



Data Protection Policy

Approved by: The Trust Board of Greensand Multi Academy Trust

Date: Monday 8th December 2025

Last reviewed on: Monday 8th December 2025

Next review due by: December 2027

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Definitions	3
4. The data controller	5
5. Roles and responsibilities	5
6. Data protection principles	6
7. Collecting personal data	6
8. Sharing personal data.....	8
9. Subject access requests and other rights of individuals.....	9
10. Parental requests to see the educational record.....	12
11. Biometric recognition systems	12
12. CCTV	13
13. Photographs and videos	13
14. Artificial Intelligence (AI)	13
15. Data protection by design and default.....	15
16. Data security and storage of records	15
17. Disposal of records	16
18. Personal data breaches	17
19. Training.....	17
20. Monitoring arrangements	17
21. Links with other policies	17
Appendix 1: Personal data breach procedure.....	18
.....	

Data Protection Policy

The Trust is registered with the Information Commissioners Office (ICO) as required Registration number ZA2926.

1. Aims

Greensand Multi-Academy Trust (“the Trust”) and its schools aim to ensure that all personal data collected about staff, pupils, parents, Governors, Trustees, Members, visitors and other individuals is collected, stored and processed in accordance with the UK Data Protection Law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation with some amendments by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)

Data Protection Act (DPA 2018).

It is based on guidance published by the Information Commissioner’s Office (ICO) on the [GDPR](#) and guidance from the Department of 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 [code of practice](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with Regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child’s educational record.

This policy also complies with our Funding Agreement and Articles of Association.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, living individual.</p> <p>This may include the individual’s:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data

	<ul style="list-style-type: none"> • Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • 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	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>
Data controller	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
Data processor	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>
Personal data breach	<p>A breach of security leading to the accidental or unlawful destruction, loss,</p>

	alteration, unauthorised disclosure of, or access to personal data.
--	---

4. The data controller

The Trust processes personal data relating to parents, pupils, staff, Governors, Trustees, Members, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will pay its data protection fee as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by and all volunteers volunteering for 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 our member schools comply with all relevant data protection obligations.

5.2 Data Protection Leads

Each school within the Trust will have an appointed Data Protection Lead (DPL). The DPL will handle the day-to-day data protection matters for their respective school and regularly report any data protection issues, at minimum once per term, to the Trust's Data Protection Officer.

5.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this Policy, monitoring compliance with data protection law within the Trust, and developing related policies and guidelines where applicable for the Trust.

The DPO will provide a termly report of their activities directly to the Trust Board's Finance, Audit & Risk Committee (FARC) and, where relevant, report to the Board their advice and recommendations on member school data protection issues. The DPO provides an annual summary report to the Trustees and provides a termly report to individual DPLs for sharing with their governance committees.

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.

The Trust's DPO is Wendy Hill who is contactable via:
--

w.hill@greensandacademytrust.co.uk.
--

5.5 Chief Executive Officer (CEO)

The CEO acts as the representative of the data controller (namely the Trust) on a day-to-day basis.

5.6 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing the school of any changes to their personal data, such as a change of address;
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
 - If they have any concerns that this policy is not being followed;
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK;
 - If there has been a data breach;
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
 - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The UK GDPR is based on data protection principles that our Trust and the schools within it 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 and its schools aim to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust/school can **fulfil a contract** with the individual, or the individual has asked the Trust/school to take specific steps before entering into a contract;

- The data needs to be processed so that the Trust can **comply with a legal obligation**;
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life;
- The data needs to be processed so that the 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/school (where the processing is not for any tasks the Trust/school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden;
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing under the 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 Data Retention and Destruction Policy.

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 child 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, pupils or Governors, Trustees or Members – for example, IT companies, or course providers. 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.

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.

In the unlikely event that we are required to transfer personal data internationally, we will do so in accordance with Data Protection Law.

Where information is provided to post 16 educational establishments, a data sharing agreement will be agreed and signed by both parties.

Where international transfers occur, the Trust will use the UK International Data Transfer Agreement (IDTA) or the Addendum to the EU Standard Contractual Clauses (SCCs) as appropriate.

