

Three Counties Academy Trust



Data Protection Policy

#FI20

Last amended 29th September 2026 (v1.0)

Policy lifespan: 1 year. Next full review 28th September 2027.

Version history

Date	Version	Details	Actioned by	PDF to Websites	Word to Governor Hub
29.09.26	1.0	Formatted to house style and checked against model for updates	MF	✓	✓

Contents:

Version history

Policy abbreviations and acronyms

Statement of intent

Member, Trustee, Local Governor and Staff Summary

Parent Summary

1. Legal framework
2. Applicable data
3. Accountability
4. Data protection officer (DPO)
5. Lawful processing
6. Consent
7. The right to be informed
8. The right of access
9. The right to rectification
10. The right to erasure
11. The right to restrict processing
12. The right to data portability
13. The right to object
14. Informing data subjects
15. Information rights requests
16. Data protection complaints
17. Automated decision making and profiling
18. Data protection by design and default
19. Data Protection Impact Assessments (DPIAs)
20. Data breaches
21. Data security

22. Safeguarding

23. Publication of information

24. CCTV and photography

25. Procurement and management of educational technology

26. Cloud computing

27. Use of generative artificial intelligence

28. Data retention

29. DBS data

Monitoring and review

Trust Glossary

Policy abbreviations and acronyms

AI	Artificial Intelligence	DUAA	Data (Use and Access) Act 2025
BCC	Blind Carbon Copy	EdTech	Educational Technology
CFO	Chief Financial Officer	ICO	Information Commissioner's Office
CCTV	Closed Circuit Television	ICT	Information Communication Technology
DBS	Disclosure and Barring Service	IP	Internet Protocol
DFE	Department for Education	MAT	Multi Academy Trust
DPA	Data Protection Act	PECR	Privacy and Electronic Communications Regulations
DPIA	Data Protection Impact Assessment	SAR	Subject Access Request
DPO	Data Protection Officer	TCAT	Three Counties Academy Trust
DSL	Designated Safeguarding Lead	UK GDPR	UK General Data Protection Regulation

NB. Where the term “parent” or “parents” is used this includes those who act as carers or have parental responsibility.

NB. Staff roles noted within this policy may also include those staff performing that role in an ‘Acting’ capacity.

Statement of intent

Three Counties Academy Trust (TCAT) and its schools collect, use, store and otherwise process personal data relating to pupils, parents and carers, employees, applicants, volunteers, Local Governors, Trustees, Members, contractors and other individuals with whom TCAT has a relationship. TCAT recognises the importance of protecting this information and is committed to ensuring that all personal data is handled lawfully, fairly, transparently and securely.

TCAT will process personal data in accordance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation and statutory requirements. Personal data will only be collected and processed where there is an appropriate lawful basis and will be limited to information that is adequate, relevant and necessary for the purpose for which it is required.

In carrying out our educational, safeguarding, employment, governance and statutory functions, TCAT may be required or otherwise permitted by law to share personal data with third parties. These may include local authorities, the Department for Education (DfE), other schools and educational establishments, safeguarding partners, children's social care, health professionals, examination and assessment bodies, regulatory authorities and other organisations where there is a lawful and legitimate reason for doing so. Personal data will not be shared simply because it has been requested; TCAT will ensure that an appropriate lawful basis exists before information is disclosed.

TCAT is committed to upholding the data protection principles set out in the UK GDPR and to respecting the rights of individuals in relation to their personal data. Appropriate technical and organisational measures will be maintained to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, alteration or damage.

Effective data protection is the responsibility of everyone who handles personal data on behalf of TCAT. This policy therefore establishes the framework through which Trustees, Local Governors, employees, volunteers and others acting on behalf of TCAT are expected to protect personal information and comply with TCAT's data protection responsibilities. It is supported, where appropriate, by more detailed procedures, privacy statements, records and guidance.

For the purposes of clarity and consistency, this policy generally uses the collective term "TCAT". Unless the context indicates otherwise, references to "TCAT" or "the Trust" include Three Counties Academy Trust and each of its individual schools, and the requirements of this policy apply across TCAT.

Member, Trustee, Local Governor and Staff Summary

Purpose of the Policy

- Explains how TCAT collects, uses, stores, shares and protects personal data relating to pupils, families, staff, volunteers, Local Governors, Trustees, Members, contractors and others connected to TCAT
- Ensures all personal data is processed lawfully, fairly, transparently and securely in line with data protection legislation, including UK GDPR and the Data Protection Act 2018
- Clarifies that protecting personal data is everyone's responsibility across TCAT and our schools

Key Responsibilities

- Handle personal information carefully and only for legitimate educational, employment, safeguarding, governance or statutory purposes
- Follow TCAT policies, procedures and guidance relating to data protection and information security
- Ensure personal data is accurate, relevant, secure and only retained for as long as necessary
- Seek advice from the CFO or Data Protection Officer (DPO) when unsure how personal data should be processed, shared or retained

Data Protection Principles

Personal data must be:

- Processed lawfully, fairly and transparently
- Collected for specified and legitimate purposes
- Limited to what is necessary
- Accurate and kept up to date
- Retained only as long as required
- Protected through appropriate security measures

