Data Protection Policy

This Data Protection Policy has been approved and adopted in March 2026 and will be reviewed in March 2028

Committee Responsible: Risk & Audit Committee

Contents

1. Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, parents and carers, 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)
- Data Use and Access Act 2025

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education and Generative AI Product Safety Standards

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information. 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, living individual. This may include the individuals: • 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: • 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

TERM	DEFINITION
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 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.
Artificial Intelligence (AI)	Technologies including machine learning, natural language processing (NLP) and large language models (LLMs) that perform tasks normally requiring human intelligence such as generating text, images or predictions.
Profiling	Automated processing of personal data to evaluate certain personal aspects of an individual (e.g. performance, behaviour or interests)
Intellectual Property (IP)	Refers to creations of the mind—inventions, literary/artistic works, designs, symbols, names, images—protected by law, giving creators exclusive rights to use and profit from them.

4. The data controller

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

The Trust is registered with the ICO and maintains a current record of the information it is processing, the legal basis for processing the information and who it is being shared with.

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 knowingly 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.

5.2 Data Protection Officer (DPO)

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 Trust is the first point of contact for individuals whose data the school processes, and for the ICO; they will liaise with the DPO on all reported breaches.

The Trust has appointed an independent Data Protection Officer as its DPO.

The independent Data Protection Officer is Roger Simmons and may be contacted via email at rsimmonsltd@gmail.com and via telephone on 07704 838512.

However, please contact the Trust in the first instance if you have a query regarding any aspect of data protection within the Trust via email: info@xaviercet.org.uk

Each school has a nominated Local Data Protection Officer who operates internally to act as liaison between the Trust DPO, support with staff training and ensure compliance at a local level.

5.3 All staff

All employees, Governors and any other individual handling personal information on behalf of the Trust have a responsibility to ensure that they comply with Data Protection legislation and the Trust's policies.

The Trust ensures that all staff who are involved in processing personal data undertake training as part of their Induction and the Trust provides mandatory data protection training as part of its Safeguarding responsibilities.

Annual data protection training for all staff will include safe and lawful use of AI, risks of bias and inaccuracy, and how to recognise and report incidents involving AI.

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 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

6. Data protection principles

The UK GDPR is based on data protection principles that our Trust 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 1 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 or another person, i.e. 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
- 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 1 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.

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 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.

8. Sharing personal data

We will share data where we have a valid legal reason for doing so. We rely on consent in most other circumstances, however, there are certain circumstances where we may be required to share personal data. 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
- 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 that can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor 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

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency 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.

We will never use personal data in open or public AI platforms unless expressly authorised by the DPO following a Data Protection Impact Assessment (DPIA) and appropriate contractual and technical safeguards.

Where AI tools are used with personal data, the Trust will apply data minimisation, purpose limitation and transparency, and will record the lawful basis for processing in the Record of Processing Activities (ROPA).

Where we choose to rely on consent for an online service (ISS), we will obtain consent from a person with parental responsibility for children under 13, and from the child themselves once they are 13 or over. We will provide clear, age-appropriate privacy information and put in place reasonable checks to verify parental consent where required.

9. Intellectual property

The Trust acknowledges that any original work created by an individual (including staff, pupils, and contractors) constitutes that individual's intellectual property under the Copyright, Designs and Patents Act 1988.

The Trust will ensure that such intellectual property is treated with respect and stored securely as far as is reasonably practicable, in line with our obligations under UK law and data protection principles.

In the interests of furthering education and learning, the Trust may use approved Artificial Intelligence (AI) tools to support analysis, marking, and feedback. This may involve uploading relevant data into secure systems such as Microsoft CoPilot, Notebook LM, Olex etc. which comply with UK GDPR and Trust security standards.

All such use will be subject to appropriate safeguards, including Data Protection Impact Assessments (DPIAs) and adherence to the Xavier AI Policy and ICT Acceptable Use Policy.

10. Subject access requests and other rights of individuals

10.1 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

Subject Access Requests must be submitted in writing, to the relevant school office, details can be found on the trust website, or it can be submitted to info@xaviercet.org.uk

If staff receive a Subject Access Request, they must immediately forward it to the DPO and info@xaviercet.org.uk

10.2 Children and subject access requests

Under the age of 13 years the parent or carer has control of their child's data. Over the age of 13 years, 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 aged 13 years or more, 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 13 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 the Trust under the age of 13 may be granted without the express permission of the pupil.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, most Subject Access Requests from parents or carers of pupils at the Trust school over the age of 13 may not be granted without **the express permission of the pupil.** The presumption of sufficient age is not law in England and a pupil's ability to understand his/her rights will always be judged on a case-by-case basis.

10.3 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. Where identification or clarification of the scope of the request is required, the 'clock' is paused until the identification / clarification has been received.

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 large in volume. 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
- It has been disclosed in the expectation of confidentiality
- 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.

The Data Use and Access Act 2025 clarifies that requests for personal data be reasonable and proportionate. The school's DPO will provide advice and guidance to assist both the data subject and the school in identifying which information meets this reasonable and proportionate standard. This helps prevent a request scope that is overly broad, which could place undue pressure on school resources and delay the timeframe in which the data subject can access the information they require.

