Data Protection Policy
Whitings Hill Primary School

Data Protection Policy			
Review Frequency	Every year	**Review Date**	July 2026
Ratified by Governors		**Website**	Yes

Table of Contents

Statement of intent 3
Equal opportunities and inclusion 3
1 Aims 4
2 Scope of the Policy 4
3 Definitions of data protection terms 5
4 Roles and Responsibilities 6
5 Personal Data Protection Principles 7
6 Lawfulness, Fairness and Transparency 9
7 Sharing personal data 10
8 Consent 10
9 Subject access requests and other rights of individuals 11
10 CCTV 12
11 Photographs and videos 13
12 Protection of Biometric information 13
13 Record keeping 14
14 Accountability, data protection by design 14
15 Data security and storage of records 15
16 Filtering and monitoring 19
17 Retention schedule 20
18 Destruction of records 20
19 Disclosure and Barring Service (DBS) data 21
20 Personal data breaches 21
21 Cyber Awareness Plan – Training and Acceptable Use 21
22 Cyber Risk Assessment 22
23 Artificial Intelligence AI 22
24 Whisteblowing for Employees 23
25 Review and Monitoring arrangements 24
Appendix A – Data Breach Procedure 24

Statement of intent

Whitings Hill Primary School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA) 2018

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the core principles of the UK GDPR as outlined in section 5.

Organisational methods for keeping data secure are imperative. Whitings Hill Primary School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the UK GDPR.

Equal opportunities and inclusion

It is the right of all children, staff and visitors to the school, regardless of their gender, ethnicity, religion or beliefs, physical disability, ability, linguistic, cultural or home background, to have their personal information collected, stored and processed in line with the requirements of the current legislation.

Links to UN Rights of the Child:

Article 13

Every child must be free to say what they think and to seek and receive all kinds of information as long as it is within the law.

Article 17

Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

1 Aims

Whitings Hill Primary School uses personal information about staff, pupils, parents/carers/guardians and other individuals who come into contact with the school. This information is gathered, in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The school has a legal responsibility to comply with data protection legislation and other statutory provisions relating to the way in which it holds and processes personal data. The school, as a corporate body, is named as the data controller under the Data Protection Act 2018 (DPA 2018).

ICO Notification and Registration. The school is required to 'notify' the Information Commissioner of the processing of personal data. This information is included in a public register which is available on the Information Commissioner's website. As a Data controller the school will register annually with the ICO as required in line with legislation.

Privacy Notices. Every member of staff, member of the governing board, contractors, and partners of the school that hold its' personal information, has to comply with the law when managing that information. Schools also have a duty to issue a privacy notice to all pupils, parents/carers/guardians, governors and its employees; these provide details of information collection and held, why it is held and the other parties to whom it may be passed on.

Data Controller. As data controller personal data collected about staff, pupils, parents/carers/guardians, governors, visitors and other individuals that is collected and held must be processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the DPA 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act 2018 and the UK GDPR. It will apply to information regardless of the way it is used, recorded, stored and whether it is held in paper files or electronically.

2 Scope of the Policy

We recognise that the correct and lawful treatment of personal data will maintain confidence in the school. Protecting the confidentiality and integrity of Personal Data is a critical responsibility, that we take seriously at all times. Under the UK GDPR, personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The school collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as

the many different types of research data used by the school. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

3 Definitions of data protection terms

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data controllers: are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our organisation for our own operational purposes.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data processors: include any person or organisation that is not a data user who processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our school's behalf.

Data Protection Officer (DPO): is the individual or organisation appointed by the school to be, responsible for monitoring our compliance with data protection law.

Data subject: means a living, identified or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data users: are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Personal data: means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

Processing: is any activity which is performed on personal data such as collection, recording, organisation, structuring, adaptation or alteration, using, storage, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special category personal data: includes information about a person's racial or ethnic origin, political opinions; religious or philosophical beliefs; trade union membership; physical or mental health or condition; genetic/biometric data held for purposes of identification or data about sexual orientation or an individual's sex life.