Individual Rights

People whose information is held by TCAT have important rights, including:

- The right to be informed about how their data is used
- The right to access their personal information
- The right to request corrections to inaccurate information
- The right to request deletion of information in certain circumstances
- The right to restrict or object to some processing activities
- The right to data portability where applicable

Sharing Information

- Personal data will only be shared where there is a lawful basis to do so
- Information may be shared with organisations such as local authorities, the Department for Education, safeguarding agencies, health services and regulators when appropriate and lawful
- Information should never be shared simply because it is requested by another party

Subject Access Requests and Complaints

- Individuals can request access to information held about them through a Subject Access Request
- Requests and complaints must be recognised and referred promptly to the appropriate person or the DPO
- Complaints relating to data protection will be investigated and responded to in accordance with TCAT procedures

Data Security Expectations

- Keep paper records secure and restrict access to those who need it
- Use secure passwords and approved TCAT systems
- Check recipients carefully before sending confidential information
- Protect personal information when working remotely or off site
- Report any suspected data breach immediately

Safeguarding and Information Sharing

- Data protection law does not prevent information being shared to keep children safe
- Staff must not allow concerns about data protection to delay safeguarding action
- Safeguarding information should be shared lawfully, appropriately and without unnecessary delay where required to protect a child or vulnerable person

Use of Technology, Cloud Services and AI

- New educational technology must be assessed before use where personal data is involved
- Cloud services must meet data protection and security requirements
- Personal, identifiable or sensitive information must not be entered into generative AI systems unless formally assessed and approved by the Trust
- AI outputs must always be reviewed by a human before being relied upon

Data Breaches

- Any loss, unauthorised disclosure, alteration or access to personal data may constitute a data breach
- All suspected breaches must be reported immediately
- TCAT has procedures to investigate breaches and, where required, notify the Information Commissioner's Office and affected individuals

Oversight and Accountability

- TCAT maintains records demonstrating compliance with data protection legislation
- A qualified Data Protection Officer provides advice, monitoring and support across TCAT
- Trustees, Local Governors and staff all play a role in ensuring compliance and protecting personal information

What This Means in Practice

- Think carefully before collecting, sharing or storing personal information
- Only access information needed for your role

- Challenge poor information handling practices
- Report concerns, breaches or uncertainties promptly
- Always balance data protection requirements with the need to safeguard children and fulfil the TCAT's statutory duties

Parent Summary

Why this Policy Matters

- TCAT and our schools collect and use information about pupils and families so they can provide education, safeguarding, pastoral support and meet their legal responsibilities
- We are committed to making sure personal information is handled lawfully, fairly, securely and transparently

How Your Information Is Protected

- Personal information is only collected when there is a valid reason to do so
- Information is only shared when there is a lawful basis and a genuine need
- Appropriate security measures are used to protect both paper and electronic records
- Staff receive guidance and training on handling personal information safely

Your Rights

As a parent, you have the right to:

- Understand how your family's information is used
- Request access to personal information held about you or your child where appropriate
- Ask for incorrect information to be corrected
- Raise concerns if you believe information is not being handled properly
- Complain to TCAT and, if necessary, to the Information Commissioner's Office (ICO)

Keeping Children Safe

- Data protection laws do not prevent schools from sharing information where this is necessary to safeguard a child
- TCAT will share relevant information with appropriate agencies when needed to protect children and young people
- Concerns about data protection must never delay safeguarding action

Photographs, Technology and AI

- TCAT seeks appropriate permission before using pupil photographs or videos
- Any educational technology that uses personal information is assessed before it is introduced
- Personal or sensitive information must not be entered into artificial intelligence systems unless TCAT has formally assessed and approved their use

Data Breaches and Concerns

- TCAT has procedures for identifying, investigating and responding to data breaches
- If a serious breach affects individuals, appropriate action will be taken and notifications made where required by law
- Parents can raise concerns through the TCAT's complaints procedures at any time

What Parents Can Expect

- Clear information about how personal data is used
- Secure handling of information about your child and family
- Respect for privacy and data protection rights
- Prompt action if concerns are raised
- A balanced approach that protects personal information while always prioritising the safety and wellbeing of children

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 \(DPA\)](#)
- [School Standards and Framework Act 1998](#)
- [Freedom of Information Act 2000](#)
- [Data \(Use and Access\) Act 2025 \(DUAA\)](#)
- [Electronic Commerce \(EC Directive\) Regulations 2002](#)
- [The Privacy and Electronic Communications \(EC Directive\) Regulations 2003](#)
- [The Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulations 2004](#)
- [The Education \(Pupil Information\) \(England\) Regulations 2005 \(as amended in 2018\)](#)
- [Protection of Freedoms Act 2012](#)
- [DfE 'Keeping children safe in education'](#)
- [ICO 'Guide to the UK General Data Protection Regulation \(UK GDPR\)'](#)
- [DfE 'Generative artificial intelligence \(AI\) in education'](#)
- [DfE 'Generative AI: product safety standards'](#)
- [DfE 'Data protection in schools'](#)
- [DfE 'The Data Use and Access Act 2025'](#)
- [ICO 'Data \(Use and Access\) Act 2025' guidance](#)

This policy operates in conjunction with the following TCAT and school policies:

