



Triumph Learning Trust

Aspiration - Collaboration - Innovation

Monitoring Policy

Policy Details

Policy Level	Trust
Document Approver	Trust Board
Document Status	Final
Applicable to	All Trust Employees
Review Frequency	Every Year

Revision History

Revision	Date	Details	Owner	Approved by
0	April 2025	First Issue	Laura Withington E&CM	PIC
1	June 2026	Revision 1	Laura Withington E&CM	ARC

Contents

1. Introduction	3
2. Scope of Policy	3
3. Responsibilities	3
4. Monitoring of IT Systems	3
Planning Monitoring Systems	4
Access to Systems Data.....	5
Monitoring Data Disclosures.....	5
5. CCTV	6
Planning CCTV Systems	6
CCTV Privacy Notices	7
Access to CCTV Recordings	7
CCTV Footage Disclosures.....	7
6. Review of Systems	8
7. Complaints	8
8. Related Policies	8

1. Introduction

This policy is concerned with the use and governance of surveillance technology, and the processing of Personal Data which has been collected by using surveillance technology. This policy is written in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and guidance issued by the Information Commissioner's Office (ICO) relating to monitoring and video surveillance. The Trust's Monitoring Policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. The Trust reserves the right to amend its content at any time.

Employees who are found to infringe this policy knowingly or recklessly may face disciplinary action. Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. The school only uses surveillance in the context of CCTV and e-monitoring software. Any covert monitoring undertaken in such circumstances will be managed separately and is outside the scope of this policy. and therefore this policy does not cover the use of such technology.

2. Scope of Policy

This policy applies to all trust employees (both those employed directly by the trust and those employed on behalf of the trust by a local authority (or other such body), any authorised agents working on behalf of the trust, including temporary or agency staff, governors, volunteers, and third-party contractors.

3. Responsibilities

The Trust recognises its responsibility to establish and maintain appropriate monitoring arrangements which are lawful, necessary, proportionate and transparent. The Trust is committed to ensuring monitoring activities are undertaken fairly and consistently.

The Trust Strategic IT Manager and School Operations Managers are responsible for providing advice and guidance under this policy and reviewing and updating the policy as required.

The Board of Trustees, as a corporate body, has the responsibility to set the strategic direction and objectives of all matters across the Trust.

The CEO takes overall responsibility for the implementation of policies and procedures, providing reports as appropriate to Trustees in relation to this policy.

The Headteachers are responsible for the implementation and the compliance with this policy within their school ensuring that those staff who are responsible for and involved in the operation of this policy understand and comply with its requirements.

All employees have a responsibility to comply with this policy and to co-operate with the schools Leadership and Management on all matters relating to this policy.

4. Monitoring of IT Systems

The IT systems, infrastructure and their contents are the property of the Trust and are provided to assist the performance of an employee's work. The Trust's systems provide the

capability to monitor telephone, e-mail, voicemail, web, and other communications traffic. For business reasons, and to perform various legal obligations in connection with our role as a Trust and as an employer, use of the Trust's systems including the telephone and computer systems, and any personal use of them, is electronically monitored from time to time. The Trust reserves the right to monitor and occasionally intercept network traffic on all aspects of its telephone and computer systems, whether stored or in transit. The Trust reserves the right to monitor and, where permitted by law, intercept communications on its systems where this is necessary, proportionate and lawful. Such monitoring will be undertaken in accordance with UK GDPR, the Data Protection Act 2018, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and other applicable legislation. In accordance with the specific monitoring provisions contained in members of staff's individual contracts of employment, monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for business purposes. Staff are referred to their individual contract of employment for further details. Regular sweeps will be made of the ICT systems, including internet activity logs to check for inappropriate files or domain names. Where such files are located, further action as is necessary will be taken to ascertain the contents and if necessary to remove them. The Trust reserves the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is non-exhaustive):

- To monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy
- To find lost messages or to retrieve lost messages due to computer failure
- To assist in the investigation a reasonable suspicion of breach of the law, this policy, or another Trust policy
- To comply with any legal obligation
- To maintain operational effectiveness
- To safeguard pupils and staff
- To protect Trust Systems from cyber threats and unauthorised access
- To investigate suspected data breaches
- To ensure compliance with statutory and regulatory requirements

Planning Monitoring Systems

Any new implementation of systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA).