Artificial intelligence (AI): Using and computer or machine to reason, learn and act in a way that would normally require human intelligence.

Generative AI: This is a part of Artificial Intelligence that uses generative models to produce, text , images, videos, music and other forms of data.

4 Roles and Responsibilities

This policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present pupils, employees, workers, or supplier contacts, website users or any other data subject.

Staff, those working on our behalf and volunteers

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf.

You must read, understand and comply when processing personal data on our behalf and attend training on its requirements. This policy sets out what we expect from you, in order for the school to comply with applicable law. Your compliance with this policy is mandatory. You must also comply with all related policies and guidelines given. Staff who do not comply with this policy may face disciplinary action.

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Ensuring that personal data held is accurate and up to date
- Ensuring that personal data held is not misused, lost or unlawfully disclosed

Data Protection Team

The Data Protection Team is made up of a Data Protection Officer (DPO), the Headteacher and the School Business Manager. The team is responsible for overseeing the implementation of this policy, monitoring the school's compliance with data protection law, and developing related policies and guidelines where applicable.

The DPT will provide an annual report of their activities directly to the Governing Body and, where relevant, will report any advice and recommendations on school data protection issues.

The DPT is also the first point of contact for individuals whose data the school processes, and for the ICO.

The Data Protection Team can be contacted at: office@whitingshill.barnetmail.net

The DPO is David Powell who can be contacted at: dpo@sapphireskies.co.uk

All staff must contact the Data Protection Team in the following circumstances:

- Where they are unsure or have questions about the operation of this policy; the purposes for which data may be used; retaining personal data; disclosing personal data or keeping personal data secure
- If there has been a data breach or a suspected data breach
- Where they are unsure if they have a lawful basis for processing personal data or wish to process for a different purpose than the one that the data was obtained
- Where they propose to engage in any activity that affects the rights of privacy of any individual i.e. where there is a legal obligation to carry out a DPIA
- Where they are unsure about what security, or other measures they need to implement to protect personal data
- If they are engaging in an activity that may affect the privacy rights of individuals
- If they need any assistance dealing with any rights invoked by a data subject
- Where they are considering sharing personal data with third parties
- Where they are entering into contracts involving the processing of personal data by another organisation
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual
- If they need to transfer personal data outside the European Economic Area

Where staff have concerns that this policy is not being followed by others, they should report this immediately to the DPO. Where they wish to raise this formally, they may do so under the school's whistleblowing policy for staff.

Governing Board

The governing board has overall responsibility for ensuring compliance with all relevant data protection obligations. All policies and documents related to data protection are reviewed annually by the FGB committee

Headteacher

The headteacher has overall operational responsibility on a day-to-day basis for the implementation of the school's policies and procedures.

Data Protection Officer

The DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also a point of contact for individuals whose data the school processes who wish to raise any complaint regarding the school's processing where they remain dissatisfied with the school's response, and for the Information Commissioner's Office (ICO).

5 Personal Data Protection Principles

Whitings Hill Primary School adheres to the principles relating to processing of personal data set out in the UK GDPR which require personal data to be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Whitings Hill Primary School is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability). Making available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).

The school is committed to maintaining the data protection principles at all times. This means that the school will:

- Inform data subjects, via privacy notices about the processing of their personal data. Who is it collected by, how is it being used and Who is it shared with
- Check the quality and accuracy of the information held
- Apply the records management policies and procedures to ensure that information is not held longer than is necessary
- Ensure that when information is authorised for disposal it is done appropriately
- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- Only share personal information with others when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as subject access request

- Train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures

6 Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. The school may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

The UK GDPR allows processing for specific purposes, some of which are set out below:

a) The data subject has given his or her consent
b) The processing is necessary for the performance of a contract with the data subject
c) To meet our legal compliance obligations
d) To protect the data subject's vital interests
e) The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions - this is known as the public task
f) To pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and DPA 2018.

