Inspiring all to excellence

The Fierté Multi-Academy Trust

Data Protection Policy

At the heart of Fierté Multi-Academy Trust are both the UNICEF Rights Respecting values and articles and Learning Behaviours. Through these, we aim to put children's rights at the heart of our schools. We work together to embed children's rights in our ethos and culture; to improve well-being and develop every child's talents and abilities to their full potential. We aspire to give children a sense of pride and achievement in all that they undertake.

Document Control

Document Title	Date Protection Policy
Author	Linda Webster
Department/Subject	Data Protection
Document Status	Approved
Approval	Trust Board
Publication Date	02.12.2019
Review Date	Autumn Term 2020
Issued to	Teams Policy Site

Version Control

Version	Date	Amended by:	Comments
V1	October 2018	Linda Webster	Issued
V2	November 2019	Linda Webster	Changes made to reflect the Data Protection Act 2018 and latest ICO guidance. See table below.

POLICY SECTION	WHAT'S CHANGED?
Section 1	Updated the link to the GDPR, added '(EU) 2016/679' to its title
Section 1	Changed the reference to the Data Protection Bill to the Data Protection Act (DPA) 2018
Section 2	Removed the reference to 'expected provisions'
Section 2	Removed the reference to the ICO subject access request code of practice
Section 3	In the definition for 'personal data', specified that the information must relate to a 'living' individual
Section 4	Added a reference to paying the data protection fee, rather than just to registration
Section 7.1	Tweaked the wording for the vital interests, public interest and legitimate interests bullet points in the first list
Section 7.1	Added new bullet point lists about conditions of processing for special category and criminal offence data
Section 7.1	Added a short paragraph on processing data fairly
Section 7.2	Added a short paragraph on ensuring data accuracy
Section 8	Changed the wording of the first paragraph
Section 8	Removed the reference to a data sharing agreement
Section 8	Removed the bullet points in the part about sharing personal data with law enforcement and government bodies
Section 9.1	Added the following bullet points to the first list: • 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 safeguards provided if the data is being transferred internationally
Section 9.1	Clarified that subject access requests can be submitted in any form
Section 9.3	Added to the third bullet point of the first list, explaining that the 1 month deadline for responding will kick in after receiving additional information needed to confirm the requester's identity, where relevant
Section 9.3	Changed the introductory sentence for the second bullet list (to "We may not disclose information for a variety of reasons, such as if it:")

POLICY SECTION	WHAT'S CHANGED?
Section 9.3	Added the following bullet points to the second bullet point list: • 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
Section 9.3	Removed the following bullet points from the second bullet point list: • Is contained in adoption or parental order records • Is given to a court in proceedings concerning the child
Section 9.3	Clarified the wording in the part about when a reasonable fee can be charged
Section 9.3	Added that, upon refusal of a request, individuals can seek to enforce their subject access right through the courts
Section 9.4	Tweaked the wording of the bullet points on asking to rectify, erase or restrict processing; objecting to processing; and challenging decisions based on automated decision marking and profiling
Section 9.4	Removed the bullet points on requesting a copy of agreements for transferring data outside of the European Economic Area and preventing processing that is likely to cause damage or distress
Section 11	Added a paragraph about parents taking photographs or videos for their personal use
Section 11	Added a line explaining that the bullet point list refers to school uses of photographs and videos
Section 12	Added a bullet point on appropriate safeguards being in place when transferring data outside of the European Economic Area
Section 12	Tweaked the wording in the bullet point about maintaining an internal record of the personal data you hold
Section 13	Data Protection Impact Assessments – new section included in line with Data Protection Legislation
Section 14	Tweaked the bullet points about papers not being left on desks and how to set passwords
Section 16	Specified in the third paragraph that breaches will be reported within 72 hours of you becoming aware of them

POLICY SECTION	WHAT'S CHANGED?
Section 18	Removed the references to the Data Protection Bill
Section 19	Added links to Internet Safety and E.Mail Policies
Appendix 1	In the bullet point about how to notify the ICO, added that you can also call the ICO's breach report line
Appendix 1	Under the bullet point about the DPO assessing the risk to individuals, added a new sub-point about including a description of the breach in clear and plain language in the notification sent out to individuals
Appendix 1	Added a line under the bullet point about the DPO assessing the risk to individuals to add that any decision on whether to contact individuals will be documented by the DPO

Contents:

1. Aims

Fierté Multi-Academy Trust aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

2. Legislation and guidance

This policy meets the requirements of the GDPR and the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

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.