- Safe Use of AI Statements
- Safe Use of AI Policy (CU14)
- Records Management Policy (FI2)
- Subject Access Request (SAR) Policy (FI9)
- Freedom of Information Policy (FI10)

- Freedom of Information Publication Scheme (FI10A)
- Privacy Statement Pupils (FI12(A))
- Privacy Statement Parents and Carers (FI12(B))
- Privacy Statement Staff (FI12(C))
- Privacy Statement Volunteers and Visitors (FI12(D))
- Privacy Statement Members, Trustees and Local Governors (FI12(E))
- Privacy Statement Job Applicants (FI12(F))
- Privacy Statement Alumni (FI12(G))
- Privacy Statement CCTV (FI12(H))
- Privacy Statement Website and Cookies (FI12(I))
- Privacy Statement Third-Party Suppliers and Contractors (FI12(J))
- Cyber-Security Policy (FI15)
- Surveillance and CCTV Policy (FI21)
- Device and Technology Acceptable Use Agreement (FI31)
- Complaints Policy and Procedure (GN9)
- Child Protection and Safeguarding Policy and Procedures (SG1)
- Photography and Images Policy (SG9)

2. Applicable data

For the purpose of this policy, **‘personal data’** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

‘Sensitive personal data’ is referred to in the UK GDPR as ‘special categories of personal data’, and is defined as:

- Genetic data
- Biometric data
- Data concerning health

- Data concerning a person's sex life
- Data concerning a person's sexual orientation
- Personal data which reveals:
 - Racial or ethnic origin
 - Political opinions
 - Religious or philosophical beliefs
 - Trade union membership
 - Principles

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 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

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

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

3. Accountability

TCAT will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR, and will provide comprehensive, clear and transparent privacy policies.

TCAT will be able to demonstrate how data is processed as a whole across our MAT and will ensure each individual TCAT school is adhering to the same procedure and that this is being implemented and enforced in line with the wider TCAT policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional
- Could result in a risk to the rights and freedoms of individuals
- Involve the processing of special categories of data or criminal conviction and offence data

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures

- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

TCAT will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy statements, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches
- Records of data protection complaints, including receipt, acknowledgement, enquiries, progress updates, outcomes and remedial action
- Decisions to rely on recognised legitimate interests, including the applicable condition and why the processing is necessary
- Records of significant decisions based solely on automated processing, including the lawful basis and safeguards applied

TCAT will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data
- Pseudonymising personal data as soon as possible
- Ensuring transparency in respect of the functions and processing of personal data
- Allowing individuals to monitor processing
- Continuously creating and improving security features

DPIAs will be used to identify and reduce data protection risks, where appropriate.

4. Data protection officer (DPO)

Schools are required to appoint a DPO who will be the central point of contact for all data subjects and others in relation to matters of data protection.

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws
- Monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed

TCAT uses Schools DPO as the Data Controller for all TCAT schools, with our named DPO being Nicola Cook, Director of Schools DPO.

The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection
- Calculating and evaluating the risks associated with TCAT and the school's data processing
- Having regard to the nature, scope, context, and purposes of all data processing
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed
- Promoting a culture of privacy awareness throughout the school community
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws
- Providing annual training for all staff on the risks, limitations and lawful processing requirements when using generative artificial intelligence (AI) technologies
- Monitoring the school's handling of data protection complaints and advising on the complaints process
- Advising on the use of recognised legitimate interests and significant automated decision-making
- Supporting staff training so that information rights requests and data protection complaints are recognised and referred promptly

The individual appointed as DPO will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to schools.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

The DPO will report to the highest level of management at the trust, which is the Trust Board.

Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

5. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

- 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
- Processing is necessary for a recognised legitimate interest specified in Annex 1 to the UK GDPR, namely responding to a request for disclosure for another organisation's public task or official function; national security, public security or defence; emergencies; preventing, detecting or investigating crime; or safeguarding vulnerable individuals

Where TCAT relies on recognised legitimate interests, we will identify and document the applicable condition and demonstrate that the processing is necessary. Where TCAT is a public authority, we will not use this basis to perform our public tasks or official functions. This basis will not be used for significant decisions based solely on automated processing. Where special category or criminal offence data is involved, TCAT will also identify an appropriate additional condition.

Where a lawful basis requires processing to be necessary, TCAT will ensure that the purpose cannot reasonably be achieved by less intrusive means or by processing less personal data. Consent will not be treated as the default lawful basis where another basis is more appropriate.

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

TCAT will ensure that it has privacy statements established which clearly outline the reasons why it needs to collect personal data. The privacy statement will include the following explicit details:

- Why TCAT needs to collect personal data
- The lawful basis relied upon and, where recognised legitimate interests is used, the applicable condition.
- What TCAT plans to do with the personal data
- How long TCAT will keep the personal data
- Whether TCAT will share the personal data with any external organisations

The privacy statement will be clear and accessible to data subjects. The privacy statement will also be reviewed by TCAT's DPO at least annually and whenever significant changes are made to how TCAT processes the data that it collects.

TCAT will ensure that any parents, pupils and staff whose personal data is included will be notified of any significant changes to the privacy statement or the way in which the school processes the data.

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 to make a data protection complaint to TCAT and to complain to the ICO in relation to any processing

TCAT and our schools have privacy statements for the following groups, which outline the information above that is specific to them:

- Pupils
- Parents
- Staff
- Volunteers
- Visitors
- Members, Trustees and Local Governors
- Job Applicants
- Alumni
- Third-Party Suppliers and Contractors

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted, and a decision made only after seeking further clarification.

Where TCAT relies on:

- 'Performance of contract' to process a child's data, TCAT considers the child's competence to understand what they are agreeing to, and to enter into a contract
- 'Legitimate interests' to process a child's data, TCAT takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place
- 'Recognised legitimate interests' to process a child's data, the school identifies the applicable condition, demonstrates necessity, and puts age-appropriate safeguards in place
- Consent to process a child's data, TCAT ensures that the requirements outlined in the 'Consent' section are met, and TCAT does not exploit any imbalance of power in the relationship between their school and the child

6. Consent

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.

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

TCAT 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.

When pupils and staff join a TCAT school, 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 complete a consent form.

Where TCAT 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, TCAT 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 TCAT on a case-by-case basis, taking into account the requirements outlined above.

7. The right to be informed

Adults and children have the same right to be informed about how TCAT or their school uses their data. The privacy statements supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language, which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy statement:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO
- The purpose of, and the lawful basis for, processing the data
- The legitimate interests of the controller or third party
- Where recognised legitimate interests is relied upon, the applicable recognised legitimate interest condition
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period
- The existence of the data subject's rights, including the right to:
 - Make a data protection complaint to TCAT
 - Lodge a complaint with the ICO
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided – this information will be supplied at the time the data is obtained.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided – this information will be supplied:

- Within one month of having obtained the data
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed
- If the data are used to communicate with the individual, at the latest, when the first communication takes place

8. The right of access

Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. TCAT will verify the identity of the person making the request before any information is supplied.

TCAT will make a reasonable and proportionate search for the requested personal data. It is not required to undertake searches that would be unreasonable or disproportionate in light of the importance of providing access to the information.

A copy of the information will be supplied to the individual free of charge; however, TCAT may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

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

Where a SAR has been made for information held about a child, TCAT will evaluate whether the child is capable of fully understanding their rights. If TCAT determines the child can understand their rights, it will respond directly to the child.

TCAT will respond without undue delay and at the latest within one month of receiving the request. Where TCAT reasonably requires information to confirm the requester's identity, evidence that a third party is authorised to act, or payment of a permitted fee, the response period will begin when that information, evidence or fee is received. The period may be extended by up to two further months where necessary because the request is complex or the individual has made a number of requests. The individual will be informed of any extension and the reasons within the initial one-month period.

Where a request is manifestly unfounded or excessive, TCAT holds the right to refuse to respond to the request. The individual will be informed of this decision 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.

TCAT 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, TCAT 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

TCAT may ask the individual to clarify the personal data requested only where clarification is reasonably required to provide an effective response. The response period will pause on the day clarification is requested and resume on the day after it is received. TCAT will not use clarification to delay a response or require the individual to narrow an otherwise clear request; where the individual does not narrow the request, TCAT will still carry out a reasonable and proportionate search.

TCAT's response will explain the individual's right to make a data protection complaint to TCAT and to complain to the ICO.

9. The right to rectification

Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, TCAT may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. TCAT reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

TCAT will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. TCAT will restrict processing of the data in question whilst its accuracy is being verified, where possible.

Where the personal data in question has been disclosed to third parties, TCAT will inform them of the rectification where possible. Where appropriate, TCAT will inform the individual about the third parties that the data has been disclosed to.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, TCAT 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.

10. The right to erasure

Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

TCAT will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

TCAT 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 establishment, exercise or defence of legal claims

TCAT has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services

Requests for erasure will be handled free of charge; however, TCAT may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

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, TCAT will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

11. The right to restrict processing

Individuals, including children, have the right to block or suppress TCAT's processing of personal data.

TCAT will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until TCAT has verified the accuracy of the data
- Where an individual has objected to the processing and TCAT is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful, and the individual opposes erasure and requests restriction instead
- Where TCAT no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim

In the event that processing is restricted, TCAT 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. TCAT will inform individuals when a restriction on processing has been lifted.

Where TCAT is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

If the personal data in question has been disclosed to third parties, TCAT will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

TCAT reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision 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. The right to data portability

Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. TCAT will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

TCAT will provide the information free of charge.

In the event that the personal data concerns more than one individual, TCAT will consider whether providing the information would prejudice the rights of any other individual.

TCAT will respond to any requests for portability 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, TCAT 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.

13. The right to object

TCAT will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy statement and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information. Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests, recognised legitimate interests, or the performance of a task in the public interest
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics

Where personal data is processed for the performance of a legal task, legitimate interests or recognised legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation
- TCAT will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where TCAT can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- TCAT will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress

Where personal data is processed for direct marketing purposes:

- The right to object is absolute and TCAT will stop processing personal data for direct marketing purposes as soon as an objection is received
- TCAT cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes
- TCAT will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data

Where the processing activity is outlined above, but is carried out online, TCAT will offer a method for individuals to object online.

The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. TCAT will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

Where no action is being taken in response to an objection, TCAT 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.

14. Informing data subjects

TCAT ensures that pupils, parents and staff whose data is processed by our schools are clearly and explicitly informed about how we deal with their personal data. The privacy statement will outline the features and functions of TCAT's use of personal data, but the privacy statement itself must be easily accessible to all who wish to view it.

TCAT will share its privacy statement with pupils:

- On the school website

The school will share its privacy statement with staff through:

- Role application
- Contract acceptance
- Regular appraisal
- The start of each school year
- Staff notice boards and other relevant staff-centric space

15. Information rights requests

As well as the right to rectification, TCAT will recognise that its pupils have information rights, meaning that they have the right to access or amend any personal information that is held about them. The most common of these are SAR.

A pupil can make an information rights request relating to any of the following:

- Changing any inaccurate information that TCAT or their school holds about them
- Removing their personal information or record from TCAT and the school's systems
- Restricting TCAT and the school from processing any data held on the pupil
- Stopping TCAT and the school from processing any personal data entirely

TCAT may ask the individual to clarify the personal data requested only where clarification is reasonably required to provide an effective response. The response period will pause on the day clarification is requested and resume on the day after it is received. TCAT will not use clarification to delay a response or require the individual to narrow an otherwise clear request; where the individual does not narrow the request, we will still carry out a reasonable and proportionate search.

TCAT's response will explain the individual's right to make a data protection complaint to TCAT and to complain to the ICO.

16. Data protection complaints

A data protection complaint is an expression of concern that TCAT has infringed data protection legislation in the way it has collected, used, shared, stored, secured, retained or otherwise processed personal data, or in the way it has responded to an information rights request. The complainant does not need to use legal terminology, refer to legislation, or use a prescribed form in order to make a data protection complaint.

TCAT will provide clear and accessible ways to make a data protection complaint, under our Complaints Policy and Procedure. Complaints made verbally, in writing, by email, through social media or through any other channel will be accepted.

Staff who receive a data protection complaint will record it and refer it without delay to the CFO/DPO or the person responsible for coordinating the response. TCAT will make reasonable adjustments and provide age-appropriate support, where required, and will respond urgently where a complaint raises an immediate safeguarding or security risk.

TCAT will:

- Acknowledge receipt of the complaint within 30 days
- Begin making appropriate enquiries and taking appropriate steps to respond without undue delay; the investigation will not be postponed until the acknowledgement period has expired
- Keep the complainant informed of the complaint's progress and explain any delay without undue delay
- Communicate the outcome without undue delay, including the findings, any action taken or proposed, and the right to complain to the ICO

Where the complainant's identity or a representative's authority is uncertain, TCAT will request only the information reasonably necessary to verify it and will do so promptly.

Where the data protection complaint forms part of a wider complaint, grievance or safeguarding matter, the data protection element will be handled under this section and will not be delayed unnecessarily by the wider process.

Where a complaint concerns processing carried out by a processor or joint controller, TCAT will coordinate with the relevant organisation under the applicable contract or arrangement while retaining responsibility for its own controller obligations.

TCAT will keep a proportionate record of the complaint, acknowledgement, enquiries, evidence, progress updates, outcome and remedial action in line with our Records Management Policy. The DPO will review recurring themes and trends to identify improvements.

Using TCAT's complaints process does not affect the individual's right to complain to the ICO or seek a judicial remedy.

17. Automated decision making and profiling

For the purposes of this policy, a decision is based solely on automated processing where there is no meaningful human involvement in taking the decision. A decision is significant where it produces a legal effect or a similarly significant effect on an individual.

TCAT will not make a significant decision based solely on automated processing unless it has identified and documented an appropriate lawful basis, the processing is necessary and proportionate, and the safeguards in this section are in place. Recognised legitimate interests will not be used as the lawful basis for such a decision.

Where a significant solely automated decision is based entirely or partly on special category data, it will only be made where either the decision is based entirely on processing for which the individual has given explicit consent, or both of the following apply: the decision is necessary for entering into or performing a contract, or is required or authorised by law; and the processing meets the substantial public interest condition in Article 9(2)(g) of the UK GDPR.

TCAT will not use solely automated processing to make a significant decision about a child.

TCAT will conduct a DPIA before introducing significant solely automated decision-making and will assess accuracy, fairness, bias, discrimination, security and the particular risks to children and other vulnerable individuals.

TCAT will ensure that safeguards are in place which:

- Provide the individual with information about the decision
- Enable the individual to make representations about the decision
- Enable the individual to obtain human intervention by TCAT
- Enable the individual to contest the decision

Any human review will be meaningful. The reviewer will be suitably qualified, will consider the relevant information independently, and will have authority to change or reject the automated outcome; a nominal approval will not be sufficient.

TCAT will not use generative AI or another automated system to determine academic grading, behaviour sanctions, admissions, safeguarding decisions or staff appraisals without meaningful human involvement.

When automatically processing personal data for profiling purposes, TCAT will ensure that appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and predicted impact
- Using appropriate mathematical or statistical procedures
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects

TCAT will keep appropriate records of the lawful basis, system logic, personal data used, safeguards applied and any human review.

