Data Protection (GDPR) Policy

Approved by:	**Full Governing Body**
Date:	**December 2025**
Next review due by:	**December 2026**

CONTENTS

1. Aims
2. Legislation and guidance
    - 2a. Alignment with Ofsted Inspection Framework 2025
3. Definitions
4. The Data Controller
5. Roles and Responsibilities
6. Data protection principles
7. Collecting personal data
    - 7a. Obtaining and Managing Consent
    - 7b. Privacy Notices
8. Sharing personal data
    - 8a. Data Processing Agreements
    - 8b. International Data Transfers
9. Subject access requests and other rights of individuals
    - 9a. Automated Decision-Making and AI
10. Parental requests to see the educational record
11. Photographs and videos
    - 11a. Children's Digital Rights and Online Safety
    - 11b. Biometric Data
12. Data protection by design and default
    - 12a. Data Protection Impact Assessments (DPIAs)
    - 12b. Record of Processing Activities
13. Data security and storage of records
    - 13a. Data Retention
14. Disposal of records
15. Personal data breaches
16. Training
17. Monitoring arrangements
    - 17a. CCTV and Surveillance
18. Links with other policies

Appendix 1: Personal data breach procedure

1. AIMS

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the:

- **UK General Data Protection Regulation (UK GDPR)** – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- **Data Protection Act 2018 (DPA 2018)**

- **Protection of Freedoms Act 2012** (in relation to biometric data)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the Data Protection Act 2018. This policy also has regard to:

- The ICO's guidance on data protection in schools (updated 2024)
- The ICO's Children's Code (Age Appropriate Design Code), which came into force in September 2020 and was updated in 2023
- The ICO's guidance on surveillance cameras and personal information
- The Education Inspection Framework 2025
- ICO guidance on international transfers and adequacy regulations
- The Data (Use and Access) Act 2025 (DUAA), which includes safeguarding as a 'recognised legitimate interest'

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

2a. ALIGNMENT WITH OFSTED INSPECTION FRAMEWORK 2025

This policy supports the school's safeguarding culture and commitment to keeping children safe, which is a key evaluation area under the Education Inspection Framework 2025.

Under the new framework (effective from 10 November 2025), safeguarding is evaluated separately and graded as 'met' or 'not met'. The Key Leaders Our data protection practices contribute to effective safeguarding by:

- Ensuring that safeguarding information is appropriately shared with relevant professionals while maintaining confidentiality
- Protecting sensitive information about vulnerable children
- Maintaining secure records that support safeguarding decision-making
- Ensuring staff understand their responsibilities for handling sensitive safeguarding data
- Having clear procedures for data breaches that could compromise children's safety

The school establishes an open and positive safeguarding culture that puts pupils' interests first, and leaders take an effective, whole-school approach to safeguarding. Ofsted State-Funded School Inspection Toolkit This includes ensuring that data protection practices support, rather than hinder, effective safeguarding.

Data protection is integral to our approach to:

- **Safeguarding:** Protecting sensitive information while ensuring appropriate information sharing. UK data protection laws do not prevent or limit us from sharing information to keep children safe. They only require us to share the information appropriately, in line with data protection principles. The Key Leaders
- **Inclusion:** Ensuring data about pupils with SEND, disadvantaged pupils, and those with other barriers to learning is handled sensitively and supports their needs. Ofsted State-Funded School Inspection Toolkit
- **Leadership and Governance:** Demonstrating accountability and compliance with statutory requirements

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: Name (including initials), Identification number, Location data, Online identifier (such as a username). It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Term	Definition
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Genetics, Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes, Health – physical or mental, Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO (registration number Z5454737) and will renew this registration annually or as otherwise legally required.

5. ROLES AND RESPONSIBILITIES

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

The governing board will:

- Ensure the school has appropriate policies and procedures in place for data protection
- Receive an annual report from the DPO on data protection compliance
- Ensure adequate resources are allocated to data protection
- Ensure data protection is considered in all decision-making
- Hold the headteacher to account for data protection compliance

5.2 Data Protection Officer

The Data Protection Officer (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 the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Nicola Cook. She can be contacted via the school office.

The DPO's responsibilities include:

- Advising the school on data protection obligations
- Monitoring compliance with data protection law and this policy
- Conducting data protection impact assessments
- Maintaining the Record of Processing Activities
- Being the point of contact for data subjects and the ICO
- Providing training and guidance to staff
- Investigating data breaches
- Reviewing and updating data protection policies
- Maintaining the register of data processors
- Providing advice to staff who are uncertain about whether sharing certain information is the right choice The Key Leaders

5.3 Headteacher/School Business Manager

The Headteacher and School Business Manager act as the representatives of the data controller on a day-to-day basis.

They are responsible for:

- Ensuring staff comply with this policy
- Promoting a culture of data protection across the school
- Ensuring adequate resources for data protection
- Supporting the DPO in their role
- Reporting data protection issues to governors
- Creating an environment where staff feel confident about when and how to share information if a child is at risk or perceived risk of harm The Key Leaders

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Taking responsibility for sharing information in order to keep children safe from harm. They must not assume someone else will pass on information. The Key Leaders
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties
    - Before selecting or using any new educational technology, apps, or online platforms that process children's personal data

6. DATA PROTECTION PRINCIPLES

The UK GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

The seventh principle is that the school is responsible for complying with these principles and must be able to demonstrate compliance. The Key Leaders

This policy sets out how the school aims to comply with these principles.

