Fioretti Trust

Aspiration Wisdom Compassion

Data Protection Policy
(2026-2028)

This policy supersedes all other ***data protection*** policies

Approved by:	Trust Board
Date of review:	7th July 2026
Next review:	July 2028
Cycle:	2 yearly

Contents

Policy statement

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a trust, Fioretti Trust will collect, store, and process personal data about pupils, workforce, parents and others. This makes us a data controller in relation to that personal data.

We are committed to the protection of all personal data and special category personal data.

The law imposes significant fines for failing to lawfully process and safeguard personal data. This policy sets out how we comply with the relevant legislation. Breaches of this policy can result in real harm to individuals, action for damages, loss of trust and reputational harm, as well as regulatory penalties including fines from the ICO.

All staff must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action. Individuals may also be prosecuted for committing offences under sections 170–173 of the Data Protection Act 2018, which create criminal offences for the unlawful obtaining, disclosing or procuring of personal data.

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 the General Data Protection Regulation (GDPR) and provisions of the Data Protection Act 2018 (DPA 2018)

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 GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

This policy has also been updated to reflect the Data (Use and Access) Act 2025, which amends the UK GDPR and DPA 2018, including widening the circumstances in which schools may rely on legitimate interests as a lawful basis for processing, with specific reference to safeguarding children.

Legislative basis: Data (Use and Access) Act 2025; Keeping Children Safe in Education 2025, which directs schools to the DfE Data Protection guidance for schools and to DfE guidance on generative AI in education.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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.

In addition, this policy complies with our funding agreement and articles of association.

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.
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.
Data users	Members of the Trust's workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this policy and any applicable data security procedures at all times.
Workforce	Includes any individual employed by the Trust such as staff, and those who volunteer in any capacity including trustees, members, local governors and parent helpers.
Data protection impact assessment (DPIA)	A tool to help identify how to comply with data protection obligations and protect individuals' rights, as set out in Article 35 of the UK GDPR. The ICO provides guidance on DPIAs at ico.org.uk. The DPO must be consulted as to whether a DPIA is required whenever the Trust introduces new technologies or changes existing ways of working

	involving personal data.
Privacy notice	A statement provided to data subjects when we collect their personal data, setting out: the identity and contact details of the data controller and DPO; the purposes and legal basis for processing; types of third parties with whom data will be shared; whether data will be transferred outside the UK; retention periods; the existence of any automated decision-making; and the data subject's rights including the right to complain to the ICO.

4. The data controller

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

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Trust Board

The Trust Board has overall responsibility for ensuring that Fioretti Trust complies with all relevant data protection obligations; but it delegates responsibilities to the Local Governing Bodies to oversee compliance at individual school level.

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 trust 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.

The Fioretti Trust has appointed an external company: Judicium Education to fulfil the DPO duties.

The DPO for The Fioretti Trust is Judicium Consulting Limited and is contactable via email: dataservices@judicium.com or telephone: 0345 548 7000

5.3 Headteacher

The CEO has delegated the headteacher to act as the representative of the data controller on a day-to-day basis.

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
- 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 European Economic Area
    - 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

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

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,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- Under the Data (Use and Access) Act 2025, safeguarding the welfare of a child or individual at risk is recognised as a legitimate interest in its own right, meaning the usual balancing test against the individual's rights does not need to be applied where data is processed for this purpose
- *Legislative basis: Data (Use and Access) Act 2025*.
- 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 which are set out in the UK GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so 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
- 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 will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- 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

Where we share personal data with data processors (suppliers or contractors who process data on our behalf and under our instruction), we will:

- Undertake appropriate due diligence before transferring any personal data to them
- Only transfer data to a processor if they agree to comply with our procedures and policies in relation to data security, or put in place adequate measures to the Trust's satisfaction
- Ensure any contract with a data processor complies with data protection legislation and contains explicit obligations on the processor to ensure compliance and to respect the rights of data subjects

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

- 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.

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.

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
- 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
- Subject access requests should include:
- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request 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.

9.3 Responding to subject access requests
When responding to requests, we:

- May ask the individual to provide two forms of identification

- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- 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 one month, and explain why the extension is necessary

We will not disclose information if 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
- Would include another person's personal data that we cannot reasonably anonymise, where we do not have that 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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

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 section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Receive certain information about the data controller's processing activities
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- 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)

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.

9.5 Consent
Where consent is relied on as the lawful basis for processing personal data, the Trust must ensure that consent is freely given, specific, informed and unambiguous. We cannot use pre-ticked boxes or make the provision of services conditional on a data subject giving consent.

For pupils under the age of 12, we will seek consent from an individual with parental responsibility. We will generally seek consent directly from pupils aged 12 or over, recognising that this may not be appropriate in all circumstances.
Any consent form must: inform the data subject of exactly what we intend to do with their personal data; require them to positively confirm that they consent (opt-in, not opt-out); and inform them of how they can withdraw their consent. The DPO must be consulted before any consent form is used.

It must be as easy for a data subject to withdraw their consent as it was to give it. Where consent is withdrawn, we will stop processing the relevant data as soon as reasonably practicable.

A record must always be kept of any consent, including how and when it was obtained.

Consent may need to be refreshed where we wish to process personal data for a different purpose that is incompatible with the original purpose disclosed when consent was first given.

9.6 Automated decision-making and profiling
The Trust does not routinely make decisions about individuals solely by automated means. However, we recognise that automated processing is increasingly used in educational settings. Examples may include:

- Admissions systems applying oversubscription criteria
- Behaviour or safeguarding monitoring systems that identify patterns or risks
- Assessment platforms that automatically mark or analyse pupil performance

Where automated processing produces outcomes that inform or influence decisions, we will seek to ensure that meaningful human involvement - such as review, oversight, or the ability to amend outcomes - is applied as part of the decision-making process.

Where a decision is made solely by automated means and produces legal or similarly significant effects on a data subject, that individual has the right to: be informed that such a decision has been made; make representations about the decision; request that a human reviews the decision; and contest the outcome. Any such request must be forwarded immediately to the DPO.

Where automated decision-making involves special category personal data, processing will only take place where the individual has given explicit consent, or the processing is necessary for reasons of substantial public interest.

The Trust will keep its approach to automated decision-making under review and will seek further advice where necessary, particularly in relation to new technologies or AI-based systems (see also section 14).

10. Parental requests to see the educational record

The Academy Trust may give parents or those with parental responsibility, the right to have access to

their child's records at a set charge of 10 pence per sheet and will receive it within 15 school days of receipt of a written request.

11. Biometric recognition systems

Where any Fioretti Trust school uses, or plans to use, pupils' biometric data as part of an automated biometric recognition system (for example, fingerprint recognition for cashless catering), the school will comply with the requirements of the Protection of Freedoms Act 2012 and the UK GDPR.

Parents and carers will be notified before any biometric recognition system is put in place, or before their child first takes part in it. The school will get written consent from at least one parent or carer before any biometric data is taken from their child and first processed.

Parents, carers and pupils have the right to choose not to use the school's biometric system(s). The school will provide alternative means of accessing the relevant services for those pupils, for example paying for school dinners in cash.

Parents, carers and pupils can withdraw consent at any time, and the school will ensure any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the school will not process that data, irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use a school's biometric system(s), explicit consent will be obtained before they first take part, and an alternative means of accessing the relevant service will be provided if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

For members of the workforce, explicit written consent will be obtained at the commencement of their employment or engagement with the Trust, before their biometric data is first processed. This consent continues to be effective unless the individual submits a written objection, at which point processing will cease and any captured data will be deleted.

12. CCTV

We use 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.

Any enquiries about the CCTV system should be directed to the Headteacher.

13. Photographs and videos

As part of our school activities, we may take photographs and record images, using a range of devices, of individuals within our schools.

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.

Uses may include:

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

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.

Parents and other attendees at Trust events (for example, school performances or sports days) are permitted to take photographs and videos for personal and domestic purposes. The Trust does not prohibit this as a matter of policy.

However, the Trust asks that parents and other attendees do not post any images or videos which include any child other than their own on social media or otherwise publish those images or videos. We will remind parents and carers of this expectation at relevant events.

Note: The personal/domestic exemption under UK GDPR (Article 2(2)(c)) applies to individuals taking images for their own personal use, not for commercial or wide publication purposes.

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Fioretti Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Trust will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 1.

15. 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 (an external company has been appointed to fulfil this role), 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 privacy 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
- Maintaining records of our processing activities, 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, how and why we are storing the data, retention periods and how we are keeping the data secure

16. 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 password protection 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 adhere to our policy that any school data and children's books must be kept within the employees' home (and not left in the car overnight).
- Passwords made up of 4 random, unrelated words, or 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.
- 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)

17. 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.

For example, 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.

The Information and Records Managements Society's (IRMS) Toolkit sets out how long we keep information about pupils and employees. Therefore, we hold data in line with the IRMS Schools Toolkit (Retention Guidelines page 35) https://irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

18. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

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

19. 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, where changes to legislation, guidance or the school's processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the trust board.

21. Complaints

The Trust takes any complaints about how it collects and uses personal information very seriously. If an individual believes our collection or use of personal information is unfair, misleading or inappropriate, or has any other concerns about our data processing, this should be raised with us in the first instance by contacting the DPO (see section 5.2).

Upon receiving a complaint, we will: acknowledge receipt within 30 days of receiving it; without undue delay, take appropriate steps to respond, including making appropriate enquiries and keeping the complainant informed on the progress of the investigation; and, without undue delay, inform the complainant of the outcome of the investigation.

22. Links with other policies

This data protection policy is linked to our: freedom of information publication scheme; privacy notices; online safety policy; safeguarding and child protection policy; and policy on the use of photographs and videos.

23. Changes to this policy

We may update this policy at any time. Where appropriate, we will notify data subjects of any material changes to this policy, for example through our privacy notices or via school communication channels.

1. Appendix 1: Personal data breach procedure

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

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

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
- The DPO will alert the executive headteacher and the chair of trustees
- The DPO 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)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

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 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.

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 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. 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

The DPO 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

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

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)

Records of all breaches will be stored on the school's computer system.

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

Actions to minimise the impact of data breaches
We will take the actions set out below to mitigate the impact of different types of data breach, 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 department to recall it.

In any cases where the recall is unsuccessful, the DPO will 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 ensure we receive 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

- Other types of breach that you might want to consider could include:
- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families.