18. Data protection by design and default

TCAT will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how TCAT has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, TCAT will ensure that only data that is necessary to achieve its specific purpose will be processed.

Where TCAT provides an online service likely to be accessed by children, it will take account of children's higher protection matters when deciding which technical and organisational measures are appropriate. This includes how best to protect and support child users, the fact that children may be less aware of data protection risks, consequences and rights, and their differing needs at different ages and stages of development. TCAT will document how these matters have been considered when designing and operating the service.

TCAT will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices
- Making data protection an essential component of the core functionality of processing systems and services
- Automatically protecting personal data in school ICT systems
- Implementing basic technical measures within the TCAT and school network and ICT systems to ensure data is kept secure
- Promoting the identity of the DPO as a point of contact

- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data

19. Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with TCAT's data protection obligations and meeting individuals' expectations of privacy. DPIAs will be conducted prior to the implementation of any generative AI tools where the processing of personal data is involved, particularly if the AI tool automates decision-making, involves profiling, or carries a risk of bias, inaccuracy, or data misuse.

A DPIA will include specific evaluation of the risks associated with AI systems, including fairness, accuracy, accountability, transparency, and security, in accordance with the DfE's 'Generative artificial intelligence in education (2025)' guidance.

DPIAs will allow TCAT to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to TCAT's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

TCAT will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, TCAT will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

20. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The CEO will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

Effective and robust breach detection, investigation and internal reporting procedures are in place throughout TCAT, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Where TCAT faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of TCAT becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Where notifying an individual about a breach to their personal data, TCAT will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

TCAT will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

TCAT will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

21. Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access, and will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up. Where digital data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, TCAT enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Where possible, staff, trustees and governors will not use their personal laptops or computers for trust purposes. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

If staff, trustees and governors need to use their personal laptops for trust purposes, particularly if they are working from home, they will bring their device into work before using it for work to ensure the appropriate software can be downloaded and information encrypted.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents should be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information staff will always check that the recipient is correct before sending.

Before sharing data, all staff will ensure:

- They are allowed to share it
- That adequate security is in place to protect it
- Who will receive the data has been outlined in a privacy statement

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from TCAT premises accepts full responsibility for the security of the data.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of TCAT containing sensitive information are supervised at all times.

The physical security of TCAT's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism, burglary or theft is identified, extra measures to secure data storage will be put in place.

TCAT will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

TCAT takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action. The Chief Finance Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

When disposing of data, paper documents will be shredded or incinerated, and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets.

TCAT holds the right to take the necessary disciplinary action against a staff member if they believe them to be in breach of the above security measures.

22. Safeguarding

TCAT understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

TCAT will identify and document the Article 6 lawful basis for safeguarding processing and, where special category or criminal offence data is involved, the relevant additional condition. Where recognised legitimate interests is relied upon, we will document the safeguarding condition and why the processing is necessary; where acting as a public authority, TCAT will not use this basis to perform its public tasks or official functions.

TCAT will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The Trust Board will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner

TCAT will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

TCAT will identify and document the lawful basis for safeguarding processing and, where special-category or criminal-offence data is involved, the applicable additional condition.

TCAT will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a child at risk. TCAT will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy and Procedures.

Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, TCAT will seek independent legal advice.

23. Publication of information

TCAT publishes a Freedom of Information Publication Scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures

- Minutes of meetings
- Annual reports
- Financial information

Classes of information specified in the Freedom of Information Publication Scheme are made available quickly and easily on request.

TCAT will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to the TCAT or school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

24. CCTV and photography

TCAT understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

TCAT notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All accessed CCTV footage will be kept for six months for security purposes; the Chief Finance Officer is responsible for keeping the records secure and allowing access.

Before TCAT is able to obtain the data of pupils or staff, it is required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

TCAT will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them. If TCAT wishes to use images or video footage of pupils in a publication, such as a website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil. Precautions, as outlined in the Photography and Images Policy, are taken when publishing photographs of pupils, in print, video or on TCAT or school websites.

Images captured by individuals for recreational or personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

Parents and others attending TCAT school events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to any TCAT school.

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

25. Procurement and management of educational technology

For the purposes of this policy, “**EdTech**” includes digital tools and systems used to support or deliver education, learning, communication, assessment, or school administration. Any EdTech tool that processes personal data will be assessed and approved before it is purchased, trialled or introduced. The CFO/DPO will be consulted from the earliest stage and throughout implementation. DSLs and the Senior ICT Technician will also be involved where safeguarding, online safety, or security risks are relevant.

Before approving an EdTech tool, TCAT will establish and document:

- The educational purpose of the tool and the categories of personal data it will process, including whether special category data is involved
- Why each category of data is necessary and proportionate, ensuring that optional data fields and non-core features that are not required are disabled by default
- The lawful basis for each processing activity and, where relevant, the condition for processing special category data
- How personal data will flow through the service, who will have access to it, where it will be stored or processed, and whether any international transfers will take place
- Whether TCAT, the supplier or any other party acts as a controller, joint controller, processor, or sub-processor for each part of the service
- Whether the tool uses AI, profiling or automated decision-making and, where it does, whether the requirements in the ‘Automated decision-making and profiling’ and ‘Use of generative artificial intelligence (AI)’ sections of this policy are met

A DPIA will be completed before approval where the processing is likely to result in a high risk to the rights and freedoms of individuals. TCAT will not proceed until identified risks have been reduced to an acceptable level. The DPIA will be reviewed and updated where the tool, its features, the supplier’s processing, or the categories of personal data change.

