TEESSIDE LEARNING TRUST

Aiming high... Daring to be great

Data Protection Policy

Teesside Learning Trust Policy

Ratification by	Board of Trustees
Ratification date	4 July 2018
Review frequency	Annually
Next review date	May 2019
Next ratification date	Summer 2019
Responsibility of	Data Protection Officer

Badger Hill Academy

Freebrough Academy

Thornaby Academy

Whitecliffe Academy

Contents

1. Statement of Policy 3
2. Aims 3
3. Legislation and guidance 3
4. Definitions 4
5. The Data Controller 5
6. Roles and Responsibilities 5
7. Data Protection Principles 6
8. Collecting personal data 6
9. Sharing personal data 7
10. Subject access requests and other rights of individuals 8
11. Biometric recognition systems 10
12. CCTV 11
13. Photographs and videos 11
14. Data protection by design and default 11
15. Data security and storage of records 12
16. Disposal of records 12
17. Personal data breaches 13
18. Training 13
19. Monitoring arrangements 13

1. Statement of Policy

The Multi Academy Trust needs to collect and use certain types of information about students, their families, employees and with whom it deals, in order to perform its functions. This includes information on current, past and perspective employees, students, persons with parental responsibilities, suppliers, customers, service users and others with whom it communicates.

Each Academy within the Trust and the Trust Central Services Team is required by law to collect and use certain types of information to fulfil its statutory duties and also comply with the legal requirements of government.

Each Academy within the Trust and all staff employed by any of the Academies or by the Trust will adhere to this guidance document and will have access to the Data Protection Officer for additional support, guidance and advice.

2. Aims

The Trust and each Academy within it aims 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 (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

3. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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

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

This policy should be considered in conjunction with:

- TLT Privacy Notice
- TLT Document & Data Retention Policy
- TLT Archive & Confidential Waste Policy
- TLT Guidance Note : Photo and Video Consent
- E-Safeguarding Policy (with particular reference to the Appendices)
- TLT Subject Access Request Process
- TLT Data Breach Process
- TLT Safeguarding Policy
- TLT Code of Conduct for Staff
- TLT GDPR Declaration for Staff

- TLT Complaints Policy / Procedure
- TLT CCTV Policy
- TLT Guidance Note: Working Off Site
- TLT Guidance Note: Password Complexity Requirements
- TLT Guidance Note: Using Personal Devices

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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.

5. The Data Controller

All Academies within the Trust process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore are a data controller.

The Trust is the legally responsible 'body' and is registered with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles and Responsibilities

This policy applies to **all staff** employed by any of the Academies within the Trust, **and** to external organisations or individuals working on it's behalf. Staff who do not comply with this policy may be subject to disciplinary action in accordance with the Teesside Learning Trusts Disciplinary Policy.

6.1 Board of Trustees
The board of trustees has overall responsibility for ensuring that our academies comply with all relevant data protection obligations.

6.2 Data Protection Officer
The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, ensuring, compliance with data protection law, and developing related policies and guidelines where applicable.

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

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

The DPO for Teesside Learning Trust is Beverley Smith and is contactable via Enterprise Centre, Freebrough Academy, Linden Road, Brotton TS12 2SJ,bevsmith@TLTrust.org, telephone 01287 676305 ext109

6.3 Head Teacher / Principal
The Head Teacher or Principal of each academy and the Data Protection Officer acts as the representative of the data controller on a day-to-day basis.

6.4 All staff
Staff must be aware that they could potentially be subject to individual prosecution and so must appreciate that they 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

7. Data Protection Principles

The GDPR is based on data protection principles that all 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 the Trust aims to comply with these principles.

8. Collecting personal data

8.1 Lawfulness, fairness and transparency

Academies within the Trust and the Central Team 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 the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school 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 which are set out in the GDPR and Data Protection Act 2018. These are

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sex life
- Sexual orientation

It is confirmed that for our Primary Academies that offer online services to pupils, such as classroom apps, which rely on consent as a basis for processing, the Academy will get parental consent (except for online counselling and preventive services).

For Secondary online services to pupils, such as classroom apps, which rely on consent as a basis for processing, we will get parental consent where the pupil is under 13yrs (except for online counselling and preventive services). Where a pupil is older than 13 their consent will be collected and the pupil will be provided with the relevant information required by data protection law prior to this occurring.

8.2 Limitation, minimisation and accuracy

Academies within the Trust will only collect personal data for specified, explicit and legitimate reasons. These reasons are published in the TLT Privacy Notices (for students, staff and governors on the Trust website).

