DATA PROTECTION POLICY

CONTENTS

Statement of Intent

The Learning Trust is required to keep and process certain information about its staff members, pupils, their families, volunteers and external contractors in accordance with its legal obligations under data protection legislation. The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, DfE, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the core principles of the UK GDPR.

1 Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- Freedom of Information Act 2000
- DfE (2023) 'Keeping children safe in education 2023'

The policy is also based on the following guidance:

- DfE (2023) Data protection in Schools
- Information Commissioner's Office's (ICO) published guidance
- Generative artificial intelligence in education

It operates in conjunction with, but not limited to, the following Trust and local policies:

- TLT Data and Cyber Security Breach Procedure Policy
- TLT Cyber Security Response Plan
- Safeguarding and Child Protection Policy
- TLT Freedom of Information Publication Scheme and List
- TLT CCTV Policy
- TLT Data Protection – Personal Data Breach Procedure
- TLT Protection of Biometric Informaton Policy
- TLT Privacy Notice – Candidates
- TLT External Privacy Notice (Pupils, Students and Parents) Privacy Notice – Employees
- TLT Staff ICT Acceptable Use Policy
- Student ICT Acceptable Use Policy
- TLT Retention of Records Policy
- TLT DBS Policy

2 Aims

Our Trust takes the security and privacy of all data seriously and 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 UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

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

The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy confirms how that personal information is dealt with properly and securely, and in accordance with GDPR and other legislation.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and will be reviewed every year as recommended by the Department for Education (DfE).

3 Roles and Responsibilities

3.1 The Learning Trust processes personal data relating to parents and carers, learners, staff, governors, visitors and others in order to provide education and associated functions, and is therefore registered as a **data controller** with the ICO. The Chief Financial Officer of the Trust will ensure that this registration is renewed annually or as otherwise legally required.

3.2 **Data subjects** are the identified or identifiable individual whose personal data is held or processed.

3.3 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this policy.

3.4 **Data processors** process personal data only on behalf of the data controller, and are usually a third party external to The Learning Trust.

3.5 The Trust's Director of IT serves as The Learning Trust's **Data Protection Officer (DPO)**, and is responsible for the overall coordination of data protection including:-

- overseeing the implementation of this Data Protection Policy and, as applicable, developing related policies and privacy guidelines;
- coordinating a proactive and preventative approach to data protection;
- providing the required training to staff members and promoting a Trust wide culture of privacy awareness;
- calculating and evaluating the risks associated with the Trust's data processing;

- prioritising and focussing on more risky activities, e.g. where special category data is being processed;
- advising on DPIAs to help identify and reduce data protection risks, where appropriate;
- carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws;
- acting as the first point of contact for the ICO;
- keeping up to date and informed with Artificial Intelligence (AI) technologies relevant to the Trust and advising on how to integrate the use of AI while complying with data protection regulations
- understanding and maintaining awareness of what the use of AI means for data protection in the Trust

3.6 The Trust's wider staff body is made aware of this policy and duties under UK GDPR as part of their induction to The Learning Trust. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

3.7 This policy applies to all staff employed by the Academy Trust, and to external organisations, volunteers and other individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

All staff are responsible for:

- collecting, storing, securing and processing any personal data in accordance with this policy;
- informing the Trust 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.

4 Personal Data

4.1 'Personal data' is information that identifies an individual. It includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain.

4.2 A sub-set of personal data is known as 'special category personal data' (previously known as sensitive personal data). This special category data is information that reveals:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Physical or mental health;
- An individual's sex life or sexual orientation;
- Genetic or biometric data for the purpose of uniquely identifying a natural person.

Information relating to criminal convictions will only be held and processed where there is legal authority to do so.

4.3 In a school, examples of personal data include:

- identity details (for example, a name, title or role);
- contact details (for example, an address or a telephone number);
- information about pupil behaviour and attendance;
- assessment and exam results;
- staff recruitment information, such as the application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- staff contracts;
- staff development reviews;
- staff and pupil references;

5 Data Protection Principles

5.1 Personal data must be processed in accordance with the principles set out in UK GDPR.

5.2 The principles say that personal data must:

- be processed lawfully, fairly and in a transparent manner;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;

- be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- not be kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed;
- be processed securely using appropriate technical and organisational measures to protect against authorised or unlawful processing and accidental loss, destruction or damage;
- not be transferred to another country without appropriate safeguards being in place; and
- be made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data.

