



Data Protection Policy

Policy | 2026-27

Policy name	Data Protection Policy
Version	1.0
Status	Live
Author	Gareth Kyle, Academy Business Leader
Approval body	Resources, Audit & Risk Committee
Date approved	7 October 2026
Review cycle	Annual
Next review due	Autumn 2027
Published on	Both (Trust website and National College)
Applies to	Trust-wide

Revision history

Version	Date	Author	Summary of change
Prior	Not recorded	Not recorded	Previous Data Protection Policy, review due December 2025 (policy register).
0.1	September 2026	Gareth Kyle	Redrafted on The School DPO Service model and updated for the Data (Use and Access) Act 2025.
1.0	October 2026	Gareth Kyle	Checked against the SBM template v25.1 and the IRMS retention schedule. Trust terms corrected. Retention table moved to a separate Records Retention Schedule. Submitted to the Resources, Audit & Risk Committee.

Index

The Policy

1. Aims.....	3
2. Legislation and guidance.....	3
3. Definitions.....	3
4. The data controller	4
5. Roles and responsibilities.....	4
6. Data protection principles.....	5
7. Collecting personal data	6
8. Sharing personal data	8
9. Subject access requests and other rights of individuals	9
10. CCTV	11
11. Photographs and videos.....	11
12. Data protection by design and default.....	12
13. Artificial intelligence (AI).....	12
14. Data security and storage of records	13
15. Disposal of records.....	14
16. Personal data breaches	14
17. Training.....	15
18. Monitoring arrangements	15
19. Data protection complaints.....	15
20. Links with other policies and documents.....	15

Appendices

Appendix 1: Personal data breach procedure.....	17
Appendix 2: Records retention schedule	19

1. Aims

- 1.1** The Cedars Academy Trust (the Trust) aims to ensure that personal data about pupils, parents and carers, staff, trustees, visitors and other individuals is collected, used, shared, stored and disposed of lawfully and securely.
- 1.2** This policy applies to all personal data, whether held electronically, on paper or in another format. It covers both of the Trust's sites, Cedars Academy: Low Fell and Cedars Academy: High Heworth, together with off-site activities and remote working undertaken on the Trust's behalf.

2. Legislation and guidance

- 2.1** This policy reflects the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.
- 2.2** It takes account of guidance published by the Information Commissioner's Office (ICO), including guidance on individual rights, information sharing, surveillance systems, personal data breaches and data protection complaints. It also takes account of the Department for Education's guidance on generative artificial intelligence in education.
- 2.3** As an academy, the Trust is not subject to the separate parental right of access to educational records under regulation 5 of the Education (Pupil Information) (England) Regulations 2005. Requests for access to a pupil's personal data will be considered under the UK GDPR and the procedures in section 9. This does not affect other applicable duties to provide information to parents and carers.
- 2.4** On 30 September 2026 the Information Commissioner's Office became the Information Commission. It is still known as the ICO, and in this policy "the ICO" means the Information Commission.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living 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.

Term	Definition
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

- 4.1** The Cedars Academy Trust is the data controller for personal data processed for the academy's activities across both sites.
- 4.2** The Trust determines why and how this personal data is processed and maintains its registration with the ICO.

5. Roles and responsibilities

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

- 5.1 Trust Board.** The Trust Board has overall responsibility for ensuring that the Trust complies 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 the Trust's 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 data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

The Trust's DPO service is The School DPO Service (office@schoolDPOservice.com, 01727 572448). Its responsibilities are set out in the Trust's service agreement. The DPO provides independent advice and monitors compliance. Responsibility for compliance remains with the Trust as data controller.

- 5.3 Leadership and operational responsibility.** The co-headteachers are responsible for implementing this policy across their areas of responsibility and ensuring that staff follow the Trust's data protection procedures.

The Trust's internal data protection contact is the Academy Business Leader, supported by the Data and Office Manager (enquiries@cedarstrust.org.uk, 0191 487 4595). The internal contact co-ordinates requests, incidents and compliance activity with the DPO.

Staff must immediately report suspected personal data breaches, and forward requests to exercise data protection rights, to the internal contact and the DPO. If the Academy Business Leader is unavailable, staff must notify the Data and Office Manager or, if neither is available, their site Headteacher, without delay.

