Abbey Multi Academy Trust

Policies & Procedures

Data Protection Policy

How we use, manage and protect personal information

Approved on	18 March 2026
Approved by	Abbey MAT Board of Trustees
Next review due	31 March 2027

In Partnership to
Educate, Nurture and Empower

Contents

Data Protection Policy

1. Aims and scope

Abbey Multi Academy Trust (the Trust) is committed to protecting personal information and handling it lawfully, fairly and transparently. This policy explains how the Trust meets its obligations under UK data protection law and how personal data is managed across the Trust and its academies.

This policy applies to all personal data processed by the Trust, including information relating to pupils, parents, staff, governors, volunteers and other individuals, regardless of whether it is in paper or electronic format.

This policy is available via the Trust website, each school website, and on request.

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 UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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.

The policy reflects updates introduced by the Data (Use and Access) Act 2025 from February 2026, including changes to subject access request time limits, recognised legitimate interests, compatible further processing, and enhanced regulatory powers.

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 .
'Sensitive 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 accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The Trust processes personal information relating to pupils, staff, governors, visitors and others, and, therefore, is a data controller. The Trust retains accountability as data controller and delegates operational data protection responsibilities at academy level to the Principal/Headteacher.

The Trust is registered as a data controller and pays an annual fee to the Information Commissioner's Office (ICO), as legally required.

5. Roles and responsibilities

This policy applies to all staff employed by our Trust, as well as all trustees, local governors and other volunteers, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Trust board and local governing boards

The Trust board has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations, including ensuring appropriate policies and processes are in place. Oversight of compliance within individual academies is delegated to the relevant local governing board.

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 Trust and its academies processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Kerry Weatherill, Head of Governance & Compliance, and is contactable via email to dpo@abbeytrust.org.

Principal, Headteacher or Academy Leader

The Principal, Headteacher, or Academy Leader acts as the representative of the data controller on a day-to-day basis within their school.

All staff and volunteers

Staff and volunteers 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 schools 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 Trust aims to comply with these principles.

7. Collecting personal data

Lawfulness, fairness and transparency

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

- The data needs to be processed so that we can **fulfil a contract** with the individual, or the individual has asked us to take specific steps before entering into a contract
- The data needs to be processed so that we can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, e.g. to protect someone's life
- The data needs to be processed so that the Trust, 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 Trust and its academies (where the processing is not for any tasks the Trust 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**

In certain circumstances permitted by data protection law, the Trust may rely on **recognised legitimate interests** as a lawful basis for processing personal data. Where this applies, the Trust will ensure that processing remains necessary, proportionate and consistent with the rights and freedoms of individuals.

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.

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.

Where the Trust intends to use personal data for a purpose other than that originally explained, we will consider whether the new purpose is compatible with the original reason for collecting the data, in accordance with data protection law.

Where required, we will provide individuals with updated privacy information before further processing takes place. Consent will be obtained where this is the appropriate lawful basis. Further processing may take place where it is considered compatible with the original purpose or otherwise permitted by data protection legislation.

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

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Retention Schedule and Records Management Policy.

Further information about how and why we process personal data can be found in our 'Privacy Notices' available to download from the websites of the Trust and its academies or on request from the DPO or school offices.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- 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 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, 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.

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

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Further information about how and why we may share personal data can be found in our 'Privacy Notices' available to download from the websites of the Trust and its academies or on request from the DPO or school offices.

9. Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust and its academies 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 is not 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 (either by letter or email) and include:

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

To make it easier for individuals to request information held about them by the Trust and its academies, the Trust has published a Subject Access Request form which can be downloaded from the website of all Abbey Multi Academy Trust schools or on request from the school office or Data Protection Officer. Requests made in other formats will still be accepted.

If staff receive a subject access request they must immediately forward it to the DPO to be recorded on the register of all school data subject access requests.

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.

In our primary schools:

Children aged 12 or under 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 primary schools 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.

In our secondary schools:

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 our secondary schools may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests:

- We may ask the individual to provide 2 forms of identification
- We may contact the individual via phone to confirm the request was made
- We will respond without undue delay and within one month of the relevant time period commencing. The relevant time period begins once the Trust has received all information required to process the request, including confirmation of identity or authority to act where necessary.
- Where further clarification or further information is required, we may pause the time limit ("stop the clock") until the required information has been received
- We may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this without undue delay and within one month, and explain why the extension is necessary
- Will provide the information free of charge

Refusing requests

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 do not 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 which takes into account administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

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

If the Trust refuses a request, we will provide a clear explanation of the reasons for the decision, explain how to raise a concern through the Trust's Data Protection Complaints Process, and inform the individual of their right to complain to the Information Commissioner's Office (ICO).