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 or a member 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 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 or email and include:

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

If staff receive a subject access request in any form, they must immediately inform the DPL in their school who will notify and forward the request to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

For Primary Schools within the Trust:

Children below the age of 12 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 children at our schools may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

For Secondary schools within the Trust:

Children aged 12 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 children at our school may not be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

In many cases, the identity of applicants is known. However, when responding to some requests, we:

- May ask the individual to provide two forms of identification;
- May contact the individual via phone to confirm the request was made;
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant);
- Will provide the information free of charge;
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the child 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 cannot 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 to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time;
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests;
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement);
- Be notified of a data breach (in certain circumstances);
- Make a complaint to the ICO;
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must notify their school's DPL and immediately forward it to the DPO.

9.5 Direct marketing

The Trust schools are certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for direct marketing (for example by e mail, text or automated calls).

The Schools will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand.

Schools will promptly respond to any individual objection to direct marketing.

9.6 Legal exemptions to Subject Access Requests

In certain circumstances, the Trust may be exempt from providing some or all of the personal data requested under a Subject Access Request. These exemptions include, but are not limited to:

- Data processed for the prevention or detection of crime, or the apprehension or prosecution of offenders.
- Confidential references provided or received for education, employment, office appointments, or service provision
- Data subject to legal professional privilege.
- Data processed for management forecasting or planning, where disclosure would prejudice the activity.
- Data relating to negotiations, where disclosure would prejudice those negotiations.
- Data that would reveal personal information about another individual who has not consented, and where it would be unreasonable to disclose without consent.

- Requests that are manifestly unfounded or excessive.
- Requests that would obstruct legal investigations or proceedings.
- Requests that would prejudice criminal prosecutions or penalties.
- Requests that would compromise public or national security.
- Requests that would infringe on the rights and freedoms of others.

Decisions to apply exemptions will be made in consultation with the Data Protection Officer (DPO), and the individual will be informed of the reasons for refusal and their right to complain to the ICO or seek judicial remedy.

9.7 Record keeping

A record of all Subject Access requests is kept by the DPO. The record includes:

The date the SAR was received.

The name of the requester and ID if required.

What data the School sent to the requester.

The date and how the information was transferred.

10. Parental requests to see the educational record

Where parents wish to see their child's educational record, this should be requested by using the procedure for subject access requests as set out at paragraphs 9.1 and 9.2 of this Policy.

11. Biometric recognition systems

Where we use children's biometric data as part of an automated biometric recognition system (for example, children use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/Carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The 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 children 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 children.

Parents/Carers and children 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 child 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 child'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

For our member schools that have CCTV, it is used in various locations around those school sites to ensure they remain safe. We will adhere to the ICO's guidance 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 Trust's Finance & Operations Director.

13. Photographs and videos

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

For Primary schools within the Trust:

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 child.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

For Secondary schools within the Trust:

We will obtain written consent from parents/carers for photographs and videos to be taken of children 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 child. Where we do not need parental consent, we will clearly explain to the child how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where member schools take 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 the Trust or member schools' 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 the Child Protection and Safeguarding Policy/Photography Policy/other relevant policies in force at the relevant member school for more information on their use of photographs and videos.

14. Artificial Intelligence (AI)

14.1 Use of AI Tools

Artificial intelligence (AI) tools are increasingly being used in educational settings. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data. To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Trust will treat this as a data breach and will follow the personal data breach procedure outlined in Appendix 1.

14.2 Automated Processing and Decision-Making

Automated decision-making refers to decisions made solely by automated means without human involvement, which may have legal or significant effects on individuals. This includes profiling activities that evaluate aspects such as performance, behaviour, or preferences.

The Trust does not currently engage in automated decision-making. If such processing is introduced, the Trust will:

- Inform affected individuals of their rights, including the right to object, request human intervention, and challenge decisions.
- Conduct a Data Protection Impact Assessment (DPIA) prior to implementation.
- Ensure appropriate safeguards are in place to protect individuals' rights and freedoms.