- 5.4 All staff.** Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the 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 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
- Completing data protection and cyber security training each year (section 17)

6. Data protection principles

- 6.1** The UK GDPR is based on data protection principles that the Trust must comply with.

- 6.2** 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

6.3 This policy sets out how the Trust aims to comply with these principles. The Trust is responsible for complying with these principles and for maintaining appropriate records and other evidence to demonstrate its compliance.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency. We will identify and document an appropriate lawful basis before processing personal data. Depending on the purpose and circumstances, the available bases are:

- Consent.
- Processing necessary for a contract with the individual, or steps requested by them before entering into a contract.
- Compliance with a legal obligation.
- Protection of someone's vital interests.
- Performance of a task in the public interest or exercise of official authority.
- Legitimate interests, where the individual's interests and rights do not override those interests.
- Recognised legitimate interest, where the specific statutory conditions are met.

We will not rely on legitimate interests or recognised legitimate interest for processing undertaken in the performance of our tasks as a public authority. We will seek DPO advice where the appropriate basis is unclear.

Where consent is used, it must be freely given, specific, informed and unambiguous, and individuals must be able to withdraw it.

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.

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 Records Retention Schedule (Appendix 2).

7.3 Privacy notices. The Trust publishes privacy notices for pupils and parents and carers, for the workforce, and for users of the Trust website, on the Trust website. They are reviewed each year.

8. Sharing personal data

- 8.1** We will share personal data only where there is an appropriate lawful basis and the sharing is necessary and proportionate. Where special category or criminal offence data is involved, we will also meet the additional legal conditions.
- 8.2** Consent is not required for every disclosure. Where we rely on another lawful basis, we will explain the sharing through our privacy information unless a lawful exception applies.
- 8.3** Circumstances in which we may share information include:
- 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 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
- 8.4** We will also share personal data with law enforcement and government bodies where we are legally required to do so.
- 8.5** 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.
- 8.6** Where we transfer personal data internationally, we will do so in accordance with data protection law.
- 8.7** **Suppliers who process personal data for us.** When a supplier processes personal data on the Trust's behalf (a data processor), the member of staff arranging the contract must make sure, with the internal data protection contact, that:
- the checks made on the supplier's security are recorded and kept;
 - the written contract meets the requirements of UK GDPR Article 28;
 - the supplier will not pass the work to another processor without the Trust's written agreement;
 - the supplier will help the Trust with personal data breaches, rights requests and enquiries from the ICO; and
 - the data will be returned or securely destroyed when the contract ends.

The DPO will advise where the processing is likely to be high risk (section 12).

- 8.8** **Sharing information in a medical or mental health emergency.** Data protection law allows the Trust to share personal information in an urgent or emergency situation, including to help prevent loss of life or serious physical, emotional or mental harm. Where there is a risk of serious harm to a member of staff or to others, the Trust will share necessary and proportionate information without delay with the emergency services or health professionals. It may also share necessary and proportionate

information, which may be more limited, with the person's next of kin or emergency contact. The workforce privacy notice explains this.

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 Trust 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

Staff must record when a request was first received and forward it immediately through the reporting arrangements in section 5.3. A request does not need to mention data protection legislation or use a particular form. School holidays and internal referral arrangements do not, by themselves, extend the response deadline.

9.2 Children and subject access requests. The right of access belongs to the child. We will assess each child's understanding of their rights and the implications of the request, providing appropriate communication support.

We will not determine competence solely by age, diagnosis or special educational needs. There is no fixed age threshold of 12 in England.

Where a child is competent, we will normally respond to them or a representative they have authorised. Where they are not competent, a person with parental responsibility may usually act on their behalf, unless there is evidence that doing so would not be in the child's best interests.

Before disclosing information, we will consider the child's wishes, any relevant court orders, confidentiality, safeguarding concerns and the consequences of disclosure or

non-disclosure. Parental responsibility does not automatically entitle someone to all information held about a child.

The assessment and reasons for the decision will be recorded, with DPO and Designated Safeguarding Lead advice where appropriate.

For pupils aged 18 or over, we will establish the authority of anyone seeking to act on their behalf and obtain advice where capacity or representation is uncertain.