7. COLLECTING PERSONAL DATA

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden. Under the Data (Use and Access) Act 2025 (DUAA), safeguarding children or vulnerable individuals is a 'recognised legitimate interest'. This means we can use this as a lawful basis for sharing information. The Key Leaders
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law.

Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law through our privacy notices (see section 7b).

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 school's record retention schedule (see section 13a).

7a. OBTAINING AND MANAGING CONSENT

When we rely on consent as our lawful basis for processing personal data, consent must be freely given, specific, informed and unambiguous, and a positive affirmation of the individual's agreement. The Key Leaders

We will ensure that consent is:

- **Freely given** – individuals have a genuine choice and can refuse without detriment
- **Specific** – consent is given for a specific purpose
- **Informed** – individuals understand what they are consenting to
- **Unambiguous** – consent is given through a clear affirmative action (not pre-ticked boxes or inactivity)

We will:

- Keep records of when and how consent was obtained
- Make it easy for individuals to withdraw consent at any time
- Review consent regularly, particularly for children, as their capacity to consent may change as they mature
- Not make services conditional on consent unless the processing is necessary for that service
- Ensure consent requests are separate from other terms and conditions
- Use clear, plain language that is easy to understand

Consent and children:

For children under 13, we will obtain consent from a parent or carer. For children aged 13-18, we will assess their capacity to consent on a case-by-case basis, taking into account:

- The child's age and maturity
- The nature of the personal data
- The potential impact on the child

- Whether the child can understand what they are consenting to

Where we have doubts about a child's capacity to consent, we will seek parental consent.

Parents and carers can withdraw consent on behalf of their child at any time by contacting the DPO.

7b. PRIVACY NOTICES

We provide privacy notices (also known as 'fair processing notices') to individuals when we collect their personal data. Privacy notices must be in clear and plain language and include information about our 'lawful basis' for processing personal data and the individual's rights in relation to their own data.

These notices explain:

- Who we are (the data controller) and our contact details
- Contact details for our DPO
- What personal data we collect and why
- Our lawful basis for processing
- Who we share data with
- How long we keep data (or the criteria used to determine retention periods)
- Individuals' rights over their data, including the right to withdraw consent where applicable
- The right to complain to the ICO
- Whether providing the data is a statutory or contractual requirement
- Whether there is any automated decision-making
- Details of any international transfers

We have separate privacy notices for:

- **Pupils and parents/carers** – provided at admission and published on our website
- **Staff** (including volunteers) – provided at recruitment and published on our website
- **Governors** – provided at appointment
- **Visitors and contractors** – available on our website and at reception

Privacy notices are:

- Published on our school website under 'Privacy Information'
- Provided to individuals when we first collect their data
- Written in clear, plain language appropriate to the audience
- Reviewed annually and updated when our processing activities change
- Available in alternative formats on request

When we update our privacy notices, we will inform affected individuals of any significant changes.

Data is processed in accordance with our school's privacy notices.

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this, unless doing so would put a child at risk of harm
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies, educational app providers, school meal providers, school photographers
- We are legally required to share data with government bodies such as the Department for Education, local authorities, Ofsted, or the Health and Safety Executive

- It is necessary for safeguarding purposes, in which case we may share information without consent if obtaining consent would put a child at risk of harm

Sharing safeguarding information:

UK data protection laws do not prevent or limit us from sharing information to keep children safe. They only require us to share the information appropriately, in line with data protection principles.

We can share information with the appropriate people if we believe that doing so is likely to support the safeguarding and protection of a child. For example, we can share information:

- To help identify patterns of behaviour for a child at risk of going missing, or who has gone missing
- With external agencies when there are concerns about multiple children associated with the same location or situation, to help build a bigger picture

We must not share information if it may harm a child or put them at risk of harm.

When sharing data with suppliers or contractors, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a data processing agreement with the supplier or contractor to ensure the fair and lawful processing of any personal data we share (see section 8a)
- Only share data that the supplier or contractor needs to carry out their service
- Ensure appropriate security measures are in place

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including:

- When ordered by a court
- To prevent or detect crime
- To protect public safety
- To comply with statutory obligations (e.g., census data, school workforce census)

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.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law (see section 8b).

8a. DATA PROCESSING AGREEMENTS

The school is responsible for making sure that 'data processors' who process personal data on our behalf follow data protection law.

Before sharing personal data with any third-party processor, we will:

- Conduct due diligence to ensure they can provide sufficient guarantees of compliance with UK GDPR
- Check their data protection policies and procedures
- Verify their security measures
- Establish a written data processing agreement that includes:
    - The subject matter and duration of processing
    - The nature and purpose of processing
    - The type of personal data and categories of data subjects
    - The obligations and rights of the school as data controller
    - The processor's obligations regarding security, confidentiality, and data breaches
    - Requirements for sub-processors (the processor must obtain our written consent before engaging sub-processors)
    - Deletion or return of data at the end of the contract
    - The processor's obligation to assist with subject access requests and other rights

- The processor's obligation to assist with data protection impact assessments
- Audit rights

The DPO maintains a register of all data processors, which includes:

- Name and contact details of the processor
- What data is being processed
- Purpose of processing
- Date of contract
- Review date

This register is reviewed at least annually to ensure all contracts remain appropriate and compliant.