If our school offers online services to pupils, such as classroom apps, and we intend to rely on public task, legal obligation and or consent as a basis for processing. we will obtain parental consent as necessary (except for online counselling and preventive services).

The purposes for which we process Personal Data to perform our public task, are set out in the privacy notice issued by the school.

When we collect personal data directly from data subjects, including for human resources or employment purposes, we provide the data subject with all the information required by the UK GDPR, including the identity of the Data Controller and DPO, how and why we will use, process, disclose, protect and retain that personal data through a fair processing (privacy) notice.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's guidance.

7 Sharing personal data

- The school will not normally share personal data with anyone else without express consent, but may do so where:
- It is necessary for the performance of our public task
- There is an issue with a pupil or parent/carer/guardian that puts the safety of another individual at risk
- For safeguarding purposes

The ICO has provided guidance regarding sharing information for safeguarding purposes. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/#:~:text=The%20ICO's%20role%20is%20as,prevent%20you%20from%20doing%20this.

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we:

(i) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
(ii) Establish either in the contract or as a standalone agreement, a data processing agreement to ensure the fair and lawful processing of any personal data we share
(iii) Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

The school will also share personal data with law enforcement and government bodies where we are legally required to do so, including for the following purposes:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff and for safeguarding purposes.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

The school may enter into information-specific sharing agreements with other public bodies for the purposes outlined above.

8 Consent

Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 13, the consent of parents/carers/guardians will be sought prior to the processing of special categories of their data, except for safeguarding to prevent harm and where the processing is related to preventative or counselling services offered directly to a child.

When gaining pupil consent, consideration will be given to the age, maturity and mental capacity of the pupil in question. Consent will only be gained from pupils where it is deemed that the pupil has a sound understanding of what they are consenting to.

9 Subject access requests and other rights of individuals

Our data subjects have rights when it comes to how we handle their personal data. These include rights to:

- withdraw consent to processing at any time;
- receive certain information about how we process their data;
- request access to their personal data that we hold;
- prevent 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;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which personal data is transferred outside of the EEA;
- object to decisions based solely on automated processing, including profiling (known as automated decision making ('ADM'));
- prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms; and
- make a complaint to the Information Commissioner.

How to make a subject access request

The UK GDPR does not specify how to make a valid request.

You can make a subject access request verbally or in writing to any part of the school and not a specific contact point. We suggest however that you email the school if possible: office@whitingshill.barnetmail.net

We have one month to respond to your request.

UK GDPR requests for personal data are free in most cases unless the request is manifestly unfounded or excessive, when a "reasonable fee" for the administrative costs of complying with the request may be charged.

A reasonable fee will be charged based on administrative costs if an individual requests further copies of their data following a request.

When responding to requests, the school may ask the individual to provide 2 forms of identification and contact the individual to confirm that they made a request.

We may inform the requester that the school will comply within 3 months of receipt of the request, where a request is complex or numerous requests have been made, informing the requester of this within 1 month, and explaining why the extension is necessary.

The school will not disclose information if by doing so it:

- might cause serious harm to the physical or mental health of the pupil or another individual
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- is contained in adoption or parental order records
- is given to a court in proceedings concerning the child
- is subject to relevant statutory exemptions.

When the school refuses a request, the individual will be advised of the reason and that they have the right to complain to the ICO.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents/carers/guardians of pupils at the school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Parents, or those with parental responsibility, have a legal right to access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

10 CCTV

Whitings Hill Primary school uses CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

The CCTV system that we use stores data for **one month**. Subject access requests apply to CCTV, and can be made by following procedures in the previous section. CCTV will only be provided to third parties such as the police, for investigative purposes, if there is a lawful reason to do so.

Any enquiries about the CCTV system should be directed to the senior leadership team.

Covert surveillance will only be possible in extreme circumstances.

11 Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

The school will obtain annual written consent from parents/carers/guardians for the general use categories of photos and videos.