9.3 Responding to subject access requests. We will:

- Make necessary and proportionate checks of identity and authority to act.
- Respond without undue delay and normally within one calendar month. Where necessary identity or authority evidence is requested, the period begins when it is received.
- Extend the deadline by up to two further months where justified by complexity or the number of requests, explaining the extension within the initial month.
- Seek clarification only where reasonably required. Any lawful pause and revised deadline will be recorded; requesters will not be required to narrow their request.
- Conduct reasonable and proportionate searches.
- Normally provide the information free of charge, securely and in an accessible format.

The DPO will advise on any restriction, redaction or exemption, including information about other people. Decisions will be assessed individually and documented.

Where a request is manifestly unfounded or excessive, we may refuse it or charge a reasonable administrative fee where legally permitted. A fee may also apply to additional copies.

Where we refuse all or part of a request, we will explain the decision as legally required and identify the rights to complain to the Trust and the ICO and seek a judicial remedy.

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
- Exercise the safeguards available under data protection law in relation to significant decisions based solely on automated processing, including obtaining human intervention, making representations and contesting the decision where applicable
- 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 internal data protection contact or the DPO (section 5). If staff receive such a request, they must forward it immediately through the reporting arrangements in section 5.3.

10. CCTV

- 10.1** We use CCTV at both sites to support the safety and security of pupils, staff, visitors and property. Its use will comply with UK data protection law and relevant ICO guidance.
- 10.2** Access to footage will be restricted to authorised individuals. Retention periods are set out in the Records Retention Schedule and reflected in system settings. Footage required for an incident, investigation or legal matter may be retained beyond the routine period where necessary and justified.
- 10.3** 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.
- 10.4** Any enquiries about the CCTV system should be directed to the DPO.
- 10.5** The CCTV Policy sets out how the system is operated, who may view footage and how requests for footage are handled.

11. Photographs and videos

- 11.1** As part of the Trust's activities, we may take photographs and record images of individuals at both sites.
- 11.2** Where we rely on consent to use photographs or videos, we will explain the intended purposes and audiences and record the choices made. These may include internal displays, the parent communication platform, the Trust website, social media and external publicity.
- 11.3** Consent will be obtained from the pupil where they have sufficient understanding to give it, or from an appropriate parent or carer where they do not. Arrangements for adult pupils will reflect their own rights and any lawful authority for another person to act on their behalf.
- 11.4** Staff must check the relevant permissions and any safeguarding restrictions before using or sharing an image.
- 11.5** Any photographs and videos taken by parents/carers at Trust events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.
- 11.6** Consent may be refused or withdrawn at any time. Withdrawal will not affect the lawfulness of earlier use. Where consent is withdrawn, we will stop further use for the relevant purpose and take reasonable steps to remove images from channels under our control. We will explain any practical limits, such as printed material already distributed.

- 11.7** Photographs and videos may identify individuals even where names are not included. We will minimise accompanying personal information and consider safeguarding risks before publication. We will not publish additional identifying details about a pupil unless specifically authorised for the intended purpose following appropriate checks.

12. Data protection by design and default

- 12.1** 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)
 - Assessing new or changed processing before it begins and completing a data protection impact assessment where it is likely to result in a high risk to individuals' rights and freedoms. This includes considering AI, automated technologies, monitoring systems and changes to the use of sensitive information. The DPO will advise on the assessment.
 - 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
 - Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws will apply
 - Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of the Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure
- 12.2** The internal data protection contact keeps the record of processing activities up to date.

13. Artificial intelligence (AI)

- 13.1** Artificial intelligence (AI), including generative AI, may support teaching, learning and administration. Its use must protect personal data, confidentiality, safeguarding and individuals' rights.

