'They will soar on wings like eagles …'

Isaiah 40:31

collaborate | enrich | trust | innovate | aspire |nurture

Multi Academy Trust Policy
Common Trust Policy, Use as Published

Data protection policy

Date adopted by Trust Board: 23/05/2018

Date of Last Review: March 2026

Date of next Review: March 2027

Version	Date	Author	Change Description
1.1	30.05.2024	T Howard	Review of the policy changed to annually
1.2	18.03.2026	T Howard	Updated the DP Policy on the following: • Corrected GDPR principles (7, not 8) • Updated international transfer wording (IDTA/adequacy) • Modern password/NCSC guidance • ROPA (Article 30) included • AI/automated decision-making section added (9.5) • SAR child wording corrected • Retention policy explicitly referenced • International data transfers (8.1) • Updated Photographs and Videos to include children's work (12) • Updated personal breaches (16) • Appendix 2 added - Personal Data Breach Risk Assessment Matrix

Contents

1. Aims

"Peace be within your walls and security within your towers!" Psalm 122:7

Aquila, The Diocese of Canterbury Multi Academies Trust (Hereafter referred to as the Trust) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance UK data protection law.

The basis of this policy is written by the Trust with our value of Collaborate at its heart. Each school will personalise this document to reflect some local operational decisions and processes.

The policy applies to all personal data, regardless of whether it is in paper or electronic format and in all of our member academies and within the Trust central team.

Please note that any reference to a school in this document means an academy supported by the Trust.

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)

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.
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 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.

4. The data controller

Our schools process personal data relating to parents, pupils, staff, governors, visitors and others, and are therefore a data controller.

The Trust 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 The Trust

The Board of Trustees and the Trust Central Team hold a duty to ensure the Trust centrally and each school adheres to the relevant data protection obligations and is making all reasonable steps to secure the data and information held at trust and local level.

5.2 The Local Governing Body

The Local Governing Body (LGB) has overall responsibility for ensuring that their school complies with all relevant data protection obligations.

5.3 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 LGB 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.
The DPO in our Trust is Tracey Howard and is contactable via 01303 905103 DPO@aquilatrust.co.uk

5.4 Head teacher

The Head teacher acts as the representative of the data controller on a day-to-day basis and is required to appoint a senior individual responsible for data protection within their school, who will liaise with the Trusts DPO.

5.5 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 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 7 data protection principles that our academies must comply with.

In accordance with Article 5 UK GDPR, personal data must be:

- Principle 1 – Lawfulness, fairness and transparency
  You must identify valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data. You must ensure that you do not do anything with the data in breach of any other laws. You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. You must be clear, open and honest with people from the start about how you will use their personal data.

- Principle 2 – Purpose limitation

  You must be clear about what your purposes for processing are from the start. You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals. You can only use the personal data for a new purpose if this is compatible with your original purpose, you get consent, or you have a clear obligation to function set out in law.

- Principle 3 – Data Minimisation
  You must ensure the personal data you are processing is:
  adequate – sufficient to properly fulfil your stated purpose;
  relevant – has a rational link to that purpose; and
  limited to what is necessary – you do not hold more than you need for that purpose.

- Principle 4 – Accuracy
  You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact. You may need to keep the personal data updated, although this will depend on what you are using it for. If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible. You must carefully consider any challenges to the accuracy of personal data.

- Principle 5 – Storage Limitation
  You must not keep personal data for longer than you need it.
  You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data. You need a policy setting standard retention periods wherever possible, to comply with documentation requirements. You should also periodically review the data you hold, and erase or anonymise it when you no longer need it. You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data. You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

- Principle 6 – Integrity and Confidentiality

  You must ensure you have appropriate technical and organisational measures in place to protect the personal data you hold.

- Principle 7 – Accountability

  Take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures in place to be able to demonstrate your compliance.

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)
- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit 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.

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.

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 Freedom of Information Publication Scheme and Email Policy

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

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.

8.1 International data transfers

Where personal data is transferred outside the UK, this will be carried out in accordance with UK GDPR. This includes ensuring that appropriate safeguards are in place, such as UK adequacy regulations or the use of the International Data Transfer Agreement (IDTA) or the UK Addendum to Standard Contractual Clauses.

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 contact the Trusts 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.
Personal data about a child belongs to that child, and not the child's parents or carers.
There is no fixed age at which a child is considered able to exercise their data protection rights. Each request will be assessed on a case-by-case basis, taking into account the child's level of understanding and ability to make an informed decision.
Where a child is not considered to have sufficient understanding, a parent or carer may exercise the child's rights on their behalf.

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

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 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 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)
- 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 Automated decision-making, profiling and AI

The Trust does not currently carry out automated decision-making or profiling that produces legal or similarly significant effects on individuals.

The Trust may make use of AI-based tools to support educational or operational activities. Where such tools are used, decisions affecting individuals will not be made solely by automated means. Appropriate human oversight will be maintained at all times.

The Trust will complete Data Protection Impact Assessments (DPIAs) where required and ensure that any use of automated processing complies with UK GDPR.

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. 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.