The school will obtain written consent from parents/carers/guardians for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer/guardian and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Marketing and promotional materials uses may include:

- Within school on notice boards and in school magazines, brochures, prospectuses newsletters, etc.
- Children's books to evidence their learning
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

When using photographs and videos in this way the school will not include any other personal information about the child, to ensure they cannot be identified, unless parent/carer/guardian consent is provided, and safeguarding is not compromised.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

12 Protection of Biometric information

Legal Framework:

Protection of Freedoms Act 2012, Data Protection Act 2018, UK GDPR and DfE guidance 'Protection of biometric information of children in schools and colleges'

At Whitings Hill Primary School, the written consent of at least one parent/carer/guardian must be obtained before the biometric data is taken from the child and used. This applies to all pupils in schools and colleges under the age of 18.

In no circumstances can a child's biometric data be processed without written consent.

We will not process the biometric data of a pupil (under 18 years of age) where:

a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
b) no parent/carer/guardian has consented in writing to the processing; or
c) a parent/carer/guardian has objected in writing to such processing, even if another parent/carer/guardian has given written consent.

We will where possible provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

We refer to the latest guidance published by the DfE for the implementation of policy https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

13 Record keeping

UK GDPR requires us to keep full and accurate records of all our data processing activities.

We keep and maintain accurate records reflecting our processing. These records include clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

14 Accountability, data protection by design

The school put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

15 Data security and storage of records

The UK GDPR General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, has a rationale to protect the rights and freedoms of individuals. Organisations including schools and colleges, are required to take security measures to mitigate the risks of destruction that is unauthorised, disclosure that is unauthorised, access that is unauthorised and any alteration that is unauthorised. The school will ensure staff are aware of risks and how to minimise them. The school will therefore have in place procedures to minimise the risk of attacks. **Please see Data Security Policy**

The DfE has produced 'Cyber security standards for schools and colleges'. The school will follow these standards where possible.

Summary:

- Protect all devices on every network with a properly configured boundary or software firewall
- Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date
- Accounts should only have the access they require to perform their role and should be authenticated to access data and services
- You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication
- You should use anti-malware software to protect all devices in the network, including cloud-based networks
- An administrator should check the security of all applications downloaded onto a network
- All online devices and software must be licensed for use and should be patched with the latest security updates
- You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site
- Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack
- Serious cyber-attacks should be reported
- You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation
- The safe necessary implementation and use of AI
- Train all staff with access to school IT networks in the basics of cyber security

The governing board will be responsible for:

- Ensuring the school has appropriate cyber-security measures in place.
- Ensuring the school meets where possible, DfE standards for cyber security
- Ensuring cyber security protocols are in place that are suitable for the setting.
- Ensuring there is a data breach procedure in place.
- Understanding the data that is available to governors
- Understanding that personal emails cannot be used regarding confidential matters
- The safe and necessary implantation use and oversight of AI
- Understanding that personal or confidential data cannot be taken off site unless there is authority and or authorisation to do so.

The headteacher/school business manager will be responsible for:

- Ensuring all staff, students, and governors and any other relevant parties are aware of their cyber security responsibilities.
- Ensuring a cyber recovery plan is in place
- Ensuring access protocols are followed.

Arranging staff training and update training – Cyber Awareness Plan

- Arranging staff training and update training – Cyber Awareness Plan
- Ensuring that alerts and monitoring are acted on relating to cyber security
- Ensuring staff receive regular training
- Ensuring a response to inappropriate online material
- The safe and necessary implantation use and oversight of AI
- Ensuring online safety within the setting, including training and policy

The DPO will be responsible for:

- The management of data security.
- Assessing the risks to the school in the event of a cyber-security breach.
- Responding to data breaches and liaising with relevant agencies, IT providers and notifying relevant organisations and data subjects.
- Arranging staff training and update training – Cyber Awareness Plan
- Monitoring and reviewing the effectiveness of this policy, alongside the headteacher, and communicating any changes to staff members.
- Strategies that mitigate risk whilst managing a data breach and strategies that mitigate risk
- To improve cyber security after a data breach with relevant agencies, IT provider, DPO and ICO recommendations.
- The safe and necessary implantation use and oversight of AI
- Monitoring this policy