- 13.2** Only tools and uses approved through the Trust's authorisation process may be used for Trust business. Approval of a tool does not authorise every use or every category of information.
- 13.3** Before approval, the Trust will consider:
- The intended purpose and whether the use is necessary and proportionate.
 - The information processed and the appropriate lawful basis and additional conditions.
 - The provider's security, contractual terms, retention arrangements, international transfers and use of information for model training or other purposes.
 - Age restrictions, safeguarding implications and suitability for pupils.
 - Whether a data protection impact assessment is required.
 - Changes needed to privacy information and staff or pupil guidance.
- 13.4** Staff, trustees, pupils and others acting for the Trust must not enter personal data, safeguarding information or confidential Trust information into an AI tool unless that tool has been approved for the specific purpose and type of information.
- 13.5** Availability through a Trust account does not, by itself, constitute approval. Removing names does not necessarily make information anonymous.
- 13.6** Anyone wishing to introduce an AI tool, trial a new tool or use an approved tool in a new way involving personal data must obtain approval from the Academy Business Leader and the Designated Safeguarding Lead, with DPO advice. Approval follows a risk assessment against the Department for Education's Generative AI: product safety expectations, as set out in the Online Safety and Acceptable Use Policy (8.4).
- 13.7** AI outputs must receive appropriate human review for accuracy, fairness and suitability before use. The Trust will not make decisions producing legal or similarly significant effects on individuals solely through automated processing without a separate assessment of lawfulness and safeguards, informed by DPO advice.
- 13.8** Suspected personal data breaches involving AI must be reported immediately under this policy.

14. Data security and storage of records

- 14.1** 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.
- 14.2** In particular:
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
 - Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
 - Staff must use individual accounts, keep credentials confidential and follow the Trust's approved password and authentication requirements. Passwords must not be reused across personal and Trust accounts.

- Portable devices and removable media used to store personal data must have Trust-approved encryption and access controls.
- Personal devices may be used to access Trust personal data only where expressly authorised and subject to approved security arrangements. Trust personal data must not be stored on personal devices (Online Safety and Acceptable Use Policy, 8.3).
- Personal data may be taken off site or accessed remotely only for an authorised work purpose, using approved arrangements. Personal data must not be taken off site on paper or on removable media unless the site Headteacher has agreed, for a specific work purpose. Anything taken off site must be protected during transport, use and storage. Staff working remotely must use the Trust's approved systems.

15. Disposal of records

- 15.1** 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.
- 15.2** 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 Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.
- 15.3** Disposal must follow the approved retention schedule and be authorised and recorded. Routine disposal must be suspended where relevant information is required for an outstanding information request, complaint, safeguarding matter, investigation, litigation or other legal obligation. Staff must seek advice from the internal data protection contact or DPO before disposing of such records.
- 15.4** The Trust's Records Retention Schedule (Appendix 2) sets out how long each type of record is kept. When that period ends, the record must be securely destroyed, unless 15.3 applies. The period is not a minimum. Where a system deletes records automatically, it must be set to match the schedule.

16. Personal data breaches

- 16.1** The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.
- 16.2** In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.
- 16.3** When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:
- A non-anonymised dataset being published on the Trust 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 Trust laptop containing non-encrypted personal data about pupils

17. Training

- 17.1 All staff and trustees are provided with data protection training as part of their induction process.
- 17.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.
- 17.3 Training will include recognising and reporting personal data breaches, handling requests for personal information, safeguarding confidentiality and the safe, lawful and secure use of approved AI tools where relevant.
- 17.4 All staff and trustees with access to the Trust's IT systems must also complete data protection refresher training and cyber security training each year. The cyber security training is the National Cyber Security Centre (NCSC) training for school staff, which is a condition of cyber cover under the Risk Protection Arrangement (RPA). A record of training completed is kept.

18. Monitoring arrangements

- 18.1 The DPO will advise on the review of this policy and monitor compliance.
- 18.2 The Trust will review the policy annually and sooner where changes to legislation, guidance, systems, processing activities or learning from incidents make this necessary. The Records Retention Schedule is reviewed at the same time.
- 18.3 The Resources, Audit & Risk Committee approves the policy and substantive amendments on behalf of the Trust Board. The approval date, last review date and next scheduled review date will be recorded on the cover.

19. Data protection complaints

- 19.1 Anyone concerned about how the Trust has handled their personal data may complain to the internal data protection contact or DPO using the details in section 5.
- 19.2 We will provide an accessible way to complain, including electronically, and offer reasonable assistance where needed. A complaint does not have to use a particular form or refer to legislation.
- 19.3 We will acknowledge complaints within 30 days of receipt. Without undue delay, we will make appropriate enquiries, keep the complainant informed and communicate the outcome and any action taken.
- 19.4 Complaints will be recorded securely and used to identify improvements. The complainant will be informed of their right to complain to the ICO (ico.org.uk, 0303 123 1113).