Relating to information already held, the law clarifies the principle that the school does not need to send information to the requester, which they already hold or have access to. This confirms there is no requirement to send copies of emails, letters and reports that were communicated by the school to and from the data subject.

If the request is manifestly unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will consider 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.

10.4 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
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that 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)
- 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)

The Trust does not make decisions about pupils, parents or staff that are based solely on automated processing (including profiling) where those decisions produce legal or similarly significant effects. If any such processing is proposed, we will complete a DPIA, ensure meaningful human involvement, and provide individuals with the right to obtain human review, express their views and contest the decision.

Individuals should submit any request to exercise these rights to the DPO, via the info@xaviercet.org.uk. If staff receive such a request, they must immediately forward it to the DPO.

10.5 Redaction and Third-Party Data

Redaction is the process of removing or obscuring personal data, ensuring that the remaining document does not identify individuals, particularly when sharing information with third parties.

In responding to requests for data, the Trust will redact, pseudonymise, or de-personalise information that identifies individuals other than the data subject, unless their consent is obtained or it is reasonable to disclose it. It will also redact any information that has been given with the understanding of confidentiality and information that if disclosed may lead to the harm of an individual.

Appropriate redaction tools will be used to ensure that redacted information cannot be recovered from electronic or paper documents.

The Trust may not redact information that constitutes professional data of staff members acting in their official capacity, unless doing so poses a safety risk.

All documents will be redacted in line with the advice provided by the DPO before being released.

11. Information Security

Information that is confidential but doesn't relate to an individual or individuals includes the following:

- Trust business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations and proceedings
- Any information which, if released, could cause problems or damage to individuals, the public, the Trust or another organisation. This could be personal, financial, reputation or legal damage.

The Trust's information security responsibilities cover the creation, acquisition, retention, transit, use, and disposal of all forms of information. It applies to all employees, Governors, volunteers and staff of service delivery partners who handle information for which the Trust is responsible. It forms the basis

of contractual responsibilities in contracts with Data Processors where reference is made to the Trust's Data Protection and Information Security Policy.

The Trust will maintain the confidentiality, integrity and security of all data ensuring it is gathered, secured, stored, shared and erased in accordance with the data protection regulation. The Trust will review its data protection policies as part of its governance process. It will also check the effective implementation of these policies through the regular Governor led Safeguarding Audits.

Information systems will be checked regularly for technical compliance with relevant security implementation standards.

Operational systems are subjected to technical examination to ensure that hardware and software controls have been correctly implemented.

12. Management Information

The Trust will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information in our schools:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

13. Trust Records

We will create and maintain adequate pupil, staff and other records to meet the Trust's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the Trust, its staff and those who have dealings with our schools; facilitate audit; and fulfil the Trust's legal and statutory obligations.

Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner, in line with the DPO's retention schedule.

14. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the Trust's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that 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, we 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 the Trust's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

15. CCTV

We use CCTV in various locations around the Trust site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

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 DPO.

16. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. This includes remote learning and video conferencing where recordings of lessons/meetings may be taken, processed and stored as evidence.

Primary 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 the pupil.

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.

Secondary schools:

On admission to the school, we will obtain written consent from parents/carers, or pupils aged 18, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

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 (or pupils where appropriate) have agreed to this.

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

- Within school on noticeboards and in school magazines, brochures, newsletters, etc.

- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the Trust's or its schools' websites or social media pages
- As part of lessons or meetings recorded during remove sessions or videoconferencing.

Consent can be refused or withdrawn at any time, including from pupils aged 13+ years. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

We will monitor regularly websites, brochures and display boards to ensure that images of pupils are not used if they have left the school unless specific consent has been provided for the use of the images after the child has left the school.

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.

17. 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 CoPilot, ChatGPT and Google Gemini. The 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.

18. 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)
- 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 matter; 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, 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, type of 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

19. 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, 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 Acceptable use of IT 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)

20. 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.

Data is stored and disposed of in line with the DPO's Retention Schedule.

21. 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, the DPO will report the data breach to the ICO within 72 hours after becoming aware of it. 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
- Personal data being entered onto an unauthorised open-AI platform.

22. 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.

23. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years and approved by the Trust Board.

24. Complaints

The Trust takes any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

The Trust has a dedicated data protection complaints procedure. Complaints about how the school has managed its data protection responsibilities must be acknowledged within 30 days and should be processed without undue delay. The school's Data Protection Complaint Procedure is managed by its DPO. The complaints procedure can be found on the DPO website, RSimmonsLtd.com

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the Local Data Protection Officer (DPO) who will immediately notify the Trust 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
- A Breach Management Form will be completed to gather the facts of the breach, what actions have been taken already and what actions must now be taken to resolve the breach.
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- The DPO will alert the Headteacher and relevant Chair of Governors, or Trustees or the Trust Chief Executive Officer.
- 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, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences
- 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.

- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO and the Headteacher electronically.
- 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
- 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 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, 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)
- 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 set out below the steps we might take to try and 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 Local DPO as soon as they become aware of the error If the sender is unavailable or cannot recall the email for any reason, the Local DPO will ask 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 Local 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 Local DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- If safeguarding information is compromised, the Local DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners