Transforming Lives

EDUCATIONAL TRUST

Data Protection Policy

November 2023

Version Control

Category:	Data	
Authorised By:	Safeguarding Standards Committee	
Author:	Director of Operations	
Version	2	
Status:	Under Review:	
	Approved:	✓
Issue Date:	November 2023	
Next Review Date:	November 2025	
Statutory Policy:	Yes	✓
	No	
Printed Copies Are Uncontrolled		

Contents

1 – The TLET Way

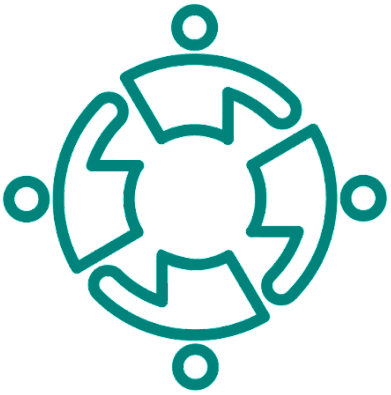
Transforming Lives Educational Trust (TLET) is a family of academies. Every TLET policy is rooted in and reflects our ambitions for pupils, students and wider stakeholders alike.

OUR AMBITIONS -
As a Trust family, our shared ambitions drive everything we do, we call this 'The TLET Way'.

Through the transformative values of courage, kindness and loyalty, together we:

NURTURE POTENTIAL

We flourish in the places we create together.



INSPIRE COMMUNITY

We champion each other to make a difference.

DELIVER EXCELLENCE

We strive to achieve our best.

2 – Definition of Terms

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 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.

3 – Roles and Responsibilities

3.1 The **Trust Board** (The Board) has overall responsibility for ensuring that the Trust and its academies comply with all relevant data protection obligations.

3.2 The **Trust 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 trust/academy data protection issues.
The DPO is also the first point of contact for the **Information Commissioner's Office (ICO)**.

3.3 **Academy Data Protection Leads (DPLs)** manage data protection day to day in individual academies and will work closely with the Trust DPO. They will be the first point of contact for individuals whose data the school processes.

3.4 The **Principal** acts as the representative of the data controller on a day to day basis in each Trust academy. The **Director of Operations** acts as a representative in the Central Team.

3.5 All staff are responsible for:

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

4 – Rationale and Statutory Requirements

4.1 This procedure is aimed to ensure that all personal data collected about staff, pupils, parents/carers, trustees, governors,, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

4.2 This policy applies to all personal data whether it be in paper or electronic format.

4.3 The Trust processes personal data relating to parents/carers, pupils, staff, partners, trustees, visitors and others and therefore is a data controller.

4.4 The procedures have been established against the following principles and legislation:

- The Data Protection Act 2018;
- The Freedom of Information Act 2000;
- The UK General Data Protection Regulation;
- The statutory duties and government guidance from the Department of Education relating to schools, including for safeguarding.

5 – Scope

This policy refers to:

Parents/Carers	✓	**Trustees**	✓
Employees	✓	**Volunteers**	✓
Pupils/Students	✓	**Visitors**	✓
Governors	✓	**Community**	✓

6 – Principles

The UK GDPR is based on data protection principles that our Trust must comply with. The principles say that personal data must be:

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

7 – Policy Statement

7.1 This policy meets the requirements of:

- UK General Data Protection (UK GDPR) - the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

- Data Protection Act 2018 (DPA 2018)

7.2 It is based on guidance published by the Information Commissioners Office (ICO) on the UK GDPR.

7.3 Where the Trust estate uses biometric data it meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

7.4 Where the Trust uses CCTV it also reflects the ICO's guidance for the use of surveillance cameras and personal information.

7.5 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.

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

8 – Procedure

8.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law (see appendix 3):

1. The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
2. The data needs to be processed so that the Trust can **comply with a legal obligation**
3. The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
4. 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**
5. The data needs to be processed for the **legitimate interests** of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
6. 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 1 of the special category conditions for processing under data protection law:

1. The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
2. The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
3. 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
4. The data has already been made **manifestly public** by the individual
5. The data needs to be processed for the establishment, exercise or defence of **legal claims**
6. The data needs to be processed for reasons of **substantial public interest** as defined in legislation
7. 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
8. 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
9. 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:

1. The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
2. 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
3. The data has already been made **manifestly public** by the individual
4. 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**
5. 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 (see Appendix 2).

8.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

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

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule.

8.3 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 UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

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

8.4 Subject access requests and other rights of individuals

8.4.1 Subject access requests

Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the Trust 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 in any form they must immediately forward it to the DPO in line with the Trusts SAR policy.

8.4.2 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 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.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils may not 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.

8.4.3 Responding to subject access requests

When responding to requests, we:

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

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

- Might cause serious harm to the physical or mental health of the 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 to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

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

8.4.4 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, individuals also have the right to:

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

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

8.5 Parental requests to see the educational record

As an academy trust there is no automatic parental right of access to the educational record. However, where possible we will seek to accommodate parental right of access to their child's educational record (which includes more information about a pupil) within 15 school days of receipt of a written request.

8.6 Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

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

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The academy will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the academy's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the academy's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the academy will delete any relevant data already captured.

8.7 CCTV

We use CCTV in various locations around the Trust's academy sites to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles. We have a Trusts CCTV policy outlining our policies and procedures.

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 Principal.

8.8 Photographs and videos

As part of our Trust 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 the pupil.

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 we take photographs and videos, uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

8.9 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 Trust DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Identifying DPLs within our academies and ensuring they have the necessary resources to fulfil their duties
- 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 where the academies processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school 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

9.0 Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our 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.

