Waterton
Academy Trust

Data Protection Policy

watertonacademytrust.org

Contents

1. Aims

Waterton Academy 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 with the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK GDPR and DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO). 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 code of practice 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, 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

Waterton Academy Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.
The Trust and member academies are 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 Waterton Academy Trust including volunteers, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Strategic Board

The Trust Strategic Board has overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will provide an annual report of their activities directly to the Strategic 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 processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.
Our DPO is Mr M Berry and is contactable via
dataprotection@watertonacademytrust.org

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school/trust 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 United Kingdom.
    - 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 data protection principles that our Trust and associated schools must comply with are;

- 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 and its associated schools aim to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

Waterton Academy Trust 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 freely given clear **consent**

For special categories of personal data, Waterton Academy Trust will also meet one of the special category conditions for processing which are set out in Article 9 of UK GDPR and the provisions of the Data Protection Act 2018.
Whenever we collect personal data pertaining to an individual, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

Waterton Academy Trust will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Data Retention 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
- 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.

Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should ideally be submitted in writing, either by letter or email to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO. Subject Access Requests may also be made by a data subject (or their representative) verbally or through social media.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to

their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 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 our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis. Children aged under 13 will never be able to submit a request however the permission to disclose data to parents of a pupil aged 13 and above will only be required when that pupil is deemed to have sufficient capacity.

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 calendar month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months (90 calendar days) of receipt of the request, where a request is complex or numerous requests have been received pertaining to the same data subject. We will inform the individual of this within 1 calendar month and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child including parental orders

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

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

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of legitimate interests
- Request a copy of agreements under which their personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- 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.

10. Parental requests to see the educational record

Please contact the Headteacher in the first instance. Please note that Regulation 5 of The Education (Pupil Information)(England) Regulations 2005 does not apply to academies and requests to accept a pupil educational record will often be considered to be a subject access request in line with UK GDPR / DPA 2018.

11. CCTV

Waterton Academy Trust uses CCTV in various locations around the school sites 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 DPO (see Section 5).

12. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional

materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.
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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our child protection, Photography Policy and safeguarding policy for more information on our use of photographs and videos.

13. 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 privacy impact assessments where processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-

party recipients, how and why we are storing the data, access controls, retention periods and how we are keeping the data secure

14. 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 to change their passwords at regular intervals
- The use of 2 form factor authentication whereby externally held (cloud technologies) sensitive material is accessed by authorised staff.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who access personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see Waterton Academy Trust's Code of Conduct for Employees).
- 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)

15. Disposal of records

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

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

The trusts data retention policy sets out detailed information on how data is managed across the trust.

16. Personal data breaches

The Trust and its associated schools will make all reasonable endeavours to ensure that there are no personal data breaches.

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

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Protection of Biometric Information

The Trust will notify each parent of a pupil under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system.

Parents/carers, students, staff members and other relevant adults have the right to not take part in the school's biometric system(s).
The name and contact details of the student's parents/carers will be taken from the school's admission register.

Where the name of only one parent/carer is included on the admissions register, the Headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent/carer.

The Trust will complete a Biometric Data Protection Impact Assessment ("DPIA") for the use of biometric data and will update this as appropriate when the system is upgraded or significantly modified.

Consent of Pupil's, Parents & Carers
As long as the child or a parent does not object, the written consent of only one parent will be required for a school or the Trust to process the child's biometric information. A child does not have to object in writing, but a parent's objection must be written.

The Trust will not need to notify a particular parent or seek his or her consent if the school is satisfied that:

- The parent cannot be found, for example, his or her whereabouts or identity is not known;
- The parent lacks the mental capacity to object or to consent;

- The welfare of the child requires that a particular parent is not contacted, for example where a child has been separated from an abusive parent who is not to be informed of the child's whereabouts; or
- Where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.

Where neither of the parents of a child can be notified for one of the reasons set out above (which would mean consent cannot be obtained from either of them), section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent:

- If the child is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained.
- If the paragraph above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing).

In the event that the Trust or an individual school is unable to obtain the appropriate consent as detailed above it will not process any biometric data.
If a parent/carer has objected in writing to such processing, the Trust will ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system even if another parent has given written consent.
Pupil's will be informed that they can object or refuse to allow their biometric data to be collected and used via a letter.

If a pupil under 18 objects or refuses (verbally or nonverbally) to participate (or to continue to participate) in activities that involve the processing of their biometric data, the school and Trust will ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system.

A pupil's objection or refusal overrides any parental consent to the processing.
Parents/carers and students can object to participation in the school's biometric system(s)or withdraw their consent at any time. Where this happens, any biometric data relating to the student that has already been captured will be deleted.

Consent of Staff & Other Adults
Where staff members or other adults use the school's biometric system(s), consent will be obtained from them before they use the system. Staff and other adults can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative Arrangements

Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s). In the event that a pupil or parent does not provide consent then alternative provisions will be made for the pupil to obtain fair access to the service to which the biometric data pertained e.g. the pupil will continue to be able to pay for school meals using cash or a PIN code as opposed to via fingerprint.

The alternative arrangements will ensure that pupils do not suffer any disadvantage or difficulty in accessing services/premises etc. as a result of their not participating in an automated biometric recognition system. Likewise, such arrangements will not place any additional burden on parents whose children are not participating in such a system.

18. 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.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary, **every 2 years** and shared with the board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Data Retention Policy
- Child Protection and Safeguarding Policy
- Acceptable use agreement (within employee code of conduct)
- Protection of Biometric Information of Children in Schools Policy

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen

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

- The DPO will alert the headteacher and the chair of governors and where appropriate, the CEO and Chair of the Trust Board.

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored electronically on the trust's secure drive

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned

  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

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

- The DPO will document each breach and near miss, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
  - Records of all breaches will be stored on the trust's secure drive

- The DPO and headteacher/CEO 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
Waterton Academy Trust will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*

- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Document Detail	
Document Name:	Data Protection Policy
Version:	5
Chief Officer Signature:	
Effective From:	01/04/2025
Approved by:	D Dickinson
Approval Meeting Reference:	18/03/2025
Next Review Date:	01/01/2027

Version Control

Version	Date	Author	Change/Reference
1	Jan 2017	V Collins	
2	Feb 2020	V Collins	Changed in line with legislation. Some responsibilities changed to DPO.
3	Jun 2022	V Collins / I Burns	Updated references to legislation Updated referral to other Trust policies Updated DPO details Updated in line with operational changes e.g 2FA Additional information and detail in reference to DPA provided.
4	Jul 2024	M Bretherton	Removed reference to external DPO and changed the name of the Trust DPO
5	Jan 2025	M Bretherton	Expanded and clarified the policy on biometric data collection and use, including parental and pupil consent requirements and alternative arrangements for those who opt out. Added specific circumstances under which consent is not required (e.g., if a parent cannot be contacted or has limited capacity). Reinforced the use of two-factor authentication (2FA) for accessing sensitive cloud-based data. Emphasised data encryption requirements for portable devices. Updated procedures for handling SARs, including timeframes for responding, verification methods, and exceptions where data may not be disclosed. Expanded the breach response procedures, including detailed steps for containment, assessment, and reporting breaches to the ICO within 72 hours if necessary. Added actions to minimise the impact of breaches involving sensitive information (e.g., recalling emails). Clarified consent requirements for using images of pupils, ensuring alignment with safeguarding and privacy considerations. Reinforced compliance with the Trust's Data Retention Policy for securely disposing of outdated or inaccurate data. Confirmed that all staff and governors receive data protection training during induction and as part of ongoing CPD when relevant updates occur.