Staff must not share personal data with any third party without first consulting the DPO to ensure appropriate agreements are in place.

8b. INTERNATIONAL DATA TRANSFERS

When we transfer personal data outside the UK, we will ensure compliance with UK data protection law.

We will only transfer personal data internationally where:

1. **The country has been deemed 'adequate' by the UK government** – meaning it provides an adequate level of protection for personal data. The ICO maintains a list of adequate countries.
2. **We have appropriate safeguards in place**, such as:
    - Standard Contractual Clauses (SCCs) approved by the ICO
    - Binding Corporate Rules
    - An approved certification mechanism
    - An approved code of conduct
3. **An exception applies**, such as:
    - The individual has explicitly consented to the transfer
    - The transfer is necessary for the performance of a contract with the individual
    - The transfer is necessary for important reasons of public interest
    - The transfer is necessary for the establishment, exercise or defence of legal claims
    - The transfer is necessary to protect the vital interests of the individual

International transfers may occur when:

- Using cloud-based services where data is stored on servers outside the UK
- Using educational apps or platforms operated by overseas companies
- Providing references for staff or pupils moving abroad
- Sharing data with international schools
- Using video conferencing or communication tools with servers abroad

Before any international transfer, staff must:

- Consult the DPO
- Identify where the data will be transferred to
- Confirm the legal basis for the transfer
- Ensure appropriate safeguards are in place

The DPO will document all international transfers, including:

- The countries involved
- The safeguards applied
- The date of transfer

- The purpose of transfer
- Categories of data transferred

This documentation is kept as part of our Record of Processing Activities.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may 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.

For children aged 12 and above, we will:

- Speak to the child to understand their wishes
- Consider the child's maturity and understanding
- Consider the nature of the personal data
- Consider any potential harm to the child

If a child does not want their parent/carer to access their data, we will carefully consider whether it is in the child's best interests to share the information.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification

- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- Is subject to legal professional privilege

Responding to requests from parents about safeguarding information:

If a parent asks to see information about their child that relates to child abuse, we can refuse if it wouldn't be in the best interests of the child.

If they ask to see education data or social work data, we can refuse if we believe that sharing it would be likely to cause serious harm to the physical or mental health of any individual.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see sections 7, 7a and 7b), individuals also have the right to:

- **Withdraw their consent to processing at any time** – where we are relying on consent as our lawful basis for processing
- **Ask us to rectify, erase or restrict processing of their personal data** (in certain circumstances):
    - Rectification: if data is inaccurate or incomplete
    - Erasure ('right to be forgotten'): in certain circumstances, such as where data is no longer necessary for the purpose it was collected
    - Restriction: to limit how we use data in certain circumstances
- **Prevent use of their personal data for direct marketing**
- **Object to processing** which has been justified on the basis of public interest, official authority or legitimate interests
- **Challenge decisions based solely on automated decision-making or profiling** (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- **Be notified of a data breach** (in certain circumstances where the breach is likely to result in high risk to their rights and freedoms)
- **Make a complaint to the ICO**
- **Ask for their personal data to be transferred to a third party** in a structured, commonly used and machine-readable format (in certain circumstances) – known as the right to data portability

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they

must immediately forward it to the DPO.

The DPO will respond to requests within one month, and will inform the individual if an extension is needed (up to a further two months for complex requests).

9a. AUTOMATED DECISION-MAKING AND AI

The school does not currently use automated decision-making or artificial intelligence (AI) systems that make decisions with legal or similarly significant effects on individuals without human involvement.

Automated decision-making means making decisions about individuals using technology alone, without human involvement. This could include, for example, automatically rejecting a job application or automatically calculating a credit score.

If we introduce such systems in the future, we will:

- Conduct a Data Protection Impact Assessment (DPIA) before implementation
- Provide clear information to individuals about the logic involved in the automated decision-making
- Ensure meaningful human oversight of automated decisions
- Give individuals the right to challenge automated decisions and request human intervention
- Ensure the system does not discriminate against individuals or groups
- Regularly test and monitor the system for bias or errors
- Comply with Ofsted's policy on AI use in schools (April 2024)

Use of AI tools to support (but not make) decisions:

Where we use AI tools to support (but not make) decisions, such as using AI to help analyse data or draft documents, we will ensure:

- Staff are trained to understand how the AI works
- Staff can question and override AI suggestions
- Human decision-makers take responsibility for final decisions
- AI tools do not process special category data unless appropriate safeguards are in place
- AI tools comply with our data processing agreements (section 8a)

Examples of AI tools that support but do not make decisions might include:

- AI writing assistants for administrative tasks
- AI tools to help identify patterns in attendance data (with human analysis and decision-making)
- AI chatbots for initial enquiries (with human follow-up)

Staff must consult the DPO before using any new AI tools that process personal data.