The school has various statutory responsibilities to protect the privacy rights of data subjects. Therefore, during this planning phase, the school will consider:

- The purpose of the system and any risks to the privacy of data subjects
- The system must be installed in a way which meets the requirement(s) of the intended

purpose(s) and not exceed the intended purpose(s)

- The obligation to ensure that the system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example, the system must record with sufficient detail to perform its task
- The system must also have a set retention period and, where appropriate, the school must also be able to delete this information before the end of the retention period to comply with the rights of data subjects
- That the school will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific system data if requested. If a data subject's activity is captured and recorded by the system, then that individual also has the right to request a copy of that data under subject access provisions

Access to Systems Data

System data will only be accessed to comply with the specified purpose. For example, if the purpose of maintaining the monitoring system is to safeguard children, then the data must only be examined where there is evidence that a child is at risk.

The system will have a nominated Information Asset Owner who will be responsible for the governance and security of the system. The Information Asset Owner will authorise officers to access the system data either routinely or on an ad-hoc basis.

Users should be aware that ICT service staff with the appropriate privilege and when occasionally required to do so, will access all files stored on a computer or personal network folder. These staff will take all reasonable steps to maintain the privacy of users. Proxy access to staff files including emails will only be given when authorisation is obtained from the Chief Executive Officer and Headteachers. Such action will normally only be granted in the following circumstances:

- A suspected breach of the law or serious breach of this or another Trust policy
- At the lawful request of a law enforcement agency e.g., the police or security services

Monitoring Data Disclosures

A request by individuals for system data that includes their activity should be regarded as a subject access request (SAR). For more information on the right of access for individuals refer to the School's Information Policy. If the school receives a request from another agency (for example a law enforcement agency) for system data, then it will confirm the following details with that agency:

- The purpose of the request
- That agency's lawful basis for processing the data.
- Confirmation that not receiving the data will prejudice their investigation
- Whether the school can inform the data subject of the disclosure, and if not, the reasons for not doing so. The school will liaise with its appointed Data Protection

Officer should it have any concerns about such requests.

5. CCTV

The trust uses [24 hour] CCTV surveillance in its premises to ensure that the grounds are safe, and to tackle and prevent criminal damage or vandalism of trust property. Triumph Learning Trust operates all its premises in accordance with UK law. The trust's CCTV systems comply with the Information Commissioners Office document The Trust's CCTV systems operate in accordance with current guidance issued by the Information Commissioner's Office.

Triumph Learning Trust is committed to the safety of staff, students, parents, and visitors on all its premises. As a public body, The Trust has a duty to protect assets purchased by UK taxpayers.

Cameras are positioned to minimise recording beyond school boundaries unless such recording is necessary, proportionate and justified for the stated purpose of the system. It is important that all staff understand that whilst on the premises, they may be recorded from time to time. There are, however, strict security controls over this recorded data.

Planning CCTV Systems

Any new implementation of CCTV systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA).