TCAT will undertake proportionate due diligence on the supplier and will require sufficient information to verify that the tool meets TCAT’s and the school’s data protection, security, and safeguarding requirements. This will include considering whether:

- Data protection by design and by default is built into the tool

- Appropriate security measures are in place, including encryption, secure authentication, audit logging, and systems for detecting unusual or unauthorised activity, with suitable independent assurance where available
- Pupil-facing services provide appropriate filtering, monitoring, moderation, and audit trails, and meet relevant age-appropriate design standards where the supplier acts as a controller or joint controller
- The supplier can support TCAT and the school in responding to information rights requests and data protection complaints, investigating incidents and demonstrating compliance
- Where AI is used, the supplier can explain how outputs are moderated, whether personal data is used to train the model, how inaccuracies and bias are mitigated, and what controls and monitoring are available to TCAT and the school

Before personal data is shared, TCAT will ensure that a written contract or data processing agreement clearly allocates responsibilities and covers:

- TCAT's documented instructions, confidentiality requirements, and access by authorised supplier staff
- Security measures, the use and approval of sub-processors, and any international transfer arrangements and safeguards
- The supplier's breach notification timescales and assistance with investigation, mitigation, and reporting
- Support for data subject rights and data protection complaints, and TCAT's ability to obtain, correct, restrict, erase or export data where required
- Retention, return, and secure deletion requirements, including agreed arrangements for backups, caches, and archives
- Audit, assurance, and compliance information required by TCAT

When an approved tool is implemented, access will be limited to authorised users and only the data fields and features necessary for the agreed purpose will be enabled. Privacy statements and other information provided to pupils, parents, staff, and other users will be updated where required, and users will receive appropriate instructions or training.

TCAT will monitor approved EdTech tools and suppliers at planned intervals and when changes or updates are proposed. Reviews will cover security, performance, processing activities, sub-processors, new features, and contractual compliance. Features that involve additional personal data will not be enabled automatically. Where processing changes, the school will reassess the lawful basis and risks and will update the DPIA, privacy statements, and other relevant policies or information as appropriate.

At the end of a contract or when changing supplier, TCAT will follow an agreed exit plan. Personal data will be securely returned or transferred within agreed timescales, access will be revoked, and any remaining copies held by the supplier, including backups, caches, and archives, will be securely deleted. TCAT will obtain confirmation of deletion and retain an appropriate record of the completed exit process.

TCAT will not procure or continue using an EdTech tool where the supplier cannot provide sufficient information, meet TCAT and the school's requirements, or reduce identified risks to an acceptable level.

26. Cloud computing

For the purposes of this policy, '**cloud computing**' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves TCAT schools accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. When assessing any cloud-based or AI-powered service, TCAT will ensure that the provider demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data, and allows TCAT to audit or verify compliance where necessary. The use of any cloud services which involves AI processing will be subject to a prior risk assessment and will require a DPIA where personal data is involved. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave TCAT.

All files and personal data will be encrypted before they leave a TCAT device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on TCAT devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert TCAT should unauthorised access, deletion or modification occur and ensure ongoing compliance with TCAT's policies for the use of cloud computing.

TCAT's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the TCAT's Data Protection Policy
- Confirm that the service provider will remove all copies of data, including back-ups, if requested
- Find out what will happen to personal data should TCAT decide to withdraw from the cloud service in the future
- Assess the level of risk regarding network connectivity and make an informed decision as to whether TCAT is prepared to accept that risk
- Monitor the use of TCAT's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the CEO

27. Use of generative artificial intelligence (AI)

TCAT recognises that generative AI technologies involve the processing of extensive datasets and may pose increased risks to data privacy and security.

Staff and pupils must not input personal, identifiable, or sensitive data into generative AI platforms unless the system has been formally assessed, and explicit approval has been granted following a full DPIA.

Only AI systems that meet UK GDPR standards and have been assessed for data minimisation, security, transparency, and retention practices will be used in TCAT and our schools' operations.

Use of generative AI tools must comply with TCAT's Device and Technology Acceptable Use Agreement. Individuals must not rely solely on AI-generated outputs without appropriate human oversight and validation.

Any incidents, breaches, or concerns arising from the use of AI tools must be reported immediately to the DPO and will be investigated in line with TCAT's data breach procedures.

28. Data retention

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former pupils or employees of a TCAT school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

29. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Monitoring and review

Lifespan of Policy: 1 Year

At any point this policy is updated or fully reviewed, it will be updated on the main TCAT website and will automatically update on all TCAT school websites simultaneously.

Where an annual check or other check results in minor changes, the Version History will be reviewed and updated with a change in the number following the decimal point, for example, v1.1 ⇒ v1.2. Where the policy is reviewed in full, then the number before the decimal point will change and reset, for example v1.4 ⇒ v2.0.

