FIERTÉ
MULTI-ACADEMY TRUST
Proudly inspiring all to excellence

Caring • Individuality • Bravery • No one left behind

Data Protection Policy

Document and Version Control

Document Title	Data Protection Policy
Effective Date	1st September 2026
Policy Owner	Ryan Byrne (Data Protection Officer)
Policy Approver	Trust Board

Version	Date	Amended by	Comments
1.0	Summer 2026	Ryan Byrne (DPO)	New policy replacing previous following appointment of new DPO. Updated to accurately reflect practice, industry guidance and the DUAA 2025.

Section	Changes Made
Throughout	Policy rewrite.

Contents

Introduction

Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, 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.

Legislation

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
- Data (Use and Access) Act 2025

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

This policy also:

- Meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
- Reflects the ICO's guidance for the use of surveillance cameras and personal information.
- Complies with our funding agreement and articles of association.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual, whether identified directly or indirectly. This may include the individual's: ▪ Name (including initials) ▪ Identification number ▪ Location data ▪ Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ▪ Racial or ethnic origin ▪ Political opinions ▪ Religious or philosophical beliefs ▪ Trade union membership ▪ Genetics ▪ Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ▪ Health – physical or mental ▪ Sex life or sexual orientation
Processing	Any activity that involves the use of personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual and includes transmitting or transferring personal data to third parties.
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 personal data. The data controller is responsible for establishing practices and policies in line with the UK GDPR.
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. A data processor acts only on the instructions of the controller and does not determine the purposes or means of the processing.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Data Controller

Our Trust processes personal data relating to parents and carers, pupils, staff, governors, visitors and others. In carrying out these activities, the Trust acts as a data controller.

The Trust is registered with the ICO and pays the data protection fee to the ICO as legally required. The Trust's registration reference is ZA100920.

Roles and Responsibilities

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

Trust Board

The Trust Board has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

Data Protection Officer (DPO)

The Trust has appointed and empowered a Data Protection Officer (DPO) to fulfil their statutory duties under UK GDPR. The DPO shall act independently, be protected from dismissal or detriment in performing their role, have a direct line of reporting to executive leadership and be appropriately resourced by the Trust.

The DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law and developing related policies and guidelines where applicable. The DPO provides advice to the Trust Board, Executive Leadership Team, Headteachers and individual staff in relation to data protection compliance. The Trust will ensure that such advice is formally considered and, where it is not followed, the reasons are appropriately documented. Full details of the DPO's responsibilities are set out in their job description.

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

Our DPO is **Ryan Byrne** and is contactable via **DPO@fierte.org**.

Please contact the DPO with any questions about data protection, UK GDPR or if you have any concerns that this data protection policy is not being or has not been followed.

Executive Leadership Team (ELT)

The Trust Executive Leadership Team (ELT) is responsible for ensuring that data protection compliance is effectively implemented across the Trust. This includes promoting a culture of data protection, ensuring that appropriate policies, procedures and controls are in place and that sufficient resources are allocated to support compliance.

The ELT will support the independence of the DPO, ensure the timely escalation of data protection risks and incidents, provide appropriate support and resources for the investigation of such matters and provide assurance to the Trust Board on the Trust's compliance.

Headteachers

Headteachers act as the representative of the data controller on a day-to-day basis within each academy. As such, they are responsible for ensuring that this policy is implemented and adhered to at academy-level. This includes:

- Promoting a culture of data protection and good information governance within the academy

- Ensuring that staff are aware of, understand and comply with this policy and related procedures
- Implementing appropriate local processes and controls to safeguard personal data
- Ensuring that personal data is processed fairly, lawfully and securely within the academy
- Supporting the identification, reporting and management of data protection risks and personal data breaches
- Ensuring that data protection considerations are embedded into new projects, systems, and activities
- Liaising with and supporting the DPO, including acting on advice and facilitating access to staff, systems and information where required

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:
    - If they have 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

Data Protection Principles

We adhere to the principles relating to processing of personal data set out in the UK GDPR, which requires personal data to be:

- Processed lawfully, fairly and in a transparent manner (*lawfulness, fairness and transparency*)
- Collected for specified, explicit and legitimate purposes (*purpose limitation*)

- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (*data minimisation*)
- Accurate and, where necessary, kept up to date (*accuracy*)
- Kept for no longer than is necessary for the purposes for which it is processed (*storage limitation*)
- Processed in a way that ensures it is appropriately secure (*security, integrity and confidentiality*)
- Not transferred to another country without appropriate safeguards in place (*transfer limitation*)
- Handled in a way that respects the rights of data subjects and allows them to exercise those rights (*data subject rights and requests*)

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (*accountability*).

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

Personal Data

Lawfulness, Fairness and Transparency

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

- The data needs to be processed so that 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 (*for example, 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 Trust (*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 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 data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes** and the processing is done by or under the direction of a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (*or their parent/carer when appropriate in the case of a pupil*) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

Limitation, Minimisation and Accuracy

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

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate. For example, the Trust uses the Arbor Parent Portal to enable parents and carers to access key personal data held about them and their child, review its accuracy and request updates - helping to ensure that information remains accurate, relevant and limited to what is necessary.

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

Sharing Personal Data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

There will be certain circumstances where we may be required to share personal data. These include, but are not limited to, situations where:

- There is an issue with a pupil, or a parent or 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 providers. 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.
- Sharing personal data with law enforcement and government bodies where we are legally required to do so.
- Sharing personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

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

Subject Access Requests and the Right of Access

What is a Subject Access Request (SAR)?

By law, individuals have a right to ask whether an organisation is using or storing their personal information and, if so, to gain access to copies of this. This is known as a '*Subject Access Request*' (SAR).

A SAR can include both information held electronically and on paper where it forms part of a structured record. A SAR is focussed on personal data and does not necessarily result in receiving copies of *full* files or email exchanges by default.

Children and Subject Access Requests

Under law, personal data about a child belongs to the child and not the child's parents or carers. For a parent or carer to make a SAR on behalf of 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, parents or carers with parental responsibility will *usually* be able to make a SAR on behalf of their child within our Trust without the express permission of the pupil. However, this is not a blanket rule as we will always assess a pupil's ability to understand their rights as well as what is in the child's best interests on a case-by-case basis.

If it is deemed that your child *does* understand their rights over their own data, we will need to obtain consent from your child before you can make a SAR on their behalf.

A SAR can be made by contacting the Data Protection Officer via email:

DPO@fierte.org

Please see the ICO's website for more information on the right of access.

Limitations and Exemptions

If a SAR is excessive or manifestly unfounded, we may refuse to act on it or may charge a reasonable fee to cover administrative costs. In making this decision, we will consider whether:

- the request is "*intended to harass [the] organisation or cause disruption*"
- the request is "*clearly unreasonable*"
- the requestor has "*no clear intention of exercising [the] right of access*"
- the request is repetitive in nature

The Trust may withhold some, or all, of an individual's personal information when responding to a SAR because of an exemption. Exemptions are in the law to protect particular types of information or how certain organisations work.

In response to a SAR, 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 a pupil or another individual.
- Would reveal that a 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.

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

Making a Subject Access Request

Individuals don't need to use any special wording when making a SAR but being clear about ***what*** information they are looking for can help us respond more efficiently and is a better guarantee that they will receive the specific data they're seeking. Individuals are also welcome to make subsequent SARs where they seek further data.

Requests for *All* Data Held

While individuals are entitled to request "**all**" personal data we hold about them, if they do so we will carry out **reasonable and proportionate** searches across systems and records. This means we are not required to search records exhaustively where it would be unreasonable or disproportionate to do so or where data is not reasonably likely to contain personal data.