10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

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

The educational record includes:

- Academic achievements and progress
- Teacher assessments and reports
- Records of behaviour and attendance
- Any information provided by parents
- Information from other professionals working with the child

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. The fee will not exceed the cost of:

- Photocopying

- Postage (if applicable)
- Any other reasonable costs of supplying the information

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if:

- Releasing the information might cause serious harm to the physical or mental health of the pupil or another individual
- It would mean releasing exam marks before they are officially announced
- The information includes details of child protection concerns, and disclosure would not be in the child's best interests
- The information includes another person's personal data that cannot be reasonably anonymised

Requests for access to the educational record should be made in writing to the DPO.

11. PHOTOGRAPHS AND VIDEOS

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

We will obtain written consent from parents/carers 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.

Our consent form specifies different uses, allowing parents/carers to consent to some uses but not others:

- Use within school (displays, newsletters)
- Use on the school website
- Use on school social media
- Use by external agencies (newspapers, promotional materials)

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, local authority campaigns
- Online on our school website or social media pages

Safeguards:

When using photographs and videos we will:

- Not accompany them with any other personal information about the child that could identify them (such as their full name)
- Not include images of children who are subject to court orders or whose safety may be compromised
- Store images securely
- Only share images with staff who need to see them
- Ensure external photographers sign agreements confirming they will comply with data protection law

Withdrawal of consent:

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will:

- Delete the photograph or video from our systems
- Not distribute it further
- Remove it from displays and publications where reasonably practicable
- Request that external agencies remove the image (though we cannot guarantee compliance)

Parents/carers can withdraw consent by contacting the school office or the DPO.

Children's own use of cameras and phones:

Pupils are not permitted to take photographs or videos of other pupils or staff without permission. Any unauthorised use of cameras or phones will be dealt with in accordance with our behaviour policy and mobile phone policy.

11a. CHILDREN'S DIGITAL RIGHTS AND ONLINE SAFETY

The school recognises that children have specific rights in relation to their personal data, particularly in online environments. We comply with the ICO's Children's Code (Age Appropriate Design Code), which sets out standards for online services likely to be accessed by children.

Selecting educational technology:

When selecting and using educational technology, online platforms, and apps that process children's personal data, we will:

- Conduct due diligence to ensure providers comply with UK data protection law and the Children's Code
- Assess whether the service uses age-appropriate privacy settings by default (e.g., high privacy settings, location services off, profiling off)
- Ensure that data collection is minimised and proportionate to the educational purpose
- Check that children's data is not used for purposes such as profiling, tracking, behavioural advertising, or targeted marketing
- Ensure that privacy information is presented in clear, age-appropriate language that children can understand
- Verify that appropriate parental controls are available where necessary
- Check whether the service shares data with third parties and ensure this is transparent and limited
- Ensure the service has appropriate security measures in place
- Verify that the service will delete or anonymise children's data when it is no longer needed
- Regularly review and audit the educational technology we use

Staff responsibilities:

Staff must not require pupils to use online services or apps that:

- Do not meet the standards above
- Have not been approved by the school
- Require pupils to provide unnecessary personal information
- Have unclear or inappropriate privacy policies
- Cannot demonstrate compliance with UK data protection law

Before using any new educational technology, apps, or online platforms that process children's personal data, staff must:

- Consult the DPO
- Complete a Data Protection Impact Assessment (DPIA) if required
- Ensure appropriate data processing agreements are in place (see section 8a)
- Obtain parental consent where necessary

Online safety and digital literacy:

We will:

- Teach pupils about their digital rights and how to protect their personal information online
- Ensure pupils understand the risks of sharing personal information online
- Provide age-appropriate guidance on privacy settings and online safety

- Regularly review our online safety curriculum to ensure it reflects current risks and best practice

11b. BIOMETRIC DATA

Where the school uses pupils' biometric data as part of an automated biometric recognition system (e.g. for cashless catering or library access), we will comply with the requirements of the Protection of Freedoms Act 2012.

Biometric data is considered a special category of personal data and requires additional safeguards.

What is biometric data?

Biometric data includes fingerprints, facial recognition data, iris patterns, and other unique biological characteristics used for identification purposes.

Our obligations:

We will:

- Obtain explicit written consent from at least one parent/carer before processing a pupil's biometric data
- Provide parents/carers with information about how the data will be used and stored
- Not process the biometric data of a pupil where a parent/carer has objected, or the pupil has objected (regardless of any parental consent)
- Provide reasonable alternative arrangements for pupils who do not use the biometric system
- Ensure biometric data is stored securely and separately from other personal data
- Delete biometric data when the pupil leaves the school or when consent is withdrawn
- Not share biometric data with third parties except where necessary for the operation of the system (and only with appropriate data processing agreements in place)
- Regularly review the necessity and proportionality of using biometric systems

Rights of parents and pupils:

Parents/carers and pupils have the right to:

- Object to participation in the school's biometric recognition system
- Withdraw consent at any time
- Request deletion of their biometric data

If a parent/carer or pupil objects or withdraws consent, we will:

- Stop processing the biometric data immediately
- Delete the data from our systems
- Provide alternative arrangements (e.g., using a PIN code or card system)

Alternative arrangements:

We will ensure that alternative arrangements for pupils who do not use the biometric system:

- Are readily available
- Do not disadvantage the pupil
- Are equally convenient to use
- Maintain the pupil's privacy and dignity

12. DATA PROTECTION BY DESIGN AND DEFAULT

We will 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, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- 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 (see section 6)

- 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) (see section 12a)
- 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities (see section 12b), including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

12a. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

The school must carry out a data protection impact assessment (DPIA) when considering using data in new ways, or implementing new technology to monitor pupils. DPIAs are required where processing presents a high risk to rights and freedoms of individuals.