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, or object to the processing of it (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
- Object to 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. Where an individual wishes to raise a concern about how their personal data has been handled, this should be done through the Trust's Data Protection Complaints Process, including the online data protection complaint form available via the Trust website.

10. Parental requests to see the educational record

Parents As an academy trust, there is no automatic parental right of access to a child's educational record.

Where a parent or carer requests access to information about their child, the Trust may consider the request as a Subject Access Request (SAR) under data protection law. Requests will be assessed on a case-by-case basis, taking into account parental responsibility, the age and understanding of the child, safeguarding considerations, and the rights of others.

Access may be limited or refused where an exemption applies, including where disclosure could cause serious harm to the physical or mental health of the pupil or another individual, or where disclosure would adversely affect the rights and freedoms of others.

Requests should be submitted to the Data Protection Officer. If a parent or carer is dissatisfied with a decision, they may raise a concern through the Trust's Data Protection Complaints Process.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils may use finger prints to receive school dinners instead of paying with cash in some of our schools), 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 school will get written consent from at least one 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 school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, we will provide pupils with a card to allow them to make payment for school dinners at each transaction if they wish.

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 school'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 school will delete any relevant data already captured.

12. CCTV

In many of our schools, we use CCTV in various locations around the school 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 school's site manager in the first instance.

13. Photographs and videos

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

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

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

- Within school on notice boards and in school magazines, 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

Where consent is required for us to use photographs or videos, consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video as soon as is reasonably practicable 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.

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

Copilot. 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 2.

15. Data protection by design and default

We have 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 privacy impact assessments (DPIA) where our 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
- Rolling out data protection training and updates for all staff and volunteers in response to changing data protection legislation and data privacy risks
- 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 schools 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 lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 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 online safety policy, ICT policies and acceptable use agreements)
- 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 our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

The Trust 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 2.

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. Recording of telephone calls

Telephone calls with our schools may be recorded for training, quality assurance and monitoring purposes, as well as to help us investigate concerns, resolve disputes, and improve the services we provide.

Where call recording takes place, individuals will be informed at the start of the call or through an appropriate notification message. Recordings will be handled in accordance with data protection law, stored securely, and retained only for as long as necessary in line with the Trust's retention schedule.

Access to call recordings will be limited to authorised staff where there is a legitimate reason to review them. Recordings may be used where necessary for safeguarding, complaint investigations, or legal and regulatory compliance.

20. Training

All staff, governors and other volunteers 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.

21. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually, updated in accordance with any changes to legislation, and approved by the Trust Board.

22. Links with other policies

This data protection policy is linked to our:

- Data Protection Complaints Policy
- Freedom of Information Publication Scheme and Policy

- Records Management Policy
- Record Retention Schedule
- Privacy Notices
- CCTV Policy
- Acceptable Use Policy
- Data Protection Handbook (guidance issued to staff)

Review frequency: Annually

Policy owner: Data Protection Officer

Appendix 1: Subject Access Request Form

Subject Access Request (SAR) Form

Ask for copies of your personal information

You have the right to ask for copies of the personal information we hold about you. This is called a Subject Access Request (SAR). You do not have to use this form to make a request, but it helps us understand what information you need so we can respond as quickly and accurately as possible.

Submitting your request: Email your request to the Trust's Data Protection Officer to dpo@abbeytrust.org or post it to: *Subject Access Requests, Abbey MAT, Moyes Centre, Bishops Way, Seacroft, Leeds, LS14 6NU.*

What happens next?: We may contact you if we need clarification or further information. We will respond without undue delay and normally within one month of the start of the relevant time period. The relevant time period begins once we have received all the information we need to process your request (for example proof of identity or authority to act). If the request is complex, we may take up to three months and will let you know if more time is needed and why.

Section 1: Your details

Please provide your contact details so we can respond and contact you if we need to

Full name	
Email address	
Contact number	
Home address	

Section 2: Details of the person you are requesting information for

If you are acting for someone else, please provide their details

Full name	
Your relationship to them	
Email address	
Contact number	
Home address	

Authority to act
If you are making this request for someone else, we may need evidence that you have permission or legal authority to act for them (for example written consent). Please provide details below. Please note we may not be able to begin processing your request until this information is received.