A good example of this distinction is CCTV. Where a SAR is made for CCTV footage between specific times and dates, we would search for and likely provide that footage. However, in response to a broad/general request for "***all***" personal data, we would not be required to review *all* CCTV footage recorded just in case they were captured at any point.

For these reasons, it's always preferable for requesters to be specific about the:

- Types of data they're seeking *(and/or examples of data which they are not interested in)*
- Timeframe when the data may have been generated or processed
- Rationale for the SAR (*optional but can help us to ensure you receive the data you seek*)

As an example, requests for "*all behavioural incident records about my child since June 2021*" or "*all SEND provision plans for my child from Year 3 onward*" can usually be responded to ***much*** more swiftly and in a more targeted manner than a request for "*all my child's data*".

Requests for "**all**" data are still valid but will likely take significantly longer to respond to and will almost certainly return excessive results including:

- children's historical lunch, snack or milk selections
- attendance marks and registration entries (*for example, daily AM/PM ticks or late codes*)
- routine timetable, class or year group allocations (*such as which class or group a child or staff member was placed in during a particular term*)
- records of routine activities, trips or clubs enrolled in

Much of this information may not be relevant to the specific purpose of a subject access request but it may still need to be reviewed as part of such broad searches.

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*).
- 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 (*these timeframes continue to apply when the school is closed during holidays*).

Other Data protection Rights

In addition to the right to make a Subject Access Request (*see above*), individuals also have the right to:

- Withdraw their consent to processing at any time (*where consent is the lawful basis for processing*)
- Receive certain information about the Trust's processing activities
- 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 conducted under the lawful basis of public task, 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 personal data breach (*in certain circumstances*)
- Make a complaint to the ICO

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (*in certain circumstances*)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

The Educational *or* Pupil Record

Our academies **do** maintain an "educational" *or* "pupil record". The content of these records is defined in separate guidance produced by the Trust.

Under The Education (Pupil Information) (England) Regulations 2005, parents, or those with parental responsibility, have a legal right to free access to their child's educational record (*which includes most information about a pupil*) within 15 school days of receipt of a written request. However, **this legislation does not apply to academies**.

As such, the best way for parents to obtain a copy of the pupil record is to submit a SAR on behalf of their child with the following content:

> **To:** *DPO@fierte.org*
>
> **Subject:** *Subject Access Request - Pupil Record*
>
> *Please provide me with a copy of my child's **pupil record**. My child is **[full name, school name, DOB]**.*

CCTV

We use CCTV in various locations around our school sites to ensure they remain safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

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

Any enquiries about the CCTV system should be directed to the DPO.

Photographs and Videos

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

We will obtain written consent from parents and carers for photographs and videos to be taken of their child for optional purposes which are not required to fulfill our public task. We will clearly explain how photographs and/or videos will be used.

Any photographs and videos taken by parents and carers at school events for their own personal use are not covered by data protection legislation. However, we 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.

Please see our "*Safe Use of Images and Videos Policy*" as well as each school's safeguarding policies for detailed information on our use of photographs and videos.

Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Fierté Multi-Academy Trust recognises that AI has many uses to help pupils learn and support efficiencies 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. Trust networks are configured to restrict access to such known, unauthorised sites.

The Trust has issued guidance to staff regarding the acceptable use of *approved* AI tools. Only AI services that are procured under contract, subject to appropriate security safeguards and that do not use Trust data to train public models may be used. Any use of such tools must comply with data protection law, Trust guidance and the principle of data minimisation. Staff must ensure that only the minimum personal data necessary is used, and only where there is a clear and lawful reason to do so.

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.

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 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.

- Completing data protection impact assessments (DPIAs) where the processing of personal data presents a high risk to rights and freedoms of individuals and when introducing new technologies (*the DPO advises 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 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.

Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a process designed to help analyse, identify and minimise the data protection risks of a project or plan which involves data processing. DPIAs are not a check-box exercise to justify new systems - they must be used to inform if *or* how a system will be implemented.