When we will conduct a DPIA:

We will conduct a DPIA when:

- Using new technologies that process personal data (e.g. new educational apps, CCTV systems, biometric systems, facial recognition)
- Processing special category data on a large scale
- Systematically monitoring publicly accessible areas on a large scale
- Processing data in ways that could result in high risks to individuals' rights and freedoms
- Processing children's data in ways that could affect their welfare
- Using automated decision-making or profiling
- Combining, comparing or matching data from multiple sources
- Processing data about vulnerable individuals (e.g. children with SEND, looked-after children)
- Processing data that might endanger the physical health or safety of individuals in the event of a security breach

DPIA process:

The DPO will lead all DPIAs, consulting with relevant staff and, where appropriate, with data subjects. The DPIA will:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity and proportionality of the processing
- Assess the risks to individuals
- Identify measures to mitigate those risks

DPIAs will be reviewed regularly and updated when there are changes to processing activities.

Consulting the ICO:

If a DPIA identifies high risks that cannot be mitigated, we will consult the ICO before proceeding with the

processing.

12b. RECORD OF PROCESSING ACTIVITIES

The school maintains a Record of Processing Activities (ROPA) that documents all processing of personal data. This is a legal requirement under UK GDPR.

What the ROPA includes:

Our ROPA documents:

- The purposes of processing
- Categories of data subjects (e.g., pupils, staff, parents)
- Categories of personal data (e.g., contact details, academic records, medical information)
- Categories of recipients of personal data (e.g., local authorities, exam boards, external agencies)
- Details of transfers to third countries (if applicable), including the safeguards in place
- Retention periods (or the criteria used to determine retention periods)
- A general description of security measures

Maintaining the ROPA:

The ROPA is:

- Maintained by the DPO
- Reviewed annually, or when there are significant changes to our processing activities
- Available for inspection by the ICO if requested
- Used to support our compliance with data protection law
- Used to identify areas where DPIAs may be required

Staff must inform the DPO of any new processing activities so that the ROPA can be updated.

13. DATA SECURITY AND STORAGE OF RECORDS

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.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- 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 ICT Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- All electronic devices are password-protected and have up-to-date anti-virus software
- Staff are trained to recognise phishing emails and other cyber security threats
- We have a clear desk policy to ensure confidential information is not left visible

- Confidential waste is disposed of securely (see section 14)

Protecting medical information:

When taking medical information on school trips, we will:

- Keep it in a locked suitcase or safe at the accommodation (for paper information)
- Encrypt any information stored on portable electronic devices
- Password protect any information kept in cloud-based storage
- Only share the information with staff who need it for the trip
- Ensure the information is returned securely to school and stored appropriately

Displaying information:

We will be careful about displaying personal information in areas accessible to visitors, such as:

- Reception areas
- Staffrooms
- Corridors and communal areas

If visitors will use spaces where personal information might be displayed, we will:

- Seek permission from parents or meet another lawful basis under UK GDPR before displaying pupil photos and information
- Avoid displaying confidential information such as pupils' medical information, test results, or safeguarding information
- Use secure noticeboards for sensitive information that can be locked or placed in staff-only areas

13a. DATA RETENTION

The school maintains a data retention schedule that sets out how long we keep different types of personal data. This schedule is based on:

- Legal requirements (e.g. employment records, financial records)
- Statutory guidance (e.g. safeguarding records)
- Best practice recommendations from the Information and Records Management Society (IRMS)

Key retention periods:

Examples of retention periods include (but are not limited to):

Type of data	**Retention period**
Pupil files (including academic records)	Until the pupil reaches age 25
Safeguarding records	Until the pupil reaches age 25 (or longer if serious concerns)
Accident and incident reports	Until the pupil reaches age 25 (or 3 years for adults)
Staff personnel files	6 years after employment ends
Payroll records	6 years after the end of the financial year
CCTV footage	30 days (unless required for an investigation)
Biometric data	Deleted when the pupil leaves or consent is withdrawn

Our full retention schedule is available from the DPO and is reviewed annually.

Applying the retention schedule:

When retention periods expire, data is securely disposed of in accordance with Section 14 of this policy.