The trust has various statutory responsibilities to protect the privacy rights of data subjects. Therefore, during this planning phase, the trust will consider:

- The purpose of the system and any risks to the privacy of data subjects
- That there are statutory requirements placed on the location and position of cameras. This means that cameras must be positioned to meet the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s)
- The obligation to ensure that the CCTV system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example, the system must record with sufficient resolution to perform its task
- The system must have a defined retention period. The standard retention period is 28 days for external cameras and 32 days for internal cameras unless footage is required for an investigation, safeguarding concern, legal proceedings or another lawful purpose.
- That the school will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific footage if requested. If a data subject is captured and recorded by the system, then that individual also has the right to request a copy of that footage under subject access provisions

The trust will ensure that a contract will be agreed between the school (as Data Controller) and the CCTV system provider. Consideration should also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation. Data Processing clauses must be included within the written contract if the provider will be processing (e.g. monitoring, storing, accessing) the data on behalf of the school

CCTV Privacy Notices

The processing of personal data requires that the individuals that the data relates to (in this case any individuals captured by the CCTV) are made aware of the processing. Therefore, the use of CCTV systems must be visibly signed. The signage will include the purpose for the system (e.g. the prevention or detection of crime), the details of the organisation operating the system and who to contact about the system (including basic contact details). The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded. A more detailed Privacy Notice for the use of CCTV must be maintained with the intention of informing data subjects of their rights in relation to surveillance data

Access to CCTV Recordings

CCTV footage will only be accessed to comply with the specified purpose. For example, if the purpose of maintaining a CCTV system is to prevent and detect crime then the footage must only be examined where there is evidence to suggest criminal activity having taken place. The CCTV system will have a nominated Information Asset Owner (Trust Strategic IT Manager) who will be responsible for the governance and security of the system. The Information Asset Owner will authorise officers (Trust Estates and Compliance Manager, Operations Manager, Headteacher, Deputy Headteachers, and Assistant Headteachers) to access CCTV footage either routinely or on an ad-hoc basis.

CCTV Footage Disclosures

A request by individuals for CCTV recordings that include footage of them should be regarded as a subject access request (SAR). For more information on the right of access for individuals captured on CCTV, refer to the trust's Data Protection Policy.

All disclosures of CCTV footage will be documented and retained in accordance with the Trust's records management arrangements.

If the school receives a request from another agency (for example a law enforcement agency) for CCTV recordings, then it will confirm the following details with that agency:

- The purpose of the request
- That agency's lawful basis for processing the footage
- Confirmation that not receiving the information will prejudice their investigation
- Whether the School can inform the data subject of the disclosure, and if not, the reasons for not doing so

The school will liaise with its appointed Data Protection Officer should it have any concerns about such requests.

Each School in the Trust will record all requests to view CCTV footage including the identity of the requester, the date of request and the outcome of the approval process including the date of disclosure of footage where approved. The requests must be forwarded to the relevant school Headteacher for approval.

The date, time, location of the requested footage and identity of the requester must be recorded as well as a full record of the request made (i.e. letter or email received). Footage exported from the CCTV system for any purpose other than for handover to the Police must be reviewed to ensure that the rights of those depicted in the footage are protected. If there is any doubt such cases must be referred promptly to the Trust Strategic IT Manager

If disciplinary action results from information gathered through monitoring, the member of staff will be given the opportunity to see or hear the information in advance of the disciplinary hearing and to make representations about it.

Employees are informed of monitoring activities through employment contracts, privacy notices, acceptable use agreements and Trust policies.

6. Review of Systems

Surveillance systems will be reviewed at least annually and following any significant change to the system, legislation or guidance by the asset owner to ensure that the systems still comply with Data Protection legislation and national standards. It is the responsibility of the Information Asset Owner to ensure reviews are completed and evidence of those reviews taking place are maintained.

7. Complaints

Complaints by individuals about the use of surveillance systems, or the way surveillance data is processed, should be treated as a data protection concern and the school's data protection officer should be made aware. Please see the trust privacy notices and data protection policy for the DPO (Data Protection Officers) contact details.

Individuals who remain dissatisfied following the Trust's complaints process may raise concerns with the Information Commissioner's Office.

8. Related Policies

- Data Protection Policy
- ICT Acceptable Use Policy
- Information Security Policy
- Staff Code of Conduct
- Disciplinary Policy
- Records Retention Schedule
- CCTV Privacy Notice
- Employee Privacy Notice