If personal data is to be used for reasons other than those published in the TLT Privacy Notices the Academy will inform the individuals concerned before the data is collected and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. 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 TLT Document & Data Retention Policy and the TLT Archive & Confidential Waste Policy

9. Sharing personal data

The Trust, and any Academy within it, will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of Trust staff at risk
- There is a need to liaise with other agencies – the Academy will seek consent as necessary before doing this from either the child if over 13 yrs or the parent unless we have a legal duty
- Suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, payroll provider. When doing this, the Trust 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, and information necessary to keep them safe while working with us

The Trust or any Academy within it will also share personal data with law enforcement and government bodies where there is a legal requirement to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided either the child if over 13 yrs or the parent unless we have a legal duty

The Trust or any Academy within it 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 there is a need to transfer personal data to a country or territory outside the European Economic Area, this will be done so in accordance with data protection law.

10.Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the establishments within 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
- 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

Subject access requests are required in writing, preferably using the pro forma on the website, by letter or email to the DPO. They should 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.

10.2 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 below the age of 12 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.

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 at our school 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.

10.3 Responding to subject access requests

All subject access requests will come to the Data Protection Officer. The Data Protection Officer will work with and support the Academy to pull together the relevant data. The Data Protection Officer will response to the request on behalf of the Academy / Trust. The Data Protection Officer :

- 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
- 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

Information will not be disclosed if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When a request is refused the individual will be informed as to why, and that they have the right to complain to the ICO.

10.4 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 any Academy with in the Trust are collecting an individual's data the data subject will also be told how the data is to be used and how it will be processed (see section 8), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the Academy 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
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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 staffs receive such a request, they must immediately forward it to the DPO.

11. 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, the Trust 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 Trust will get written consent from at least one 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 school's biometric system(s). Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or 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 school's biometric system(s), the Trust will also obtain their consent before they first take part in it, Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12.CCTV

The Trust use CCTV in several locations around the various Academy sites to ensure it remains safe. The Trust will adhere to the ICO's code of practice for the use of CCTV, refer to the CCTV Policy.

The Trust does not need to ask individuals' permission to use CCTV, but will 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 Head Teacher or Principal of the Academy

13.Photographs and videos

As part of activities undertaken by academies in the Trust, photographs may be taken and images of individuals recorded.

The Trust will obtain written consent from parents/carers, or pupils aged 13 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where parental consent is needed, the Trust will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where parental consent is not required) pupils over the age of 13 yrs.) the Trust will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, the Trust will delete the photograph or video and not distribute it further with the exception of marketing material where outstanding stocks will be used up.

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

For more information on our use of photographs and videos please refer to the ESafeguarding Policy and the TLT Guidance Note:.Photographic and Video Images

14.Data protection by design and default

The Trust will put measures in place to show that all academies 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 7)

- Completing privacy impact assessments where the school'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; records of attendance will be kept
- Regularly conducting reviews and audits to test our privacy measures and make sure the Trust is compliant
- 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 that is required is shared about how data is used and how the data is processed (via our privacy notices)
    - For all personal data that is held, maintaining an internal record of the type of data, data subject, how and why the data is being used, any third-party recipients, how and why the data is being stored, retention periods and how the data is kept secure

15. Data security and storage of records

Each Academy within the Trust 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, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site please refer to the Guidance Note: Working Off Site
- When setting passwords these should be in line with the Guidance Note: Password Complexity Requirements
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils and trustees who chose to access or store personal information on their personal devices do so at their own risk and shouldn't consider this without reviewing. The TLT Guidance Note: Using Personal Devices.
- 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 9)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where the Trust cannot or do not need to rectify or update it. For example, the Trust will shred or incinerate paper-based records, and overwrite or delete electronic files. The Trust may also use a third party to safely dispose of records on the school's behalf. If

we do so, the third party will have to provide sufficient guarantees that it complies with data protection law.

17.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, each Academy will follow the procedure set out by the Trust.

When appropriate, the Trust will report the data breach to the ICO within 72 hours. Such breaches in an Academy context 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 school laptop containing non-encrypted personal data about pupils

18.Training

All staff and trustees are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19.Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually.

General Data Protection Regulation - Declaration

By signing this declaration you are acknowledging that you have read and understood the Trusts Data Protection Policy which has been prepared in accordance with the General Data Protection Regulations 2016/679.

Non Negotiable Behaviour

- Don't collect data or information without ensuring that it is either covered in the Privacy Notice or consent has been obtain
- Don't hang on to data which the Trust no longer has a right to keep
- Ensure that paper based records and portable electronic devices such as laptops are locked away when not in use
- Dispose of paper records in accordance with the Archive and Confidential Waste Policy
- Only use encrypted data sticks or encrypted drives
- Before taking a photograph or video ensure that consent has been obtained from the individual
- Don't leave personal or sensitive data/ information unattended in public areas
- It will not be acceptable to not report a data breach

Declaration

I have read and understood the 'Teesside Learning Trust Data Protection Policy' and I agree to comply with these rules. I understand that if I breach any of these rules, I may be subject to disciplinary action in accordance with the 'Teesside Learning Trusts Disciplinary Policy'.

I also understand that if I need any advice in relation to this I can contact the Data Protection Officer bevsmith@tltrust.org for help.

Date……

Print Name……

Signed……