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

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered as the data controller and has paid its data protection fee to the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Trust board

- The trust board has overall responsibility for ensuring that all academies within the Fierté Multi-Academy Trust comply with all relevant data protection obligations.

5.2 Data protection officer

- The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
- They will provide an annual report of their activities directly to the trust board and, where relevant, report to the board their advice and recommendations on academy data protection issues.

- The DPO is also the first point of contact for individuals whose data our academies process, and for the ICO.
- Full details of the DPO's responsibilities are set out in their job description.
- Our DPO is Mrs. Linda Webster and is contactable via email: **DPO@fierte.org**

5.3 Headteacher

Each Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the academy 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 European Economic Area
    - 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 GDPR is based on data protection principles that our academies 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 our academies 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 our academies can fulfil a contract with the individual, or the individual has asked the academy to take specific steps before entering into a contract
- The data needs to be processed so that our academies can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual 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 our academies 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 clearly 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 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.
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/records management 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 pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the academy 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

If staff receive a subject access request they must immediately forward it 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.

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

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 if it:

- Might cause serious harm to the physical or mental health of the pupil 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 which takes into account 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, or object to the processing of it (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 (decisions taken with no human involvement, that might negatively affect them)
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. CCTV

We use CCTV in various locations around the academy site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.
We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
Any enquiries about the CCTV system should be directed to Headteacher.

11. Photographs and videos

As part of academy activities, we may take photographs and record images of individuals within our academies.
We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.
Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil 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 our academies take photographs and videos, uses may include:

- Within academies on notice boards and in academy magazines, brochures, newsletters, etc.
- Outside of academies by external agencies such as the academy photographer, newspapers, campaigns
- Online on our Trust and/or academy websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.
See our Policy for the Safe Use of Children's Photographs for more information on our use of photographs and videos.

12. 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 impact assessments where the academy'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 European Economic Area (EEA), 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 academies and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data Protection Impact Assessments

The Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.
The Trust will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered.
The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, or 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 academy offices
- Passwords that are recommended to be a combination of 3 – 4 short words adding capital letters, numbers and symbols are used to access academy computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils, trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for academy-owned equipment (see our Internet Safety Policy/acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The academy 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 an academy context may include, but are not limited to:

- A non-anonymised dataset being published on the academies 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 an academy laptop containing non-encrypted personal data about pupils

17. Training

All staff, trustees and governors are provided with data protection training as part of their induction process.

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

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **annually** and shared with the full trust board.

19. Links with other policies

This data protection policy is linked to our:

- Internet Safety policy/acceptable use agreement
- E.mail policy
- Policy for the safe use of children's photographs
- Safeguarding policy
- The Freedom of Information Act 2000 (see appendix 2)

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert a member of the Executive Leadership Team (DELT, CFO or CEO), the academy headteacher, trustees and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in password protected files on One Drive.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or through their breach report line (0303 123 1113) within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - 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

  As above, any decision on whether to contact individuals will be documented by the DPO
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, 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 in password protected files on One Drive.
  The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

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.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- Details of pupil premium interventions for named children being published on the academy website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- An academy laptop containing non-encrypted sensitive personal data being stolen or hacked
- The academy's cashless payment provider being hacked and parents' financial details stolen

Appendix 2 : Freedom of Information Act 2000

The Freedom of Information Act 2000 gives the public right of access to information produced in the course of the Trust's work. There are exemptions to this right. In particular, data about living, identifiable people ('personal data') continues to be covered by the Data Protection Act and is not generally publicly available except to the "subject" of the data – that is, the person whom the data is about.
Under the Freedom of Information Act, Fierté Trust will publish all the documents which the Trust will make public as a matter of routine.

Contact us

If you have any questions, concerns or the information you are looking for is not available on the academy website, you can make a request for the information you require in writing, or by email to the data protection officer:
Mrs. Linda Webster
email address: DPO@fierte.org