14.3 Data Protection Impact Assessments (DPIAs)

Before implementing any AI system or tool that involves personal data, the Trust will carry out a DPIA to assess risks and ensure compliance with UK GDPR. DPIAs will be conducted in the following circumstances:

- Use of new or changing technologies.
- Large-scale processing of special category data.
- Automated decision-making or profiling.
- Systematic monitoring of publicly accessible areas (e.g., CCTV with AI analytics).

Each DPIA will include:

- Description of the processing and its purpose.
- Assessment of necessity and proportionality.
- Evaluation of risks to individuals.
- Measures to mitigate those risks.

14.4 Staff Responsibilities

Staff must seek advice from the Data Protection Officer (DPO) before engaging in any activity involving AI tools or automated processing. This includes:

- Drafting privacy notices for AI-related tools.
- Determining lawful bases for processing.
- Ensuring data minimisation and security.
- Reviewing contracts with third-party AI providers.

The Trust will monitor developments in UK AI regulation and update the policy accordingly to ensure continued compliance.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6);
- Completing data protection and impact assessments where the Trust's/school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);
- Integrating data protection into internal documents including this Policy, any related policies and privacy notices;
- Regularly training members of staff on data protection law, this Policy, any related policies and any other data protection 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 our Trust's DPO and each member school's DPL 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.

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, 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 should be at least 10 characters long containing upper and lower case letters, numbers and special characters to access school computers, laptops and other electronic devices. Staff and children are reminded that they should not re-use passwords from other sites. Password prompts will take place on a regular basis, but this varies across the schools;
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, children, Governors, Trustees or Members who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. (Please see individual member schools' websites for the relevant linked policies);
- 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);
- In some cases logins may be supplemented by the use of multi-factor authentication (MFA) for additional security.

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. Disposal of records will be undertaken in accordance with the Trust's Data Retention & Destruction Policy.

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 a member school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with Data Protection Law.

A summary of key retention periods is available in the Data Retention and Destruction Policy.

18. Personal data breaches

Both the Trust and the member 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 after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium;
- Safeguarding information being made available to an unauthorised person;
- The theft of a school laptop containing non-encrypted personal data about pupils;
- The school's cashless payment provider being hacked and parents' financial details stolen;
- Hardcopy reports sent to the wrong pupils or families.

19. Training

All staff, governors and trustees are provided with data protection training through the National Cyber Security Centre (NCSC) as part of their induction process. All parties will complete annual refresher training.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's/schools' processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this Policy. Termly meetings are held with school data champions who monitor school activities. The DPO will add D at protection issues to the risk register where appropriate.

This Policy will be reviewed **every two years** and shared across the Trust.

21. Links with other policies

This Data Protection Policy is linked to our:

- Child Protection & Safeguarding Policies (at school level);
- Data Retention & Destruction Policy, and to the
- Acceptable use of ICT policies/procedures (at school level).

This policy is also informed by the Online Safety Act 2023, where applicable.

Please also see individual member schools' websites for their linked policies.

This Policy will be reviewed every two years, or sooner if changes are made to data protection legislation.

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, volunteer or data processor must immediately notify their school's DPL who, in turn, must immediately notify the Trust's DPO by e mail or telephone.
- 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 CEO to the Trust and the relevant Headteacher and Chair of Governors.
- 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 on the Trust's computer system and in hard copy by the DPO.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned;
 - The categories and approximate number of personal data records concerned;
 - The name and contact details of the DPO;
 - A description of the likely consequences of the personal data breach;

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

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

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

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

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause;
- Effects;
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored electronically and in hard copy by the DPO.

The DPO and Head Teacher 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 CEO will meet termly to assess recorded data breaches and identify any trends or patterns requiring action by the Trust's school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We 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.

Special category data (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 their DPL & 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 DPL/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 endeavor to obtain 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.

If safeguarding information is compromised, the DPO will inform the DSL and discuss whether the school should inform any, or all, of its three local safeguarding partners.

This Policy will be reviewed every two years.