As an academy we have opted to follow the legal right to free access to a child's educational record for best practice that applies to local authority-maintained schools.

11. CCTV

Some of our schools 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 school.

12. Photographs, videos and children's work

As part of our school activities, we may take photographs and record images of pupils, staff and visitors. We may also display pupils' work, including drawings, written work and other creative outputs.

We will obtain appropriate consent from parents/carers for photographs, videos and the use of pupils' work for communication, educational, marketing and promotional purposes. We will clearly explain how images and work may be used to both parents/carers and pupils.

Where photographs, videos or pupils' work are used, this may include:

- Within school, such as on display boards, in classrooms, and in school publications (e.g. newsletters)
- Outside of school, including by external agencies such as school photographers or local media
- Online, including on the school website or official social media channels

Where pupils' work is displayed, we will minimise the use of identifying personal information where appropriate. For example, first names may be used, but full names or other identifying details will only be included where this is appropriate and consent has been provided.

Consent can be refused or withdrawn at any time. Where consent is withdrawn, we will take reasonable steps to stop further use of the image or work and, where possible, remove it from circulation.

Photographs and videos taken by parents/carers at school events for personal use are not covered by data protection legislation. However, we ask that images or recordings that include other pupils are not shared publicly, including on social media, without the consent of the relevant parents/carers, in line with safeguarding expectations.

Where photographs and videos are used by the school, we will minimise the use of identifying personal information where appropriate. Images will only be used for the purposes outlined in the relevant consent, and consideration will be given to safeguarding and the potential risks of identification.

For further information, please refer to the Trust's Child Protection and Safeguarding Policy.

13. Data protection by design and default

We will implement appropriate technical and organisational measures to demonstrate that data protection is integrated into all of our processing activities, in accordance with the principle of data protection by design and default. This includes:

• Appointing a suitably qualified Data Protection Officer (DPO), and ensuring they have the necessary resources, independence and access to maintain their expert knowledge

• Only processing personal data that is necessary for each specific purpose, and always in line with the data protection principles set out in relevant data protection law (see section 6)

• Completing Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to the rights and freedoms of individuals, including when introducing new systems or technologies. The DPO will advise on this process

• Ensuring that any use of new or emerging technologies, including AI-based tools, is subject to appropriate data protection safeguards. This includes completing DPIAs where required, ensuring lawful processing, and maintaining appropriate human oversight so that decisions affecting individuals are not made solely by automated means

• Integrating data protection into internal documents including this policy, related policies and privacy notices

• Providing regular data protection training to staff and maintaining records of attendance

• Conducting regular reviews and audits to test our data protection measures and ensure ongoing compliance

Maintaining Records of Processing Activities (Article 30 UK GDPR) to document how personal data is processed across the Trust. This includes:

- Making available to data subjects the required information about how their personal data is used (via privacy notices), including the identity and contact details of the Trust and the DPO
- Maintaining internal records of the personal data we hold, including the type of data, categories of data subjects, purposes of processing, recipients, storage arrangements, retention periods and security measures

14. Data security and storage of records

We will protect personal data and ensure it is kept secure against unauthorised or unlawful access, alteration, disclosure or processing, and against accidental loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, will be stored securely when not in use (e.g. in locked cabinets or rooms)
- Papers containing confidential personal data must not be left unattended in areas accessible to others, including desks, staffrooms or display boards
- Where personal data needs to be taken off site, this will be done in accordance with Trust procedures, including appropriate authorisation and secure handling
- Access to systems containing personal data will be controlled through secure authentication methods. Passwords should follow current best practice guidance (for example, using strong passphrases of appropriate length), must not be shared, and should only be changed where there is a suspected or actual security risk. Multi-factor authentication will be used where available
- Encryption will be used where appropriate to protect portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who access or store personal data on personal devices (Bring Your Own Device – BYOD) must ensure appropriate security measures are in place. This includes the use of encryption, secure authentication (such as passwords or biometrics), automatic screen locking, and minimising or avoiding the local storage of personal data wherever possible (see ICT Security Policy)
- Where personal data is shared with third parties, we will carry out appropriate due diligence and ensure that suitable security measures and contractual safeguards are in place (see section 8)

15. Disposal of records

Retention periods for personal data are set out in the Trust Data Retention Policy. Personal data will only be kept for as long as necessary to fulfil the purposes for which it was collected.

Personal data that is no longer required will be disposed of securely. Personal data that is inaccurate or out of date will also be securely deleted or destroyed where it is not necessary to retain or update it.

This may include the secure shredding or incineration of paper records, and the secure deletion or overwriting of electronic files. Where third parties are used to dispose of records on the Trust's behalf, we will ensure that appropriate due diligence is carried out and that they provide sufficient guarantees of compliance with data protection law.

16. Personal data breaches

The school will make all reasonable endeavours to prevent personal data breaches.

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

All personal data breaches will be risk assessed using a standard risk-based approach, taking into account the likelihood and severity of potential harm to individuals. This assessment will inform decisions on containment, mitigation and whether notification to the ICO and/or affected individuals is required. Where appropriate, we will report the data breach to the ICO within 72 hours of 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

17. 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.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

The Local Governing Body will make arrangements to monitor the schools' approach to GDPR and compliance with this policy.