Any changes made by the CEO in collaboration with the Board Appointed Trustee will be passed to the Trust Board for ratification and subsequently be notified to Clerks to Local Governing Bodies and Headteachers/Heads of School.

The next scheduled full review date for this policy is 28th September 2027.

Date approved by the Board Appointed Trustee: 29th September 2026.

To be ratified and recorded in the minutes at the first Trust Board Meeting after 29th September 2026.

Trust Glossary

AA	Admissions Authority	H&S	Health and Safety
AAI	Adrenaline Auto-Injector (Epi Pen)	HoS	Head of School
ACM	Asbestos Containing Materials	HSE	Health and Safety Executive
AHT	Assistant Headteacher	ICO	Information Commissioners Office
AIR	Attendance Intervention Reviews	IDSR	Inspection Data Summary Report
APDR	Assess Plan Do Review Cycle	IHP	Individual Healthcare Plan
APIs	Application Programming Interfaces	IRMS	Information and Records Management Society
ASC	Autistic Spectrum Condition	IWF	Internet Watch Foundation
ASP	Analyse School Performance	KCSIE	Keeping Children Safe in Education
ATH	Academy Trust Handbook	KS1/2/3/4	Key Stage 1/2/3/4
BAME	Black, Asian and Minority Ethnic Backgrounds	LAC	Looked After Child
BAT	Board Appointed Trustee	LADO	Local Authority Designated Officer
BCP	Business Continuity Plan	LGB	Local Governing Body
BFR	Budget Forecast Return	LLC	Low-Level Concerns
CEO	Chief Executive Officer	LSA	Learning Support Assistants
CFO	Chief Financial Officer	MASH	Multi-Agency Safeguarding Hub
CIF	Condition Improvement Fund	MAT	Multi-Academy Trust

CIN	Child in Need	MFA	Multi-Factor Authentication
CLA	Children Looked After	MFL	Modern Foreign Language
CMIE	Child Missing in Education	NCSC	National Cyber Security Centre
COO	Chief Operating Officer	NoV	Note of Visit
COSHH	Control of Substances Hazardous to Health	NPQ	National Professional Qualifications
CP	Child Protection	PA	Persistent Absence
CPD	Continuing Professional Development	PAN	Published Admission Number
CPOMS	Child Protection Online Management System	PECR	Privacy and Electronic Communications Regulations
CSCS	Children's Social Care Services	PEP	Personal Education Plan
CSE	Child Sexual Exploitation	PEEP	Personal Emergency Evacuation Plan
CTIRU	Counter-Terrorism Internet Referral Unit	PEx	Permanent Exclusion
CWD	Children with Disabilities	PP	Pupil Premium
CYPMHS	Children and Young People's Mental Health Services	PPG	Pupil Premium Grant
DBS	Disclosure and Barring Service	PSHE	Personal, Social and Health Education
DDSL	Deputy Designated Safeguarding Lead	PSED	Public Sector Equality Duty
DfE	Department for Education	PTFA	Parent, Teacher and Friends Association
DHT	Deputy Headteacher	QA	Quality Assurance

DSE	Display Screen Equipment	RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations
DSL	Designated Safeguarding Lead	RHE	Relationships and Health Education
DPO	Data Protection Officer	RPA	Risk Protection Arrangement
EAL	English as an Additional Language	RSHE	Relationships, Sex and Health Education
ECT	Early Career Teacher	SA	Severely Absent
EDIB	Equality, Diversity, Inclusion and Belonging	SALT	Speech and Language Therapist
EHA	Early Help Assessment	SARC	Sexual Assault Referral Centre
EHENA	Education, Health and Care Needs Assessment	SBM	School Business Manager
EHCP	Education, Health and Care Plan	SCC	Standard Contractual Clause
EHE	Elective Home Education	SCITT	School-Centred Initial Teacher Training
ELSA	Emotional Literacy Support Assistant	SCR	Single Central Record
ESFA	Education and Skills Funding Agency	SDP	School Development Plan
EVC	Educational Visit Coordinator	SDQ	Strengths and Difficulties Questionnaire
EWOSSE	Education Welfare and Safeguarding Support Officer	SEF	Self-Evaluation Form
EYFS	Early Years Foundation Stage	SEMH	Social, Emotional, and Mental Health
FBV	Fundamental British Values	SENCO	Special Educational Needs Coordinator
FFT	Fischer Family Trust	SEND	Special Educational Needs and Disabilities

FGM	Female Genital Mutilation	SIP	School Improvement Partner
FGMPO	FGM Protection Order	SLA	Service Level Agreement
FOI	Freedom of Information	SLCN	Speech, Language and Communication Needs
FSM	Free School Meals	SLT	Senior Leadership Team
FTS	Find a Tender Service	SPOC	Single Point of Contact
GAG	General Annual Grant	STEM	Science, Technology, Engineering and Maths
GDPR	General Data Protection Regulation	TA	Teaching Assistant
GIAS	Get Information about Schools	TAC	Team Around the Child
HASH	Herefordshire Association of Secondary Heads	TCAT	Three Counties Academy Trust
HBA	Honour Based Abuse	TUPE	Transfer of Undertakings (Protection of Employment)
HR	Human Resources	VSH	Virtual School Headteacher