Staff must:

- Not keep personal data for longer than necessary
- Follow the retention schedule when managing records
- Consult the DPO if unsure about retention periods
- Ensure that data is securely stored throughout the retention period

14. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

Methods of disposal:

For paper-based records:

- Shredding using a cross-cut shredder
- Incineration
- Using a confidential waste disposal service

For electronic records:

- Overwriting data
- Deleting files and emptying recycle bins
- Physically destroying storage devices (e.g., hard drives)
- Using data erasure software
- Degaussing (for magnetic storage devices)

Using third-party disposal services:

We may 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
- Establish a data processing agreement (see section 8a)
- Obtain a certificate of destruction for audit purposes
- Ensure the third party uses secure methods of disposal

Recording disposal:

The DPO will maintain a record of data disposal, including:

- What data was disposed of
- When it was disposed of
- The method of disposal
- Who authorised the disposal

15. PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

Examples of data breaches:

Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of

pupils eligible for the pupil premium

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils
- An email containing sensitive information being sent to the wrong recipient
- Loss of unencrypted USB drives containing personal data
- Unauthorised access to school systems by hackers
- Ransomware attacks that prevent access to personal data
- Personal data being posted on social media without consent

Reporting to the ICO:

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

We must report a breach to the ICO if it is likely to result in a risk to the rights and freedoms of individuals. We will use the ICO's self-assessment tool to determine whether we need to report the breach.

Notifying individuals:

Where a breach is likely to result in a high risk to

Please continue from 15

15. PERSONAL DATA BREACHES (continued)

Notifying individuals:

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify those affected without undue delay.

The notification will include:

- A description of the nature of the breach
- The name and contact details of the DPO
- A description of the likely consequences
- A description of the measures taken or proposed to address the breach and mitigate its effects

Staff responsibilities:

All staff must be aware of the data breach procedure and know how to report a suspected breach immediately to the DPO.

16. TRAINING

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.

Our data protection training programme includes:

- **Induction training** for all new staff and governors covering the basics of UK GDPR and this policy
- **Role-specific training** (e.g. for teachers, administrative staff, senior leaders, designated safeguarding leads)
- **Regular refresher training** (at least annually)
- **Specific training** when new systems or processes are introduced
- **Training on responding to data breaches**
- **Training on recognising and responding to subject access requests**
- **Training on safeguarding information sharing**
- **Training on the Children's Code and online safety**
- **Training on cyber security and recognising threats**

Training content:

Training will cover:

- The principles of data protection
- Understanding the lawful bases for processing
- How to handle personal data securely
- Recognising and reporting data breaches
- Responding to subject access requests
- Understanding consent requirements
- Safeguarding information sharing
- Using educational technology safely
- Staff responsibilities under this policy

Training records:

The DPO maintains records of all data protection training, including:

- Who has been trained
- When training took place
- Topics covered
- Attendance records
- Assessment results (where applicable)

Mandatory training:

All staff must complete data protection training as part of their professional responsibilities. Failure to complete mandatory training may result in disciplinary action.

Staff must also:

- Read and understand this policy
- Confirm they have read and understood the policy by signing an acknowledgement form
- Attend refresher training when required
- Seek guidance from the DPO when unsure about data protection matters

17. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy and the school's compliance with data protection law.

Monitoring activities include:

- **Conducting annual data protection audits** using the ICO's audit framework
- **Regular spot-checks** of data processing activities
- **Reviewing and updating** the Record of Processing Activities
- **Monitoring data breach reports** and identifying trends
- **Reviewing data processing agreements** with third parties
- **Assessing the effectiveness** of data protection training
- **Reviewing privacy notices** to ensure they remain accurate and up-to-date
- **Checking compliance** with retention schedules
- **Reviewing security measures** and access controls
- **Monitoring new processing activities** to identify where DPIAs may be required

Annual audit:

The completed audit will be used as:

- Part of a report to governors

- A source of evidence should a serious data breach occur
- A tool to identify areas for improvement
- Evidence of our commitment to data protection compliance

Reporting to governors:

The governing board receives an annual report from the DPO covering:

- Compliance with data protection law
- Data breaches and incidents
- Subject access requests and other rights requests
- Training completion rates
- Audit findings and recommendations
- Updates to policies and procedures
- Emerging risks and issues
- Resource requirements

Policy review:

This policy will be reviewed **every two years**, or sooner if:

- There are changes to relevant legislation or guidance
- There are significant changes to our processing activities
- A serious data breach occurs
- The ICO issues new guidance
- Audit findings identify areas for improvement

The review will involve:

- The DPO
- The headteacher
- The governing board
- Input from staff where appropriate

17a. CCTV AND SURVEILLANCE

The school uses CCTV systems to ensure the safety and security of pupils, staff, and visitors, and to protect school property.