20. Links with other policies and documents

- 20.1 This policy should be read alongside the Trust's:
 - Privacy notices
 - Records Retention Schedule (Appendix 2)
 - CCTV Policy

- Freedom of Information Policy and Publication Scheme
- Safeguarding and Child Protection Policy
- Online Safety and Acceptable Use Policy
- Protection of Biometric Information Policy

Appendix 1: Personal data breach procedure

- A1.1** A personal data breach may involve the accidental or unlawful loss, destruction, alteration, disclosure of, or access to, personal data.

Reporting and immediate action

- A1.2** Any member of staff, trustee or processor who discovers or suspects a breach must report it immediately to the internal data protection contact and DPO. If the Academy Business Leader is unavailable, they must notify the Data and Office Manager or, if neither is available, their site Headteacher, without delay.
- A1.3** The report should identify what happened, when it occurred or was discovered, the information and individuals potentially affected, and any action already taken. Reporting must not wait until all details are known.
- A1.4** Safe steps to contain the incident should be taken immediately, without destroying evidence. Staff must co-operate with enquiries. The breach investigation is separate from any disciplinary process that may subsequently be required.

Assessment and containment

- A1.5** The Trust will co-ordinate its response with DPO advice and involve the site Headteacher, the Trust's IT provider, the Designated Safeguarding Lead and other relevant staff as necessary.
- A1.6** The response will establish the facts, contain the breach, preserve evidence and assess the likely consequences for individuals before and after mitigation. The Chair of Trustees will be informed where a breach has occurred or is considered likely.

Reporting to the ICO and affected individuals

- A1.7** The Trust, advised by the DPO, will assess whether notification is required.
- A1.8** A breach must be reported to the ICO unless it is unlikely to result in a risk to individuals' rights and freedoms. Where required, notification must be made without undue delay and, where feasible, within 72 hours of the Trust becoming aware of the breach. Any delay must be explained.
- A1.9** Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will be informed without undue delay, unless a lawful exception applies.
- A1.10** Notifications will describe the breach, likely consequences, action taken or proposed, and the DPO's contact details. ICO notifications will also include the categories and approximate numbers of affected individuals and records where available. Incomplete information may be supplied in stages without undue further delay.

Records and review

- A1.11** All breaches will be recorded, including those not reported to the ICO. Records will include the facts, cause, effects, containment action, reporting decisions and reasons, and measures to prevent recurrence.
- A1.12** Records will be stored securely with access restricted to authorised individuals.
- A1.13** The Trust and DPO will review the incident and ensure that agreed improvements are implemented.

Information sent to an incorrect recipient

- A1.14** Where information has been sent to an unauthorised recipient, staff must report the incident immediately and attempt any available safe containment action, such as recalling the message or restricting access to a shared link.
- A1.15** Recall must not be assumed to have succeeded without confirmation. IT support will assist where appropriate, preserving evidence where necessary.
- A1.16** The Trust will consider whether it is appropriate to contact the recipient to request deletion, prevent further sharing and seek written confirmation. Any safeguarding implications of contacting the recipient must be considered first.
- A1.17** Where safeguarding information is affected, the Designated Safeguarding Lead must be involved promptly to assess protective action and any referral to safeguarding partners.

Appendix 2: Records retention schedule

- A2.1** The Trust's Records Retention Schedule is kept as a separate workbook, so that it can be updated without reissuing this policy. It is approved and reviewed with this policy, and published with it.
- A2.2** It is based on the Information and Records Management Society (IRMS) Information Management Toolkit for Schools, through the SBM Services retention schedule (version 24.1, October 2024), adapted for the Trust.
- A2.3** Each line shows how long a type of record is kept. When that period ends, the record must be securely destroyed, unless section 15.3 applies. The period is not a minimum.
- A2.4** The Academy Business Leader owns the schedule, supported by the Data and Office Manager. Staff who cannot find a type of record in the schedule should ask the internal data protection contact before keeping or destroying it.