5.3 The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

6 Lawful Processing

6.1 The Trust will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The **consent** of the data subject has been obtained;
- Processing is **necessary for a contract held with the individual**, or because they have asked the school to take specific steps before entering into a contract;
- Processing is necessary for **compliance with a legal obligation** (not including contractual obligations);
- Processing is necessary for the performance of a task carried out **in the public interest** or in the exercise of official authority vested in the controller;
- Processing is necessary for protecting **vital interests** of a data subject or another person, i.e. to protect someone's life;
- Processing is necessary for the purposes of **legitimate interests** pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the school in the performance of its tasks.

6.2 The Trust will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

6.3 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;
- Whether the personal data will be shared, and if so, with whom;
- The existence of the data subject's rights in relation to the processing of that personal data;
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

6.4 **'Processing'** means any operation which is performed on personal data such as:

i. collection, recording, organisation, structuring or storage;
ii. adaption or alteration;
iii. retrieval, consultation or use;
iv. disclosure by transmission, dissemination or otherwise making available;
v. alignment or combination;
vi. restriction, destruction or erasure; and
vii. transmitting or transferring to third parties.

This includes processing personal data that forms part of a filing system and any automated processing.

We can process personal data for these purposes without an individual's knowledge or consent. We will not use personal data for an unrelated purpose without telling the individual about it and the legal basis that we intend to rely on for processing it.

6.5 Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject;
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent;
- Processing relates to personal data manifestly made public by the data subject;
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement;

- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards;
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law;
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices;
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law;
- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

6.6 This personal data might be provided to us by the person it relates too, or someone else (such as a former employer, a former school, their doctor, or a credit reference agency), or it could be created by us.

7 Consent

7.1 Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words, or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

7.2 Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

7.3 The Trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.4 When pupils and staff join a school in the Trust, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

7.5 Where the Trust opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

8 Sharing personal data

8.1 The Trust will not normally share personal data with anyone else without consent, except as set out in the Trust's privacy notices. However, certain circumstances may require us to do so and these include, but are not limited to, the following situations:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- We need to liaise with other agencies – we will seek consent as necessary before doing this;
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a stand-alone 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.

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

- 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 to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

8.2 Sometimes we might share personal data with other schools in the Trust or our contractors and agents to carry out our obligations under our contract with an individual or for our legitimate interests. Further details of such third parties are set out in the Trust's Privacy Notices.

The Trust has the following separate Privacy Notices for the following groups, which outline the information that is specific to them:

- Candidates
- Pupil, Students and Parents
- Employees

A copy of these privacy notices can be found on the Trust's website.

8.3 We do not send personal data outside the European Economic Area. If this changes, data subjects will be notified of this and the protections which are in place to protect the security of the data will be explained.

9 How the Trust's employees should process personal data for the Trust

9.1 Everyone who works for, or on behalf of, the Trust has some responsibility for ensuring data is collected, stored and handled appropriately and to protect personal and special category data in accordance with data protection legislation.

9.2 The Trust's employees should only access personal data covered by this policy if it is needed for the work to be carried out, or on behalf of the Trust, and only if the staff member is authorised to do so. Our staff should only use the data for the specified lawful purpose for which it was obtained.

9.3 Personal data must not be shared informally.

9.4 Personal data must be kept secure and not shared with unauthorised people.

9.5 All employees should use strong passwords.

9.6 Computer screens should be locked when employees are not at their desks.

9.7 Our employees must ensure that individual monitors do not show confidential information to passers-by.

9.8 All Trust employees should regularly review and update personal data which they have to deal with for work. This includes telling us if their own contact details change. Employees should not make unnecessary copies of personal data and should keep and dispose of any copies securely

9.9 Personal data should be encrypted where particularly sensitive before being transferred electronically to authorised external contacts. Employees should speak to IT Support for more information on how to do this.

9.10 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

9.11 Under no circumstances should employees save personal data to their own personal computers or other devices.

9.12 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the DPO.

9.13 Drawers and filing cabinets, should be locked where possible. Do not leave paper with personal data lying about.

9.14 Trust employees should not take personal data away from Trust's premises without authorisation from their line manager or DPO.

9.15 Data security must be maintained by protecting the confidentiality, integrity and availability of personal data defined as follows:

9.16 Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

9.17 Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

9.18 Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

9.19 Personal data should be shredded and disposed of securely when the user has finished with it.

9.20 Any deliberate or negligent breach of this policy by an employee may result in disciplinary action being taken against that employee in accordance with our disciplinary procedure.

9.21 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in dismissal.

9.22 Trust employees should ask for help from the Trust's DPO (or the DPO's nominated representative in each school) if unsure about data protection or if they notice any areas of data protection or security we can improve upon.

- The Learning Trust's nominated representative is Darran Jones, CEO
- The ICT Support Team nominated representatives are John Blundell and Dan Mateus
- CHS' nominated representative is Nia Roberts, Deputy Headteacher
- QPHS' nominated representative is Tom Gregory, Deputy Headteacher
- BPS' nominated representative is Lynne Taylor, Deputy Headteacher
- CIS' nominated representative is Daryl Goodwin, Vice Principal

10 Data Protection and employees of The Learning Trust

As well as Trust employees collecting, storing, securing and processing personal data on behalf of the Trust, they are also data subjects. This policy explains how the Trust will hold and process its employees information and explains our employees rights as subjects. It also explains employee obligations when obtaining, handling, processing, or storing personal data in the course of working for, or on behalf of, the Trust.

- An employee's compliance with this Data Protection Policy is mandatory and any breach may result in disciplinary action.

- Related policies and privacy notices are available to help our employees to interpret and act in accordance with this Data Protection Policy. Employees must also comply with all such related policies and privacy guidelines as detailed in section 1 of this policy.

- This policy does not form part of a contract of employment (or contract for services if relevant) and can be amended by the Trust at any time. It is intended that this policy is fully compliant with the 2018 Act and the UK GDPR. If any conflict arises between those laws and this policy, the Trust intends to comply with the 2018 Act and the UK GDPR.

- If an employee chooses not to provide us with certain personal data they should be aware that we may not be able to carry out certain parts of the contract between us. For example, if they do not provide us with their bank account details we may not be able to pay them. It might also stop us from complying with certain legal obligations and duties which we have such as to

pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability they may suffer from.

10.1 The Trust has to process an employees personal data in various situations during their recruitment, employment (or engagement) and even following termination of their employment (or engagement). Examples of when we might procees an employees personal data are:

- to decide whether to employ (or engage) an applicant;
- to decide how much to pay a new employee, and the other terms of their contract with us;
- to check an individual has the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training new employees and reviewing their performance*;
- to decide whether to promote an employee;
- to decide whether and how to manage an employees performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to an employee or someone else;
- to determine whether we need to make reasonable adjustments to their workplace or role because of their disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the Trust, of individuals, our other staff, pupils and others;
- to monitor and protect the health, safety and welfare of our employees, pupils and third parties*;
- to pay an employee and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions*;
- monitoring compliance by an employee, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to an employee*;
- running the Trust and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Trust in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;
- to safeguard pupils;
- for any other reason which we may notify our employees of from time to time.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of employees' personal information.

10.2 We will only process special categories of an employees personal data in certain situations in accordance with the law. For example, we can do so if we have their explicit consent. If we asked for an employee's consent to process a special category of personal data then we would explain the reasons for our request. An employee does not need to consent and can withdraw consent later if they choose.

We do not need an employees consent to process special categories of their personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect our employee's vital interests or those of another person; where our employee/they are physically or legally incapable of giving consent;
- where an employee has made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of an employees working capacity.

10.3 We might process special categories of an employees personal data for the purposes in paragraph 10.1 above which have an asterisk beside them. In particular, we will use information in relation to:

- an employees race or ethnic origin to monitor equal opportunities;
- an employees sickness absence, health and medical conditions to monitor their absence, assess their fitness for work, to pay them benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after our employee's health and safety; and
- en employee's trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

10.4 We envisage that we will hold information about criminal convictions as it is appropriate given the nature of the role our employees work in, and to comply with our legal obligations. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by an employee in the course of them working for us. We will use information about criminal convictions and offences in order to maintain appropriate safeguards for working with children.

10.5 The Trust does not take automated decisions about employees using their personal data or use profiling in relation to them.