9.1 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 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 Trust Destruction and Retention Policy).

9.2 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 may include, but are not limited to:

- A non-anonymised dataset being published on the website, which shows the exam results of pupils eligible for the pupil premium.

- Safeguarding information being made available to an unauthorised person.
- The theft of a laptop containing non-encrypted personal data about pupils.

9.3 Training

All staff, Trust Board, and governors are provided with data protection training as part of their induction process. We will also provide additional training to those acting as Data Protection Officers in single academies.

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

10 – Equality Statement

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 it is fair, it does not prioritise or disadvantage any individual (with due regard to their protected characteristics), and it helps to promote equality across the Trust.

11 – Monitoring

It is the responsibility of the Trust Board and those they delegate authority, to ensure that the principles and procedures of this policy are adhered to. The use of this policy will be subject to routine monitoring to ensure its fidelity in practice. The evidence gathered from monitoring at regular intervals shall inform any reviews and future revisions to the policy, and no later than that stated on Page 1 of this policy.

12 – Related Documents

This data protection policy is linked to our:

- Retention and destruction policy
- Acceptable use 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 Principal of the Academy or the CEO of the Central Team.
- The Principal/CEO will notify the DPO immediately and then, under their direction, investigate the report and determine whether a breach has occurred. To decide, they 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 third parties

- The Principal of the Academy or the CEO will alert the DPO, Chair of LGB and the Trust Board Chair.
- The Principal of the Academy or the CEO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members, DPO or data processors where necessary.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will, in consultation with the Principal/ CEO determine whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, 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 of identity theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation o Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it is 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.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website 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 Principal/ CEO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO and Principal/ CEO
- 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 Principal/ CEO 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/ DPL's 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)

The DPO and DPL's will 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) could include but is not limited to:

- 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 Principal will ask IT Services to recall it
- In any cases where the recall is unsuccessful, the Principal 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 Principal will ensure we those individuals concerned receive a written response from all the individuals those who received the data, confirming that they have complied with this request
- The Principal will carry out undertake 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

Other types of breach could include, but is not limited to:

- *Details of pupil premium interventions for named children being published on the academy's website*
- *Non-anonymised pupil exam results or staff pay information being shared with Aim partners and/or trustees*
- *A laptop or other electronic data storage device containing non-encrypted sensitive personal data being stolen, lost or hacked*
- *The academy's cashless payment provider being hacked and parents' financial details stolen*

Complaints

Complaints about the above procedures should be made via the Complaint's Policy and the Trust Board will decide whether it is appropriate for the complaint to be dealt with in accordance with the Trust's complaint procedure.

Complaints which are not appropriate to be dealt with through the Trust's complaints procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts
If you have any queries or concerns regarding these policies / procedures then please contact the Principal.

Appendix 2: Additional Guidance for Staff

These guidelines represent the latest information and guidance and are subject to updates

- Staff should familiarise themselves with the contents of this policy and ensure they comply with the General Data Protection Regulations
- Staff should not remove any 'personal' or 'sensitive' data from the academy if at all possible, the preferred method of access being remotely via a secure connection

Article 4 (1) of GDPR defines personal data as being:

- '*Any information relating to an identified or identifiable natural person*' ('*data subject*');
- '*An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'

This now includes IP addresses, biometric data, mobile device ID's, cookies on websites.

- Any electronic use of this type of personal or sensitive data should be strictly limited to whole academy analysis by authorised staff only.
- If personal and sensitive data is removed electronically, then it is encrypted – encrypted memory sticks are available from IT Services.
- 'Day to day data' such as electronic mark books and assessment data does constitute personal and sensitive information and should still be kept securely against theft or loss. The individual being mindful of how this data could be used in conjunction with other data.
- This data should not be transferred to the hard disk of home computers / laptops.
- Measures should be taken to ensure the security of devices, which contain personal data when not in academies.
- If data is lost then it should be reported immediately to the Principal.
- Any communication/transfer of data to a third party should only take place with written parental consent.
- The capture and use of pupil/student-photographs should be limited and parental permission received.
- Parents should be informed of how we collect, use and safeguard student data.
- Parents should be informed of all data which is held on their children, its use, its life-span and the potential risk involved and how the school mediates against that risk – this is communicated via the Privacy Statement issued to parents and available on the Trust's academy websites.
- Every member of staff should be informed of what data is held on them by the Trust, why, for what purpose, how long it will be kept and how it is safeguarded.

Appendix 3: Checklist for obtaining consent under the GDPR

Action	✓
Asking for consent	
We have checked that consent is the most appropriate lawful basis for processing	
We have made the request for consent prominent and separate from other terms and conditions	
We ask people to positively opt in	
We don't use pre-ticked boxes, or any other type of consent by default	
We use clear, plain language that is easy to understand	
We specify why we want the data and what we're going to do with it We have named our organisation and any third parties We tell individuals they can withdraw their consent and we don't make consent a pre-condition of a service	
We ensure that the individual can refuse to consent without detriment	
Recording consent	
We keep a record of when and how we got consent from the individual and what they were told at the time	
Managing consent on an on-going basis	
We regularly review consents to check that they relationship, the processing and the purposes have no changed We have processes in place to refresh consent at appropriate intervals, including any parental consents	
We make it easy for individuals to withdraw their consent at any time, and publicise how to do so	
We act on withdrawals of consent as soon as we can	
We don't penalise individuals who wish to withdraw consent	