Section 3: What information are you requesting?

Please tell us what personal information you are looking for. Being specific helps us respond more quickly.

Describe your request
Please describe the information you would like to receive. Try to be as clear and specific as possible about what you are looking for, including the type of information, where it may be held, or who it relates to. This helps us identify and provide the information you need more quickly.
Date range (if known)
If you know the dates relevant to your request, please tell us the time period you would like us to search. This could include specific dates or an approximate date range, which will help us identify the correct information more quickly.
Further information to help us locate the information
Please include any additional information that may help us locate the information you are requesting. This might include previous names or aliases, date of birth, staff or pupil number, year group or school attended, or any relevant reference numbers. Providing as much detail as possible will help us respond more quickly and accurately.

How would you like us to respond to your request?
☐ Email ☐ Post ☐ Other (please specify below) *If you need any adjustments (for example large print), please tell us:*

Email your request to the Trust's **Data Protection Officer** to dpo@abbeytrust.org or post it to: *Subject Access Requests, Abbey MAT, Moyes Centre, Bishops Way, Seacroft, Leeds, LS14 6NU.*

Appendix 2: Personal Data Breach Procedure

Abbey MAT Personal Data Breach Procedure

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

Procedure to be followed in the event of a breach or potential breach

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by email to dpo@abbeytrust.org.

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

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal/Headteacher.

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).

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 and the individuals affected using the ICO's self-assessment tool.

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 in the Trust's data breach log.

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/trust'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/trust is required to communicate with individuals whose personal data has been breached, the DPO will ensure that the school/trust 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)

Records of all breaches will be stored in the Trust's data breach log.

The DPO and Principal/Headteacher or relevant Head of Service will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

The DPO and Principal/Headteacher or relevant Head of Service will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We have set out some examples below of action that we will take 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, we will ask the ICT department to attempt to recall it from external recipients and remove it from the trust's email system (retaining a copy if required as evidence)

In any cases where the recall is unsuccessful, we will consider whether it is 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.

We will request that staff ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

We 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, we will inform the designated safeguarding lead and discuss whether the school should inform any of its local safeguarding partners.

Personal information accidentally being published on the school website (e.g. named pupil premium interventions, residential address details, etc.)

Should any staff member become aware that personal or special category data may have been accidentally published on a school website, they must immediately inform the DPO, Head of ICT, and the Website Manager as soon as they become aware of the potential error to ensure that action can be taken at the earliest opportunity to remove the information from the website.

The Head of ICT and the Website Manager together will ensure that the information is immediately removed and that it cannot be linked to or otherwise accessed or retrieved, for example, in search engine results.

We will ensure that an internet search is carried out to check that the information has not been made public elsewhere; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

On identifying the source of the breach following the DPO's investigation, the Head of ICT and Website Manager will ensure that procedures for publishing information to school websites are reviewed and action taken to prevent a similar breach from occurring in the future. This may include identifying training needs, further restricting permissions for publishing information, etc.

A laptop or device containing non-encrypted sensitive personal data being stolen or hacked

Where an individual believes that a laptop or device containing or otherwise allowing access to personal data may have been lost, stolen, hacked, or accessed by unauthorised persons, they must take immediate personal action to contain the loss in addition to notifying the DPO, regardless of whether the data is encrypted or not. This must include ensuring that suspected theft or loss is reported to the Police at the earliest opportunity in order to increase the likelihood of the device being recovered.

The individual must immediately provide to the DPO details of the categories and extent of the personal data contained on the device itself and with details of any programmes, systems, apps, or websites through which personal data may be accessed using the device. For the avoidance of doubt, this must include details of any websites or apps allowing access to personal data where log in credentials may have been stored either in part or in full (for example, to keep a user logged in or to

provide the username) even if the user believes that the information has been cleared.

The individual must immediately change the passwords to all such systems and services and notify the DPO as soon as this has been completed. The individual must also retrieve any audit or access logs which may allow for any instances of unauthorised access to be identified. They must seek the advice and support of the Trust's Head of ICT in doing this, particularly with regard to school/ Trust based or hosted systems, and immediately notify the DPO of their findings. This will allow the DPO to advise on any possible action that may be taken to further contain the data breach.