The ICT provider will be responsible for:

- Maintaining records and or an inventory on Software and hardware
- Ensure data is logged for a long enough period to help investigate and determine the source of a cyber-attack and identity and vulnerabilities and causation factors.
- Ensuring effective monitored firewalls are in place
- Ensuring appropriate user privileges are in place as agreed with SLT
- Removal from the school ICT. Former staff, students, and other relevant parties
- Updating software and removing out of date software
- Ensuring appropriate data security software is installed on devices that are not owned by the school and used for school purposes. This includes installing software as appropriate.
- Ensuring regular backups are undertaken including offline where possible.
- Ensuring updated malware protection
- Updating software and removing out of date software
- Enabling multi-factor authentication where possible
- Up to date password and username inventory.
- Ensuring effective filtering is in place
- Informing the SLT of any inappropriate content or other alerts
- The safe and necessary implantation use and oversight of AI

The DSL will be responsible for:

- Safeguarding within cyber security
- Filtering and Monitoring
- The safe and necessary implantation use and oversight of AI

All staff members will be responsible for:

- Understanding their responsibilities
- Completing training and update training
- The safe and necessary implantation use and oversight of AI

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage and consider:

Network security - The ICT company and or technician will ensure that network security is effectively operating and updating.

Offline backup – The ICT company will provide an offline backup where possible, as recommended by the National Cyber Security Centre

Software updates (patch management) – The ICT company and or technician will ensure effective patch management, to minimise vulnerabilities.

Malware protection – Antivirus and anti-malware software will be installed to prevent, malware, which is intentionally designed to cause damage to a computer, server, client, or computer network.

Access control – Access to systems will be minimised and be based on the need and requirement of users.

Firewalls – A firewall that monitors and controls incoming and outgoing network traffic, based on predetermined security rules. Will be installed at all times to establish a barrier between the school's trusted network and the internet (untrusted network).

Secure configuration - Secure configuration will be adopted when installing computers and network devices, to reduce the risk of cyber threats.

Data Protection Impact Assessments - DPIA's will be undertaken to systematically analyse, identify and minimise the data protection risks of a project or plan

Web filtering - Web filtering will be employed at all times (content control software)

Staff training - Cyber security including, phishing attacks, ransomware and awareness of further training, from the National Cyber Security Centre.

Devices owned by staff – Staff should ensure that reputable anti-virus software is installed on their personal devices and approved by the IT provider. Personal devices include mobile phones, tablets and computers. Staff should use secure apps linked to the device to access email etc. where possible.

Practical measures include and are not limited to:

- Passwords that are at least 8 characters long where possible containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Passwords must be kept confidential and must not be made disclosed to another person on IT system without the permission of the SLT
- Forgotten passwords should be reported to the ICT lead or person/company responsible for IT as appropriate. On restoration passwords should be changed.
- Passwords should be remembered and only written down if they can be stored securely and out of context.
- Passwords should not be left in the view of others or cctv image capture technology.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy/ICT policy/acceptable use agreement/policy on acceptable use])
- Where the school needs to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and is adequately protected
- Confidential paper records will be kept in a locked filing cabinet, locked cupboard, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted: teaching staff are provided with encrypted memory stick by the school.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff will not use their personal laptops or computers for school purposes if it involves the identifiable data of pupils, staff member or any other stake holder.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data.
- They will check if unsure.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Whitings Hill Primary School takes its duties under the UK GDPR seriously, and any unauthorised disclosure may result in disciplinary action.

The school business manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Storage of records

Whitings Hill Primary School has a responsibility to maintain its records and record keeping systems. When doing this, 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
- Their accessibility.