Legal compliance:

Our use of CCTV complies with:

- UK GDPR and Data Protection Act 2018
- ICO's guidance on surveillance cameras and personal information
- The Surveillance Camera Code of Practice

How we use CCTV:

We will:

- Display clear signage informing people that CCTV is in operation, including:
    - That CCTV is in use
    - The purposes for which it is used
    - Who to contact for more information (the DPO)
- Only use CCTV for specified purposes:
    - Security and protection of property

    - Safeguarding pupils and staff
    - Preventing and detecting crime
    - Supporting disciplinary and safeguarding investigations
- Ensure cameras are positioned to:
    - Minimise intrusion into privacy
    - Avoid capturing images of areas where individuals have a reasonable expectation of privacy (e.g., toilets, changing rooms)
    - Focus on areas where security or safeguarding concerns exist
- Limit access to CCTV footage to authorised personnel only:
    - The headteacher
    - The DPO
    - Designated staff responsible for security
    - Police or other authorities where legally required
- Retain footage for no longer than necessary (typically **30 days** unless required for an investigation or legal proceedings)
- Store footage securely with appropriate access controls
- Respond to subject access requests for CCTV footage within statutory timeframes (see section 9)
- Conduct regular reviews of our CCTV systems to ensure ongoing compliance

Subject access requests for CCTV footage:

Individuals have the right to request access to CCTV footage that shows them. When responding to such requests, we will:

- Verify the identity of the requester
- Locate the relevant footage
- Consider whether disclosure would reveal the identity of other individuals (if so, we may need to blur or redact their images)
- Provide the footage within one month
- Refuse the request if it is manifestly unfounded or excessive

CCTV policy:

Further details about our CCTV systems are set out in our **[CCTV Policy/Security Policy]** [insert reference to your separate CCTV policy if you have one, or note that this section constitutes your CCTV policy].

18. LINKS WITH OTHER POLICIES

This data protection policy is linked to our:

- **Safeguarding and Child Protection Policy** (including allegations against staff)
- **Freedom of Information Policy**
- **ICT and Internet Acceptable Use Policy**
- **Mobile Phone/Camera Policy**
- **Use of Photographic Images and Videos of Children in Schools Policy**
- **Staff Code of Conduct**
- **Volunteer Policy**
- **Visitor Policy**
- **CCTV Policy** (if separate)
- **Records Management Policy**
- **Information Security Policy**

- **Retention Schedule**
- **Staff Capability Policy**
- **Recruitment and Selection Policy**
- **Health and Safety Policy**
- **Supporting Pupils with Medical Conditions Policy**
- **Educational Visits Policy**
- **Online Safety Policy**

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

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

Reporting a breach

- On finding or causing a breach, or potential breach, the staff member or data processor must **immediately notify the DPO by email** [insert DPO email address]
- The report should include:
    - What happened
    - When it happened
    - What data was involved
    - Who was affected
    - What action has been taken so far

Initial investigation

- The DPO will investigate the report, and determine whether a breach has occurred
- To decide, the DPO 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
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions)
- The investigation will not be treated as a disciplinary investigation

Escalation

- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the **headteacher** and the **chair of governors**
- For serious breaches, the headteacher will convene an emergency meeting with the DPO and relevant senior leaders

Containment and recovery

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach
- Relevant staff members or data processors should help the DPO with this where necessary
- The DPO should take external advice when required (e.g. from IT providers, legal advisors, the ICO)
- Actions may include (depending on the type of breach):
    - Attempting to recall emails sent in error
    - Changing passwords and access credentials
    - Recovering lost or stolen devices

    - Informing third parties (e.g., email recipients) and requesting they delete information
    - Shutting down systems to prevent further unauthorised access
    - Restoring data from backups

Risk assessment

- The DPO will assess the potential consequences of the breach, based on:
    - How serious they are
    - How likely they are to happen
    - Whether steps taken have mitigated the consequences
- The assessment will consider:
    - The type and sensitivity of data involved
    - The number of individuals affected
    - The potential harm to individuals (e.g., identity theft, financial loss, damage to reputation, emotional distress)
    - Any special characteristics of affected individuals (e.g., children, vulnerable adults)
    - Whether the data was protected by security measures (e.g., encryption, passwords)

Deciding whether to report to the ICO

- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the **ICO's self-assessment tool**
- A breach must be reported to the ICO if it is **likely to result in a risk** to the rights and freedoms of individuals
- A breach must be reported to affected individuals if it is **likely to result in a high risk** to their rights and freedoms
- The DPO 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 business computer [or specify location]

Reporting to the ICO

Where the ICO must be notified, the DPO will do this via the **'report a breach' page of the ICO website** or through its **breach report line (0303 123 1113)**, within **72 hours** of the school's awareness of the breach.

As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - 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 of the school's awareness of the breach. 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.

Notifying individuals

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- 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

The notification will be sent without undue delay.

Notifying third parties

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example:

- The police (if a crime has been committed)
- Insurers
- Banks or credit card companies (if financial data has been compromised)
- Action Fraud (the UK's national fraud and cybercrime reporting centre)
- The National Cyber Security Centre (for significant cyber incidents)

Documentation

The DPO 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)
- Whether the breach was reported to the ICO
- Whether affected individuals were notified
- Lessons learned

Records of all breaches will be stored on the school's business computer [or specify location] and will be kept securely.