11 How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place, please see the Trust's **Data and Cyber Breach Prevention Policy**. Should a breach of personal data occur then we must take notes and keep evidence of that breach as soon as it/they are discovered. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

Examples of a breach are:

- making safeguarding information available to an unauthorised person;
- the theft of a school laptop containing non-encrypted personal date about pupils;
- a staff member fails to carry out checks to confirm who they are speaking to on the phone leading to verbal disclosure of a child's personal data to an unauthorised person;
- human error, such as falling victim to phishing attacks remains a significant factor in data breaches in schools.

11.1 If an individual becomes aware that a data breach has occurred the individual must contact the Trust's DPO immediately and keep any evidence they have in relation to the breach.

11.2 Please see the **TLT Personal Data Breach Procedure** for further details.

12 Subject access requests

12.1 Any individual whose personal data is held by an education setting (data subject) can make a '**subject access request**' ("SAR") to find out the information we hold about them.

This request can be in any format ie verbal or written via letter, text, or email. Once an individual as made their request we cannot ask them to change the format they made the request in. When an individual asks for their personal data, they do not have to call it a SAR.

12.2 Please be aware that someone could be making a SAR if they:

- make a complaint
- quote other legislation, such as a freedom of information request

A requester can ask for any personal data that relates to:

- themselves
- someone they have parental responsibility for

- someone they have permission to act on behalf of

Some requests will be non-specific and ask for "all the information you hold".

In most cases when an individual makes a SAR, it will be necessary to ask for identification (ID) from them.

If one of the Trust's schools receives a request, it should be forwarded immediately to the Trust's DPO, who will work with the school to coordinate a response.

We are not permitted to ask the requester to narrow or reduce their request, but can ask for clarification of what specific information the requester is looking for. This might be helpful when the requester asks for a lot of information because they are not sure what they need.

If the requester already has access to the information they want to see, the Trust can direct them to this. For example, the requester may already have access to personal data stored on the school's website.

The Trust does not have to treat this request as a SAR, provided the individual can access the information within one calendar month.

12.3 If a Trust employee would like to make a SAR in relation to their own personal data, they should make this in writing to the Trust's DPO. The Trust must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request. The Trust will verify the identity of the person making the request before any information is supplied.

12.4 Requesting a SAR is a child's right. A child can request access to information about themselves from any education setting that holds data about them.

A child does not have to be a certain age to make a SAR.

The InformationCommissioner's Office (ICO) provides guidance on the rights of children when making SARs, which must be referred to and followed on every occasion that a SAR is received from or on behalf of a child.

Parents, or those with parental responsibility, do not have an automatic parental right of access to their child's educational record. Any requests from parents will be treated as subject access requests in accordance with the above.

12.5 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

12.6 There is no fee for making a SAR. However, if the individual's request is manifestly unfounded, excessive or a request for further copies of the same information we may charge a reasonable administrative fee or refuse to respond to their request. The individual will be informed of a decision to refuse to respond to the request and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

12.7 The Trust will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the school will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

13 Other data subject rights

13.1 Data subjects have the right to information about what personal data we process, how and on what basis as set out in this policy. The following rights are provided:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to objection;
- rights in relation to automated decision making and profiling.

13.2 Data subjects have the right to access their own personal data by way of a subject access request (see above).

13.3 The right to rectification:

- Data subjects can correct any inaccuracies in their personal data. To do so, they should contact the school or if a member of the Trust's staff, the Trust's HR team.
- Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible. Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.

- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13.4 The right to erasure:

- Individuals, including children, have the right to request that their personal data is erased where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so the data subject should contact the Trust/school (or if a member of the Trust's staff, its HR team).
- The Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:
    - To exercise the right of freedom of expression and information.
    - To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
    - For public health purposes in the public interest.
    - For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
    - The exercise or defence of legal claims.
- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question

13.5 The right to restriction:

- While requesting that their personal data is corrected or erased or are contesting the lawfulness of our processing, a data subject can apply for its use to be restricted while the application is made. To do so, individuals should contact the Trust/school, of if a Trust employee, contact HR.
- In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
- The Trust will restrict the processing of personal data where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.
- If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

- The Trust will inform individuals when a restriction on processing has been lifted.