16 Filtering and monitoring

Keeping Children Safe in Education
Role of the safeguarding lead
The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)

Governing board/proprietor responsibilities

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age

range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

Filtering appropriateness

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

• identify and assign roles and responsibilities to manage filtering and monitoring

systems.

• review filtering and monitoring provision at least annually.

• block harmful and inappropriate content without unreasonably impacting teaching

and learning.

• have effective monitoring strategies in place that meet their safeguarding needs

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

Please see data security policy for further information.

17 Retention schedule

The retention schedule broadly follows the guidelines from the Annual Review of School Records and Safe Data Destruction IMRS (Information and Management Records Society) checklist approved by the DfE.

Approved Information (hard copy and electronic) will be retained for at least the period specified in the retention schedule. When managing records, the school will adhere to the standard retention times listed within that schedule. Paper and Electronic records will be regularly monitored by school staff. The retention periods are based on business needs and legal requirements.

18 Destruction of records

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.

We will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

.

19 Disclosure and Barring Service (DBS) data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

20 Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. A personal data breach is more than just losing personal data. It is a breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

In the event of a suspected data breach, we will follow the school's Personal Data Breach Procedure (see Appendix A) and take all steps we can to remedy the breach that has occurred.

When appropriate, we will report the data breach to the ICO within 72 hours.

21 Cyber Awareness Plan – Training and Acceptable Use

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Train students and staff

Training students and staff in cyber security is a vital step in maintaining safety and security. Cyber training should be given at least annually, or more regularly if there is a known cyber risk to those who use school or college digital technology.

The SLT digital lead will need to coordinate training with IT support, the DPO and the designated safeguarding lead. This training is for:

- students
- staff
- at least one current governor or trustee
- anyone else with a login (for example supply teachers or agency workers) who may need more focussed training using your own resources – this should happen as soon as it's feasible

Training should be age-appropriate and suited to your school or college's risks, but should generally include training on:

- methods hackers use for tricking people into disclosing personal information, including phishing
- password security

- online safety
- social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
- the physical security of devices, for example not leaving a laptop unlocked and unattended
- the risks of using removable storage media, such as USBs
- multi-factor authentication
- how to report a cyber incident or attack
- how to report a personal data breach
- data protection for all staff, with staff who are exposed to higher risk data having more frequent training, such as administrative staff, management or agency workers with a login
- **Create an acceptable use policy**
- An acceptable use policy describes what a person on the network can or cannot do when using digital technology.
- Anyone who has access to the school or college network or data will need to be made aware of, and sign up to, the acceptable use policy. This will include guests and supply teachers who want to use the school or college network and wifi.
- **The SLT digital lead and or other appropriate member of staff will work with IT support, the designated safeguarding lead and the DPO where possible to create and update the acceptable use policy.**

22 Cyber Risk Assessment

Create a risk management process and cyber response plan

The SLT digital lead will work with the business professionals or the finance team, estate management and IT support to:

- create a simple reporting structure for cyber risks to be captured, escalated and actioned – cyber risks should be captured in the risk register and placed into a regularly tested business continuity plan
- maintain documentation and your business continuity plan in at least one or more (diverse) locations – for example, in the cloud or as a hard copy
- **flag any risks** or issues identified to the governors or trustees as part of the school or college's risk management process
- **put a cyber response plan in place**

23 Artificial Intelligence AI

To minimise risks, the appropriate/inappropriate use of AI, the misuse of AI and the safe implementation of necessary AI tools should be considered in relation to cyber security.

Appropriate use of AI in school

- Work should be labelled when using AI.
- Pupils work should not be used to train AI tools.

- Pupils work should not be entered into AI tools without the consent of the owner and the school.
- Any data entered into AI should not be personal data that is confidential and or sensitive in nature.
- Any data entered into AI by staff and governors/trustees is the responsibility of staff and governors/trustees in relation to content, confidentiality, security, safeguarding and training AI tools.