19. Links with other policies

This policy should be read in conjunction with the following Trust policies:

- Data Retention Policy
- ICT Security & Email Policy
- Freedom of Information Publication Scheme
- Child Protection and Safeguarding Policy
- ICT Acceptable Use policy

Appendix 1: Personal data breach procedure

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

Reporting a breach
On discovering or causing a personal data breach, or suspected breach, any staff member, governor or data processor must notify the Data Protection Officer (DPO) immediately upon becoming aware of it. This should be done by email to DPO@aquilatrust.co.uk or in person.

Investigation and initial response
The DPO will investigate the report and determine whether a personal data breach has occurred. This will include considering 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 individuals

Staff and governors are required to cooperate fully with any investigation, including providing access to relevant information and responding to questions. This process will not, in itself, be treated as a disciplinary investigation.

Where a breach is confirmed, or likely to have occurred, the DPO will inform the Headteacher and the Chair of Governors.

Containment and risk assessment
The DPO will take all reasonable steps to contain the breach and minimise any impact on individuals. Relevant staff members or data processors must support this process where required, and external advice (e.g., from IT providers) will be sought where appropriate.

All personal data breaches will be risk assessed using a risk-based approach, taking into account the likelihood and severity of potential harm to individuals. This assessment will inform decisions on containment, mitigation and whether notification to the ICO and/or affected individuals is required.

Recording the breach
The Trust will maintain a record of all personal data breaches (the breach register), regardless of whether they are reported to the ICO. This record will include:

- The facts and cause of the breach
- The likely and actual effects
- The action taken to contain the breach and prevent recurrence
- The rationale for decisions made

Records of all breaches will be securely stored on the Trust's designated systems.

Reporting to the ICO
Where required, the DPO will report the breach to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it.
The report will include:

- 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 breach

- A description of the measures taken, or proposed, to address the breach and mitigate its effects

Where full details are not yet available, the DPO will provide the information available within 72 hours and submit further details as soon as possible, explaining any delay.

Communication with affected individuals
Where required, the DPO will notify affected individuals without undue delay. This communication will be clear and in plain language, and will include:

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

The DPO will also consider whether relevant third parties (e.g., police, insurers, banks) should be notified to help mitigate potential harm.

Review and learning
Following a breach, the DPO and Headteacher will meet as soon as reasonably possible to review the incident and identify actions to prevent recurrence.

The DPO and Headteacher will also review breach records periodically to identify trends or patterns and take appropriate action to reduce the risk of future breaches.

Actions to minimise the impact of data breaches
The Trust will take appropriate steps to mitigate the impact of different types of data breaches, particularly those involving sensitive personal data. These actions will be reviewed and updated as necessary following any incident.

Example: Sensitive information disclosed via email (including safeguarding records)

- The sender must attempt to recall the email immediately upon becoming aware of the error
- Any recipient of personal data sent in error must inform the sender and the DPO immediately
- Where recall is not possible, the DPO will work with ICT support to attempt removal of the data from systems (retaining a copy if required for evidence)
- The DPO may contact unintended recipients to request deletion of the information and confirmation that it has not been shared or retained
- The DPO will seek written confirmation from recipients where appropriate
- The DPO will take reasonable steps to ensure the information has not been made publicly available and request removal if necessary
- Where safeguarding information is involved, the DPO will inform the Designated Safeguarding Lead and consider whether safeguarding partners should be notified

Other examples of potential breaches

- Publication of non-anonymised pupil data on a website
- Sharing of sensitive pupil or staff information with unauthorised individuals
- Loss or theft of a device containing personal data
- Cyber incidents affecting third-party systems (e.g., payment providers)
- Sending reports or letters to the wrong recipient

Appendix 2 - Personal Data Breach Risk Assessment Matrix

Step 1: Assess Likelihood of Harm

Score	Likelihood	Description
1	Low	Unlikely to result in harm (e.g., quickly contained, limited exposure)
2	Medium	Possible risk of harm (e.g., some data exposed, limited sensitivity)
3	High	Likely to result in harm (e.g., sensitive data widely exposed)

Step 2: Assess Severity of Harm

Score	Severity	Description
1	Low	Minimal impact (e.g., inconvenience, no sensitive data)
2	Medium	Moderate impact (e.g., distress, minor financial or reputational risk)
3	High	Significant impact (e.g., safeguarding risk, identity theft, serious distress)

Step 3: Calculate Risk Rating

Risk Score = Likelihood × Severity

Severity ↓ / Likelihood →	**1 (Low)**	**2 (Medium)**	**3 (High)**
1 (Low)	1	2	3
2 (Medium)	2	4	6
3 (High)	3	6	9

Step 4: Risk Outcome & Required Action

Risk Score	Risk Level	ICO Notification	Notify Individuals	Action Required
1–2	Low	Not required	Not required	Record only
3–4	Medium	Consider	Consider	Record + mitigate
6–9	High	Required	Likely required	Immediate action + report