13.6 The right to object:

- Data subjects have the right to object to data processing where we are relying on a legitimate interest to do so and they think that their rights and interests outweigh the Trusts own interest and wish us to stop. Where personal data is processed foFartificial r the performance of a legal task or legitimate interests, an individual's grounds for objecting must relate to his or her particular situation. The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- Data subjects have the right to object if we process their personal data for the purposes of direct marketing. The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received. The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

13.7 The right to data portability:

- Data subjects have the right to receive a copy of their personal data and to transfer their personal data to another data controller in relation to:
    - personal data that an individual has provided to a controller;
    - processing based on the individual's consent or for the performance of a contract;
    - processing carried out by automated means.
- We will not charge for this and will in most cases aim to do this within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
- Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.
- Personal data will be provided in a structured, commonly used and machine-readable form but the Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

13.8 With some exceptions, individuals have the right not to be subjected to automated decision-making.

13.9 Data subjects will be notified without undue delay of a data security breach concerning their personal data, if the breach is likely to result in a high risk of adversely affecting the individuals' rights and freedoms.

13.10 In most situations we will not rely on consent as a lawful ground to process personal data. If we do however request consent to the processing of personal data for a specific purpose, data subjects have the right not to consent or to withdraw their consent later. To withdraw consent contact the Trust's DPO.

13.11 Data subjects have the right to complain to the Information Commissioner, by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on data subjects' rights and our obligations.

14 Artificial Intelligence

The Trust is aware of the data privacy implications when using generative AI tools, as is the case with any new technology.

If it is strictly necessary to use personal and special category data in generative AI tools within the Trust, the Trust will ensure that the products and procedures comply with data protection legislation and their existing data privacy policies to protect the data.

The Trust will also be open and transparent, ensuring any affected data subjects (pupils/students) understand that their personal or special category data is being processed using AI tools.

15 Biometric recognition systems

Biometric data means personal information resulting from specific technical processing relating to the individual's physical, psychological or behavioural characterisitcs, which allow or confirm the unique identification of that person, such as facial images, voice recognition or fingerprints.

The DPO has completed a data protection impact assessment (DPIA) to identify the additional risks associated with using automated biometric technology and documented his decisions. This DPIA will be reviewed annually together with the policy.

Please see TLT Protection of Biometric Information Policy.

16 CCTV

Please see TLT CCTV Policy.

The Trust currently uses CCTV around our schools as outlined below. The Trust believes that such use is necessary for legitimate business purposes, including:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- for the personal safety of staff, pupils, parents, visitors and other members of the public and to act as a deterrent against crime;
- to support law enforcement bodies in the prevention, detection and prosecution of crime;
- to assist in day-to-day management, including ensuring the health and safety of staff, pupils and others;
- to monitor student behaviour;
- to prevent bullying;
- to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings; and
- to assist in the defence of any civil litigation, including employment tribunal proceedings.

This list is not exhaustive and other purposes may be or become relevant.

Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated by the Trustees to the relevant Headteachers.

Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the centralised Trust IT Department.

17 Photographs and videos

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

The Trust obtains written consent from parents/carers via the completed and signed Admission Form for photographs and videos to be taken of their child for communication, marketing and promotional materials.

The Trust will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

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

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

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified unless consent has been obtained from parents/carers.

18 Data security and storage of records

The Trust is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible to the appropriate individuals. In line with the requirements of the UK GDPR, the Trust also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The Trust has measures in place to protect the security of all personal data and also to manage how records are stored, accessed, monitored, retained, and disposed of to meet its statutory requirements.

Please see **TLT Retention of Records Policy** (a copy of this can be obtained from the Trust's DPO) and **Data and Cyber Breach Prevention Policy**, which detail how 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.

The Trust will only hold data for as long as necessary for the purposes for which we collected it.

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, the Trust will shred sensitive paper-based records; all shredding is collected by a third-party confidential waste specialist to safely dispose of records on the Trust's behalf.

When using a third-party, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19 Questions

Please contact the DPO with any questions about the operation of this Data Protection Policy or UK GDPR or with any concerns that this Data Protection Policy is not being or has not been followed.

Trust employees should always contact the DPO in the following circumstances:

- if they are unsure of the lawful basis which they are relying on to process personal data (including the legitimate interests used by the Trust);
- if they are unsure of the retention period for the personal data being processed;
- if they are unsure about what security or other measures need to be implemented to protect personal data;
- if there has been a personal data breach;
- if they require assistance to deal with any rights invoked by a data subject; and
- if they plan to undertake any activities involving automated processing.

20 Changes to this policy

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.