AI Misuse

- Staff will consider the potential pupil misuse of use of AI tools when assessing pupil's work.
- School devices used for assessments and exams should not have access to AI tools or should have them disabled for the duration.
- Staff should investigate the inappropriate use of AI tools and report the use to the SLT.
- Pupils should declare AI use within their work
- Pupils may be subject to school sanctions regarding the inappropriate use of AI including online safety and the submission of work.

Implementation of AI

- Assess curriculum needs to determine the most necessary and appropriate AI tools.
- Assess the staff needs to determine the most necessary and appropriate AI tools.
- Provide appropriate training within the school community.
- Consider safeguarding procedures.
- **Consider appropriate cyber security procedures in line with the DfE digital and technology standards where possible.**
- **Consider any other and / or future factors that may come to light.**
- **Consider AI policy.**

24 Whisteblowing for Employees

There are existing procedures in place to enable staff to lodge a grievance relating to employment, seek access to information, or complain regarding the way in which the school is handling staff's personal data. Whistleblowing covers major concerns that fall outside the scope of other procedures. These include but are not limited to:

- concerns over practices observed by staff that adversely impacts on the security of personal data held by the school
- concerns over unauthorised disclosure or use of personal data held by the school
- concerns over actions leading to the corruption or loss of integrity of any of the personal data held by the school
- other unethical conduct which staff believe is a breach of the schools obligations as a Data Controller

Thus, any serious concerns that staff have about any aspect of the school's handling of personal data or of others acting on behalf of the school in their handling of personal data can be reported to line managers and or DPO and or ICO.

The school has detailed procedures in place for whistleblowing with regards to safeguarding and financial management. These procedures would be followed in relation to whistleblowing relating to data protection.

This process does not replace the schools complaints procedure.

25 Review and Monitoring arrangements

This policy is reviewed at least annually by the School Business Manager, the Data Protection Officer (DPO), the Governor with responsibility for UK GDPR and the Headteacher.

For help or advice on this policy and further specialist information may be sought form the school's DPO please contact the Data Protection Team at: office@whitingshill.barnetmail.net

This policy is reviewed and ratified by the Full Governing Body.

Appendix A – Data Breach Procedure

Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, a potential breach, or a breach that is likely to have occurred, the staff member or data processor must immediately notify the DPT (Data Protection Team).

2. The DPT will decide if there are any conflicts of interest within the team and, if there are, the relevant person will step away from the process.

3. The DPT will investigate the report, and determine whether a breach has occurred. To decide, the DPT will consider whether personal data has been accidentally or unlawfully:

- lost
- stolen
- destroyed
- altered
- disclosed or made available where it should not have been
- made available to unauthorised people.

4. The DPT will alert the Chair of Governors.

5. The DPT will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.(Actions relevant to specific data types are set out at the end of this procedure)

6. The DPT will assess the potential consequences, based on how serious they are, and how likely they are to happen

7. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- loss of control over their data
- discrimination
- identify theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation (for example, key-coding)
- damage to reputation
- loss of confidentiality
- any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. The DPT will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- a description of the nature of the personal data breach
- the categories and approximate number of individuals concerned
- the categories and approximate number of personal data records concerned
- the name and contact details of the DPO
- a description of the likely consequences of the personal data breach
- a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

8. The DPT will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- the name and contact details of the DPO
- a description of the likely consequences of the personal data breach
- a description of the measures that have been, or will be, taken to deal with the
- data breach and mitigate any possible adverse effects on the individual(s) concerned.

9. The DPT will notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies.

10. The DPT will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- facts and cause
- effects
- action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored securely. The DPT will review what happened and how it can be stopped from happening again. This review will occur as soon as reasonably possible.

11. For serious breaches the DPT will consider:

- Informing the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk
- Contacting your local police via Action Fraud Action Fraud website or call 0300 123 2040
- Contacting the Local Authority (LA)
- Contacting the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk

Actions to minimise the impact of data breaches

In the event of a data breach, the school will take action to mitigate the impact of the breach, particularly if it involves sensitive information. The school will review the effectiveness of these actions and amend them as necessary after any data breach.