Review and learning

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again
- This meeting will happen as soon as reasonably possible after the breach has been contained
- Actions may include:
    - Updating policies and procedures
    - Providing additional staff training
    - Implementing new security measures
    - Reviewing access controls
    - Updating risk assessments
    - Reviewing contracts with third-party processors
- The DPO and headteacher will meet regularly (at least termly) to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

ACTIONS TO MINIMISE THE IMPACT OF DATA BREACHES

We set out below the steps we might take to try to mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT support team to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

Details of pupil premium or SEND interventions being published on the school website

- The information will be removed from the website immediately
- The DPO will check whether the information has been cached by search engines or archived on other websites
- If so, the DPO will request removal from search engine caches and archived sites
- The DPO will assess whether the breach needs to be reported to the ICO and/or affected individuals
- Parents of affected pupils will be notified if required
- The website publishing process will be reviewed to prevent future occurrences

Non-anonymised pupil exam results or staff pay information being shared with governors

- The DPO will immediately contact all governors who received the information and request that they:
    - Delete the information from all devices
    - Delete any printed copies securely
    - Confirm in writing that they have done so
- The DPO will send the correct, anonymised version
- The breach will be recorded and the process for sharing information with governors will be reviewed
- Additional training may be provided to staff responsible for preparing governor reports **A school laptop containing non-encrypted sensitive personal data being stolen or hacked (continued)**
- The theft/hack must be reported to the police immediately and a crime reference number obtained
- The DPO will assess what data was on the device and who is affected
- If the device can be remotely wiped, this should be done immediately
- Passwords for school systems should be changed if there is a risk they were compromised
- The ICO must be notified within 72 hours if the breach is likely to result in a risk to individuals
- Affected individuals must be notified if the breach is likely to result in a high risk to them
- The school's insurance provider should be notified
- A full review of device security and encryption policies will be conducted
- All staff will receive refresher training on data security and the requirement to encrypt portable devices
- Disciplinary action may be considered if policies were not followed
- **The school's cashless payment provider being hacked and parents' financial details stolen**
- The DPO will immediately contact the payment provider to:
- Confirm the extent of the breach
- Understand what data has been compromised

- Establish what action the provider is taking
- Confirm whether the provider is reporting to the ICO
- The school will assess whether it also needs to report the breach to the ICO (as data controller)
- Parents whose financial details were compromised will be notified immediately and advised to:
- Monitor their bank accounts for suspicious activity
- Contact their bank to report the breach
- Consider changing payment cards
- Be alert to phishing attempts
- The school will provide parents with information about Action Fraud and how to report fraud
- The contract with the payment provider will be reviewed
- Alternative payment providers may be considered
- The incident will be reported to the governing board
- **Hard copy reports sent to the wrong pupils or families**
- The DPO will immediately contact the families who received the wrong reports and:
- Explain what has happened
- Request that they return the reports to school or destroy them securely
- Apologise for the error
- Confirm in writing once the reports have been returned/destroyed
- The correct reports will be sent to the intended recipients with an explanation and apology if appropriate
- The families whose reports were sent to others will be notified of the breach
- The breach will be assessed to determine if ICO notification is required
- The process for distributing reports will be reviewed to include additional checks
- Staff involved will receive additional training on handling confidential information
- **Loss of USB drive containing pupil data**
- The area where the USB drive was last seen will be thoroughly searched
- If not found within 24 hours, the breach must be reported to the DPO
- The DPO will assess:
- What data was on the USB drive
- Whether it was encrypted
- Who might have access to it
- The likelihood of the data being accessed
- If the USB drive was not encrypted, the ICO must be notified within 72 hours
- Affected individuals may need to be notified depending on the sensitivity of the data
- All staff will be reminded about the prohibition on using USB drives for storing personal data
- The use of USB drives will be reviewed and potentially restricted through technical controls
- **Unauthorised access to school systems by hackers (cyber attack)**
- IT support must be contacted immediately to:
- Isolate affected systems
- Assess the extent of the breach
- Identify what data has been accessed or compromised
- Secure systems and prevent further access

- All passwords must be changed immediately
- The National Cyber Security Centre should be contacted for advice
- The police should be informed via Action Fraud
- The ICO must be notified within 72 hours
- Affected individuals must be notified if there is high risk to them
- The school's insurance provider should be notified
- A full security audit will be conducted
- Additional security measures will be implemented
- Staff will receive cyber security training
- **Personal data posted on social media without consent**
- The DPO will immediately contact the person who posted the information and request removal
- If the post is not removed promptly, the DPO will report it to the social media platform using their reporting mechanisms
- Screenshots will be taken as evidence before the post is removed
- The DPO will assess whether the breach needs to be reported to the ICO and/or affected individuals
- If the post was made by a staff member, disciplinary action may be considered
- If the post was made by a pupil, the incident will be dealt with in accordance with the behaviour policy
- Social media policies and training will be reviewed
- **Safeguarding information disclosed to unauthorised person**
- The DPO will immediately inform the Designated Safeguarding Lead (DSL)
- The DSL and DPO will assess:
- What information was disclosed
- To whom it was disclosed
- Whether this puts any child at increased risk
- If a child is at increased risk, immediate safeguarding action will be taken, which may include:
- Informing the local authority designated officer (LADO)
- Informing children's social care
- Informing the police
- Implementing additional safety measures for the child
- The unauthorised person will be contacted and asked to:
- Not share the information further
- Delete or return any copies
- Confirm in writing that they have done so
- The ICO must be notified within 72 hours
- The breach will be reported to the governing board
- Safeguarding information handling procedures will be reviewed
- Additional training will be provided to all staff on handling safeguarding information