Bacton Primary School · Cedars Park Primary School · Mendlesham Primary School · Stowupland High School · The John Milton Sixth Form at Stowupland High School

MENDLESHAM STOWUPLAND

JOHN MILTON ACADEMY TRUST

Ambition • Aspiration • Excellence

Data Protection Policy

JMAT 007

History of Document:

Issue No	Author/ Owner	Date Written	Reviewed by Trust on	Comments
V.1	CEO/DPO	April 2018	25-May-18	
V.2	CEO/DPO	Oct 2019	29-Nov-19	amendments made in line with model policy from Schools' Choice (DPO)
V.3	CEO /DPO	Dec 2020	n/a	pg14/ 4.3.9 changed Chair of Governors to Chair of Local Board.
V.4	CEO/DPO	Oct 2023	30-Nov-23	Removed the FOI section (now a separate document) and updated the whole policy

Contents

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

1. Introduction

The schools of the John Milton Academy Trust collect and use certain types of personal information about staff, learners, students, parents, trustees, local board members and other individuals in order to provide education and associated functions. The Trust and/or its schools may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that all personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation and other related legislation.

The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something such as the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed annually.

Our school aims to ensure that all personal data collected about staff, learners, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with 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 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

3.1 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.

3.2 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

Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

3.3 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.

3.4 Data subject

The identified or identifiable individual whose personal data is held or processed.

3.5 Data controller

A person or organisation that determines the purposes and the means of processing personal data.

3.6 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.

3.7 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

The Trust and schools process personal data relating to parents and carers, learners, staff, trustees, local board members, visitors and others, and therefore is a data controller.

The Trust is registered with the ICO and has paid its data protection fee, as legally required.

The Trust **does not** intend to seek or hold sensitive personal data about staff or students except where schools have been notified of the information, or it comes to the attention of schools via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to any Trust school their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

5. Roles and responsibilities

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

5.1 Trustees

The Trustees have overall responsibility for ensuring that the Trust and its schools complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

The Trust has appointed Schools' Choice as its data protection officer. Their role is to inform and advise the Trust on its data protection obligations. They can be contacted at data.protection@schoolschoice.org and questions about this policy, or requests for further information, may be directed to them. The DPO is the first point of contact for the ICO.

The DPO will provide an annual report directly to the Trust Board and, where relevant, report to the board their advice and recommendations on data protection issues.

5.3 Trust and School GDPR Leads

The Trust GDPR Lead is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The school GDPR Lead is the first point of contact for individuals whose data the school processes.

The GDPR Leads' details are as follows:

Bacton Primary School	Mrs Simonds	admin@bactonschool.org.uk
Cedars Park Primary School	Mrs Knights	admin@cedarspark.suffolk.sch.uk
Mendlesham Primary School	Mrs Simonds	admin@medleshamschool.org.uk
Stowupland High School	Mrs Coppen	enquiries@stowuplandhighschool.co.uk
Trust Central Office	Mrs Stringer	enquiries@johnmiltonacademytrust.co.uk

5.3 Executive Headteacher / Headteacher / Head of School

The Executive Headteacher / Headteacher / Head of School 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 such as:

  - To access only data that they have authority to access and only for authorised purposes
  - Not to disclose data except to individuals (whether inside or outside of the Trust) who have appropriate authorization
  - To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction)
  - Not to remove personal data, from the school or Trust premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the local or Trust GDPR Lead 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

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the school's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

6. Data protection principles

The UK GDPR is based on data protection principles that our school/Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

In addition to this, the Trust is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law.

The Trust and its schools are committed to complying with the principles above at all times. This means that the Trust will:

- inform individuals as to the purpose of collecting any information from them, as and when we ask for it;
- be responsible for checking the quality and accuracy of the information;
- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention schedule;
- ensure that when information is authorised for disposal it is done so appropriately;

- ensure appropriate security measures to safeguard personal information whether it is held in paper files or on a computer system, and follow the relevant security policy requirements at all times;
- share personal information with others only when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access requests;
- report any breaches of the GDPR in accordance with the procedure in section 17 / appendix A.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the 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 learner) has freely given clear **consent**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a learner) 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 learner) 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 record retention schedule.

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 learner 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 learners – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that 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 learners or staff.

Where we transfer personal data internationally, we will do so in accordance with UK 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 Trust or school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

All requests should be sent to the Executive Headteacher / Headteacher / Head of School, and must be dealt with in full without delay and at the latest within one month of receipt. The Trust's HR Manager will be informed of all subject access requests made by employees. The DPO will be informed of all Subject Access Requests.

