media including Facebook, LinkedIn, Twitter, Wikipedia, Instagram, TikTok, WhatsApp and all other social networking sites and all other internet postings including blogs.

It applies to the use of social media for both work and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Breach of this policy may result in disciplinary action up to and including dismissal.

Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether the School's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Personnel Responsible for Implementing This Policy

The Board of Governors have overall responsibility for the effective operation of this policy but have delegated day-to-day responsibility for its operation to the Headteacher.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Headteacher in liaison with the IT Manager.

All senior School Staff have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All School Staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Headteacher in the first instance. Questions regarding the content or application of this policy should be directed by email to the School Business Manager.

Compliance with Related Policies and Agreements

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- Breach our electronic information and communications systems policy;
- Breach our obligations with respect to the rules of relevant regulatory bodies;
- Breach any obligations they may have relating to confidentiality;
- Breach our Disciplinary Rules;
- Defame or disparage the School, its Staff, its pupils or parents, its affiliates, partners, suppliers, vendors or other stakeholders;
- Harass or bully other Staff in any way or breach our Anti-harassment and bullying policy;
- Unlawfully discriminate against other Staff or third parties or breach our Equal Opportunities policy;
- Breach our Data Protection policy (for example, never disclose personal information about a colleague, student, parent, or any other individual online);
- Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements); and
- Breach our obligations for Keeping Children Safe in Education.

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the School and create legal liability for both the author of the reference and the organisation.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Personal Use of Social Media



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems.

Staff should not use a work email address to sign up to any social media. Staff personal social media pages should not make reference to their employment with the School (excluding LinkedIn, where prior permission is sought from the Headteacher).

Staff must not take photos or posts from social media that belong to the School for their own personal use.

Monitoring

The contents of our IT resources and communications systems are the School's property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message or any other kind of information or communications transmitted to, received or printed from or stored or recorded on our electronic information and communications systems.

The School reserves the right to monitor, intercept and review, without further notice, Staff members activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes. By your acknowledgement of this policy consent to such monitoring of this policy and your use of such resources and systems. This might include without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The School may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

All Staff are advised not to use our IT resources and communications systems for any matter that he or she wishes to be kept private or confidential from the School.

Educational and Extra-Curricular Use of Social Media

If your duties require you to speak on behalf of the School in a social media environment, you must follow the protocol outlined below.

The Headteacher may require you to undergo training before you use social media on behalf of the School and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the School for publication anywhere, including in any social media outlet, you must direct the inquiry to the Headteacher and must not respond without advanced written approval.

As part of this role, you will be required to ensure individuals have given prior consent before posting their personal information. You will also need to monitor the messages/posts coming through. Subject Access Requests (SARs) can be made via social media platforms.

Recruitment

The School may use internet searches to perform pre employment checks on candidates in the course of recruitment. This is after the shortlisting and interview stage in order to make a final decision on where to recruit, including criminal record information, references, information regarding qualifications. Where the School does this, it will act in accordance with its data protection and equal opportunities obligations.

Responsible Use of Social Media

Photographs for use with social media:



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

Any photos for social media posts may only be taken using school cameras/devices or devices that have been approved in advance by the Headteacher. Where any device is used that does not belong to the School, all photos must be deleted immediately from the device, once the photos have been uploaded to a device belonging to the School.

Staff protocol for use of social media:

Where any post is going to be made on the School's own social media the following steps must be taken:

- Ensure that specific permission from the child's parent/carer has been sought before information is used on social media (consents available on Arbor). Note: A parent/carer may have provided permission for one social media platform but not another. Staff should ensure that the appropriate permission is specific.
- Ensure that there is no identifying information relating to a child/children in the post - for example, any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work. The School should seek additional consent to include any names when posting on social media.
- The post must be a positive and relevant post relating to the children, the good work of staff, the School or any achievements.
- Social Media can also be used to issue updates or reminders to parents/guardians. The Headteacher will have overall responsibility for this. Should you wish for any reminders to be issued you should contact the Headteacher by email to ensure that any post can be issued.
- The proposed post must be presented to the Headteacher for confirmation that the post can 'go live' before it is posted on any social media site.
- The Headteacher will post the information but all staff have responsibility to ensure that the Social Media Policy has been adhered to.
- Personal information shared/published on social media will be required to be disclosed under a subject access request.

Protecting our business reputation:

Staff must not post disparaging or defamatory statements about:

- The School;
- Current, past or prospective Staff as defined in this policy
- Current, past or prospective pupils
- Parents, carers or families of (iii)
- The School's suppliers and services providers; and
- Other affiliates and stakeholders.
- Current, past or prospective governors

Staff should also avoid social media communications that might be misconstrued in a way that could damage the School's reputation, even indirectly.

If Staff are using social media they should:

- Make it clear in any social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal rather than School e-mail address when communicating via social media.
- Staff are personally responsible for what they communicate in social media. Staff should be mindful that what they publish might be available to be read by the masses (including the School itself, future employers and social acquaintances) for a long time. Staff should keep this in mind before they post content.
- If Staff disclose directly or indirectly their affiliation to the School as a member of Staff whether past, current or prospective, they must also state that their views do not represent those of the School.
- Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents.
- Staff must avoid posting comments about confidential or sensitive School related topics. Even if Staff make it clear that their views on such topics do not represent those of the School, such comments could still damage the School's reputation and incur potential liability.



Christ Church Hanham CE Primary School

Nurture with love - Grow through knowledge and wisdom - Flourish in hope

- If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they have discussed it with his/her Line Manager or Head of Department.
- If a member of Staff sees content on social media that disparages or reflects poorly on the School including its Staff, pupils, parents, service providers, stakeholders or governors, they are required to report this in the first instance to the Headteacher without unreasonable delay. All staff are responsible for protecting the School's reputation.

Respecting intellectual property and confidential information:

- Staff should not do anything to jeopardise School confidential information and intellectual property through the use of social media.
- In addition, Staff should avoid misappropriating or infringing the intellectual property of other School's, organisations, companies and individuals, which can create liability for the School as well as the individual author.
- Staff must not use the School's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Headteacher.
- To protect yourself and the School against liability for copyright infringement, the Staff member should, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Headteacher in the first instance before making the communication.

Respecting colleagues, pupils, parents, clients, service providers and stakeholders:

- Staff must not post anything that their colleagues (past and/or current), pupils (prospective and/or current), parents, service provider, stakeholders or governors may find offensive, including discriminatory comments, insults or obscenity.
- Staff must not post anything relating to colleagues (past and/or current) or pupils, parents (prospective and/or current) service providers, stakeholders or governors without their advanced written permission.

Monitoring and Review of This Policy

The School Business Manager together with the Headteacher shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice. The Board of Governors has responsibility for approving any amendments prior to implementation.

The Headteacher has responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties. If Staff have any questions about this policy or suggestions for additions that they would like to be considered on review, they may do so by emailing the School Business Manager in the first instance.