Anyone proposing or leading a new project, system or change which may involve the processing of personal data - including staff, governors and trustees - must consult the DPO at the earliest opportunity. The DPO will advise as to whether a Data Protection Impact Assessment (DPIA) is required and will ensure that any privacy risks are identified and addressed before the project proceeds. Early consultation allows the Trust to ensure our data protection obligations are met and that privacy by design is embedded into new activities.

In some cases, the DPO may advise that a full DPIA is not required. Where this applies, the DPO may ask for a "screened" DPIA to be completed instead. This provides a brief overview of the project, the types of data involved and documents the reasons as to why a full DPIA has not been considered necessary - helping the Trust to demonstrate accountability and evidence that data protection risks have been considered at an early stage.

The Trust's Data Protection Officer (DPO) is responsible for interrogating DPIAs but is reliant on the accuracy and honesty of statements within. Misrepresentation of the facts during the DPIA process can be cause for disciplinary action.

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 containing personal data are kept under lock and key when not in use. Such documents must not be left on desks, staffroom tables or anywhere else where there is general access.
- Portable electronic devices, such as laptops and hard drives, are encrypted where possible and/or kept under lock and key when not in use.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- The Trust password policy must be adhered to and technical enforcement controls are in place where possible. Users received annual cyber security training and are reminded not to reuse passwords across sites.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (*see our "Device Policy"*). The Trust enforces Conditional Access controls and Mobile Application Management (MAM) technology where possible.
- 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.

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 parties to safely dispose of records and equipment 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.

Please see the Records Management Policy for further information.

Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that personal data breaches do not occur. In the event of a suspected data breach, the Trust 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 test 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.

We will also notify the data subject where we are legally required to do so.

Complaints

We take any complaints about how we collect and use personal information seriously.

If you think that our collection or use of personal information is unfair, misleading, inappropriate or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us at any time by contacting the Data Protection Officer - Ryan Byrne - via **DPO@fierte.org**.

Upon receiving a complaint, we will:

- Acknowledge receipt of the complaint within 30 days of receiving it
- Without undue delay, take appropriate steps to respond to the complaint, including:
    - Making appropriate enquiries based on the circumstances of the complaint
    - Keeping the complainant informed on the progress of the investigation
- Without undue delay, inform the complainant of the outcome of the investigation

Training

All staff, governors and trustees are provided with data protection training as part of their induction process. Data protection also forms part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary. Staff are expected to undertake refresher training at least annually.

Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

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

Appendix 1
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, governor or data processor must immediately notify the data protection officer (DPO) via email (DPO@fierte.org), telephone or Teams call.
- 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, governors and trustees 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 DPO will alert the Vice-CEO. In some cases, it will also be appropriate for the DPO to inform the relevant headteacher or line-manager.
- 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*). Please see the actions relevant to specific data types at the end of this procedure.
- The DPO will assess the potential consequences (*based on how serious they are and how likely they are to happen*) before and after the implementation of steps to mitigate the consequences.
- The DPO will determine whether the breach must be reported to the ICO and the individuals affected. The DPO may rely upon the ICO's self-assessment tool to support this process.
- The DPO will document the decisions (*either way*), in case the decisions are later challenged by the ICO or an individual affected by the breach. Documented decisions are stored within the Data Protection Teams site under the "Data Breaches" folder structure.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO's website or through the breach report line (0303 123 1113) within 72 hours of the Trust's awareness of the breach. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:

        - *The categories and approximate number of individuals concerned.*
        - *The categories and approximate number of personal data records concerned.*
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the required details are not yet known, the DPO will report as much as they can within 72 hours of the Trust'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 within the Data Protection Teams site under the "Data Breaches" folder structure.
- Where appropriate, the DPO and Vice-CEO will meet to review what happened and how it can be stopped from happening again.
- The DPO and Vice-CEO meet regularly and assess recorded data breaches and identify any trends or patterns requiring action by the Trust to reduce risks of future breaches.