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

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Headteacher must, however, be satisfied that:

- the child or young person lacks sufficient understanding; and
- the request made on behalf of the child or young person is in their interests.

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 learners at our school may not be granted without the express permission of

the learner. This is not a rule and a learner's ability to understand their rights will always be judged on a case-by-case basis.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Trust must have written evidence that the individual has authorised the person to make the application and the Headteacher of the school involved must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

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

- Might cause serious harm to the physical or mental health of the learner or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

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

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that 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 GDPR Lead. If staff receive such a request, they must immediately forward it to the GDPR Lead.

10. Parental requests to see the educational record

As an academy there is no automatic parental right of access to your child's educational record. However, the Trust has agreed that parents, or those with parental responsibility, can access their child's educational record (which includes most information about a learner) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the learner concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the learner or another individual, or if it would mean releasing exam marks before they are officially announced.

To make a request, please contact the school.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Matt Cook, Operations and Facilities Manager: enquiries@johnmiltonacademytrust.co.uk

12. Photographs and videos

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

Primary schools:
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 the learner.

Secondary schools:
We will obtain written consent from parents/carers, or learners aged 18 and over, for photographs and videos to be taken of learners 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 the learner. Where we don't need parental consent, we will clearly explain to the learner 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 learners are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or learners where appropriate) have agreed to this.

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

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns

- Online on our school website or social media pages

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.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, learners 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 learners 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 A.

14. 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. The Trust has appointed Schools' Choice as its data protection officer
- 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 impact assessments where the school/Trust'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 may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school, 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

15. 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 that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and learners are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, learners, Trustees and Local Board members who store personal information on their personal devices are expected to follow the same security procedures as for school/Trust-owned equipment (see our Online Safety policy and Acceptable use of IT and Internet Policy)
- 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).

16. 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 or Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The school 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 A.

Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Headteacher of the school who will inform both the Chief Executive Officer of the Trust and the Data Protection Officer for the Trust.

Once notified, the Chief Executive Officer and Data Protection Officer shall assess:

- the extent of the breach;
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information;
- any measures that can be taken immediately to mitigate the risk to the individuals

When appropriate, the data breach will be reported to the ICO within 72 hours after becoming aware of it, unless a delay can be justified. 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 learners eligible for the learner premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about learners

The Information Commissioner shall be told:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries (which shall usually be the Chief Executive Officer);
- the likely consequences of the breach;
- measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Chief Executive Officer shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- the nature of the breach;
- who to contact with any questions;
- measures taken to mitigate any risks.

The Chief Executive Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations and decisions for further training or a change in procedure shall be reviewed by the Business and Risk Committee of the Trust. Within the context of the breach, any employment investigation will remain confidential.

18. Training

All staff and Trustees / Local Board members 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 Trust GDPR Lead is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Trust Board.

20. Links with other policies and documents

This data protection policy is linked to our:

- Freedom of information publication scheme
- Clear Desk Policy
- Taking Documents out of School Policy
- Acceptable Use of ICT
- Online Safety Policy
- Data Retention Schedule
- Privacy Notices

Appendix A: Personal data breach procedure

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

- On finding or causing a breach or potential breach, the staff member, Trustee, Local Board member or data processor must immediately notify the Headteacher of the school who will inform both the Chief Executive Officer (CEO) of the Trust and the GDPR Lead.
- Once notified, the CEO or GDPR Lead will inform the data protection officer (DPO).
- In liaison with the DPO, the CEO and GDPR Lead will investigate the report and determine whether a breach has occurred. To decide, the DPO, CEO and GDPR Lead 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 Trustees / Local Board members will co-operate 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 CEO/GDPR Lead will alert the headteacher and the chair of the Local Board or Trustees
- The GDPR Lead will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the GDPR Lead with this where necessary, and the GDPR Lead should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The GDPR Lead 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 and GDPR Lead 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 and GDPR Lead 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
- 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 GDPR Lead 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/GDPR Lead
- 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 and GDPR Lead 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 and GDPR Lead 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 on the Trust's computer system

- The GDPR Lead and 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
- The GDPR Lead and CEO will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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 GDPR Lead as soon as they become aware of the error. The GDPR Lead will alert the DPO (Schools' Choice)
- If the sender is unavailable or cannot recall the email for any reason, the GDPR Lead will ask IT support to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the GDPR Lead/DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The GDPR Lead/DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The GDPR Lead/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 GDPR Lead will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners