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 2025
Policy Owner	Data Protection Officer
Policy Approver	Trust Board

Version	Date	Amended by	Comments
1.0	Autumn 2019	DPO	
1.2	Autumn 2020	DPO	
1.3	Autumn 2021	DPO	Re-write of policy to reflect UK GDPR Legislation and to meet the needs of academies across the Fierté Multi-Academy Trust
1.4	Summer 2022	DPO	New sections added - "Data Security" and "Appendix 3"
1.5	Summer 2023	DPO	Changes made to links to policies
1.6	Summer 2024	DPO	Reference to Trust Record of Processing. Name and contact details of DPO changed.

Section	Changes Made

Contents

This policy is drafted in accordance with the requirements of the UK General Data Protection Regulation ("UK GDPR") and the UK Data Protection Act 2018.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any individual and it helps to promote equality across Fierté Multi-Academy Trust.

Policy Statement

Everyone has rights regarding the way their personal data is handled. During our activities as a Trust and associated academies across the Trust, we will collect, store and process personal data about our pupils, workforce, parents/ carers and others. This makes us a **data controller** in relation to that personal data.

We are committed to the protection of all personal data and special category personal data for which we are the **data controller**.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

About this Policy

The types of personal data that we may be required to handle include information about pupils, parents, trustees, governors, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018, 2021 update, and is based on guidance published by the Information Commissioner's Office (ICO). (Collectively 'Data Protection Legislation').

This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

Definitions

Data is information that is stored electronically, on a computer, or in certain paper-based filing systems.

Personal Data means any information relating to an identified or identifiable, living individual. This may include the individual's:

- Name (including initials)
- Date of birth

- 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.

Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Data Controllers are the people or organisations who determine the purposes for which, and the way, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. The Trust are the **data controllers** of all personal data used in our business for our own purposes.

Data Users are those of our workforce (including trustees, governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data Processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.

Processing is any activity that involves the use of data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.

Special Category Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

Workforce includes any individual employed by the Trust such as staff and those who volunteer in any capacity including trustees, members, member of a local governing body, parent helpers and community volunteers.

Data Protection Officer

As a Trust we are required to appoint a Data Protection Officer (DPO). Our DPO is Ryan Byrne and can be contacted at: DPO@fierte.org

The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

Data Protection Principles

The UK GDPR is based on data protection principles, anyone processing personal data must comply with these principles:

- 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 purpose for which it is processed.
- Processed securely using appropriate technical and organisational measures.

Personal Data must also:

- Be processed in line with data subjects' rights.
- Not be transferred to people or organisations situated in other countries without adequate protection.

This policy sets out how the Trust will comply with these principles in relation to any processing of personal data.

Fair and Lawful Processing

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing (see below).
- Whether the personal data will be shared, and if so with whom.
- The period for which the personal data will be held.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right to raise a complaint with the Information Commissioner's Office in relation to any processing.

We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered and ensure that we have a lawful basis for any processing.

For personal data to be processed lawfully, it must be processed based on one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:

- Where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract.
- Where the processing is necessary to comply with a legal obligation that we are subject to, (e.g the Education Act 2011).
- Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest.
- Where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.
- When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds.
- Where the processing is necessary for employment law purposes, for example in relation to sickness absence.
- Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment.
- Where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities.
- Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

If any data user is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

Vital Interests

There may be circumstances where it is considered necessary to process personal data or special category personal data to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not able to give consent to the processing.

We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

Where none of the other bases for processing set out above apply then the school must seek the consent of the data subject before processing any personal data for any purpose.

There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

When pupils and / or employees join the Trust a consent form will be required to be completed in relation to them.

This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

Processing for Limited Purposes

As a Trust at times, it will be necessary to collect and process personal data. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other schools, parents, other pupils, or members of our workforce).

We will only process personal data for specific purposes or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

Notifying Data Subjects

If we collect personal data directly from data subjects, we will inform them about:

- Our identity and contact details as Data Controller and those of the DPO.
- The purpose or purposes and legal basis for which we intend to process that personal data.
- The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- Whether the personal data will be transferred outside UK and if so the safeguards in place.
- The period for which their personal data will be stored, by reference to our Retention Schedule.
- The existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making.
- The rights to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible, thereafter, informing them of where the personal data was obtained from.

Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by Data Protection Legislation.

Under Article 30 of the General Data Protection Regulations (GDPR), the Trust are required to document procedures of processing activities within our academies, which is known as Records of Processing. This document informs:

- How we are processing data
- Why we are processing data
- What kind of data is being processed
- Where the processing is taking place
- Who the data is disclosed to

Accurate Data

- We will ensure that personal data we hold is accurate and kept up to date.
- We will take reasonable steps to destroy or amend inaccurate or out-of-date data.
- Data subjects have a right to have any inaccurate personal data rectified.

Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.

Processing in line with data subject's rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any personal data we hold about them.
- Object to the processing of their personal data, including the right to object to direct marketing.
- Have inaccurate or incomplete personal data about them rectified.
- Restrict processing of their personal data.
- Have personal data we hold about them erased.
- Have their personal data transferred.
- Object to the making of decisions about them by automated means.

The Right of Access to Personal Data

Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the Trust's Subject Access Request Procedure.

The Right to Object

In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking based on a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

An objection to processing does not have to be complied with where the Trust can demonstrate compelling legitimate grounds which override the rights of the data subject.

Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

In respect of direct marketing any objection to processing must be complied with.

The Trust is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

The Right to Rectification

If a data subject informs the Trust that personal data held about them by the Trust is inaccurate or incomplete, then we will consider that request and provide a response within one month.

If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the data subject within one month of their request that this is the case.

We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why. In those circumstances we will inform the data subject of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

Data subjects have a right to "block" or suppress the processing of personal data. This means that the Trust can continue to hold the personal data but not do anything else with it.

The Trust must restrict the processing of personal data:

- Where it is in the process of considering a request for personal data to be rectified (see above).
- Where the Trust is in the process of considering an objection to processing by a data subject.
- Where the processing is unlawful, but the data subject has asked the Trust not to delete the personal data.
- Where the Trust no longer needs the personal data, but the data subject has asked the Trust not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the Trust.

If the Trust has shared the relevant personal data with any other organisation, then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

Data subjects have a right to have personal data about them held by the Trust erased only in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was originally collected.
- When a data subject withdraws consent – which will apply only where the Trust is relying on the individuals consent to the processing in the first place.
- When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object.
- Where the processing of the personal data is otherwise unlawful.
- When it is necessary to erase the personal data to comply with a legal obligation.
- If the Trust offers services to a pupil and consent is withdrawn in respect of that pupil in relation to those services.

The Trust is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- To exercise the right of freedom of expression or information.
- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, research, or statistical purposes.
- In relation to a legal claim.

If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

Right to Data Portability

In limited circumstances a data subject has a right to receive their personal data in an electronic readable format, and to have this transferred to another organisation.

If such a request is made, then the DPO must be consulted.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

Security procedures include:

- **Entry controls**
    - Any stranger seen in entry-controlled areas should be challenged and reported to the headteacher and academy office.
- **Secure lockable desks and cupboards**
    - Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal**
    - Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. In line with the Trust Cyber Security and IT Administration Policy, IT assets must be disposed of in accordance UK GDPR, Waste Electrical and Electronic Equipment Directive (WEEE Directive) and the Information Commissioner's Office guidance on the disposal of IT assets.
- **Equipment**
    - Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock PC's / tablets when left unattended.
    - USB storage should not be used, there is no record of data transferred through USB/external storage drives and the Trust is unable to ensure that data stored this way is used and deleted appropriately after use. There is an increased risk of a security breach when using external drives and is prohibited when working in schools. All Trust / school devices no longer have the facility to use a USB device. All school related data should be stored in OneDrive or Teams for which all staff have had relevant training.
- **Working away from the school premises – paper documents**
    - Paper documents should only be removed from site where there is a clear and compelling case to do so. No confidential information should be removed from the site, except where this is necessary to fulfil an agreed purpose of the school; for example, the risk assessment protocols carried on school visits. Where this is the case, document sign out procedures will apply.
- **Working away from the school premises – electronic working**
    - The Trust supports remote and electronic working as central to our delivery of educational services across our academies. However, remote working must be within the parameters of the Homeworking Protocol. This includes prohibitions on the use of USB drives; protections preventing the download of information, and prohibitions on accessing confidential or personal data offsite.
- **Document Printing**
    - Documents containing personal data must be collected immediately from printers and not left on photocopiers.

- **Data Transfer**
    - Any documents/data that need to be transferred whether internally across academies or externally to outside organisations are to be done electronically with documents being scanned and sent via email, with recipients being asked to confirm receipt.
    - Should the need arise for anything to be hand delivered this will need to have a covering letter in duplicate outlining the contents and the date transfer occurred signed by both the person delivering and the person accepting, with a copy being retained by both parties. (see appendix 3).

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

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 (DPIA) is required, and if so how to undertake that assessment.

Disclosure and Sharing of Personal Information

We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, and / or Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

The Trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

In some circumstances we will not share safeguarding information. Please refer to our Child Protection / Safeguarding Policy.

Data Processors

We contract with various organisations who provide services to the Trust, including payroll providers, information management service providers, IT and other data management contractors. The services delivered by these companies are integral to the work of the Trust, including educational delivery in schools, record keeping including safeguarding records, analysis of data returns, and academy improvement.

In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.

Images and Videos

Parents and others attending Trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child where this is specifically permitted prior to the performance and is not disruptive. The Trust does not prohibit this as a matter of policy.

The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

As a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of parents / carers where appropriate, before allowing the use of images or videos of pupils for such purposes.

Whenever a pupil joins an academy in our Trust their parent / carers will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

Personal Data Breaches

The Trust 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.

CCTV

CCTV is in place at some of our academies to ensure they remains safe. Please refer to the Trust CCTV Policy.

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 individual academy Headteachers.

Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy. It may be necessary to make amendments at any time. Where appropriate, we will notify data subjects of those changes.

Links with Other Policies

This data protection policy is linked to our:

- Online Safety Policy
- Acceptable Use Agreements
- Communication and Email Policies
- Policy for the Safe use of Children's Images
- Child Protection / Safeguarding Policy
- Cyber Security and IT Administration Policy
- CCTV Policy
- Freedom of Information Policy

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 (CEO, Vice CEO, COO) and the academy headteacher.
- 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
    - Identity theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Another significant economic or social disadvantage to the individual(s) concerned.
- If it is likely that 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 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 ate 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.
    - Actions taken to contain 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 OneDrive.

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 3: Data Transfer Template

Inspiring All to Excellence

The Fierté Multi Academy Trust

Transfer of Data / Documents

From: *Name of academy*

To: *Receiving organisiation*

Documents included:

Delivered by: ……

Received by: ……

Date: ……