Atomix Educational Trust

Surveillance Policy

Version 1.1 2026

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. The policy is written in accordance with various Data Protection legislation, which includes but is not limited to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), and the Information Commissioner's Office's (ICO) surveillance code of practice.

Queries about this policy should be directed to the Atomix Educational Trust(the Trust) Data Protection Officer (Veritau Ltd SchoolsDPO@veritau.co.uk)

Scope

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.

This Policy will refer to all individuals within scope of the policy as 'employees'. Employees who are found to knowingly or recklessly infringe this policy 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 Trust only uses surveillance in the context of CCTV and e-monitoring software.

The Trust does not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

CCTV

The purpose of the CCTV system is crime prevention and detection. This includes the apprehension and prosecution of offenders on the premises, ensuring security and safety of campus users, maintaining the security of the premises by preventing crime and enabling subsequent investigation.

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 should record with sufficient resolution to perform its task.

- The system must also have a set retention period (one month) and, where appropriate, the Trust must also have the ability to delete this information prior than the set retention period in order to comply with the rights of data subjects.

- That the Trust 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.

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 must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

The CCTV 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 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 Information Policy.

If the Trust 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 Trust can inform the data subject of the disclosure, and if not, the reasons for not doing so.

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

Access & Review of CCTV

CCTV systems can be reviewed where there is a genuine reason to do so by a designated member of staff from each site at the trust. This may include for safeguarding purposes or in regard to investigating potential criminal offences. The staff member(s) designated to this must complete the CCTV review log which is available to them at each site. An example of the CCTV review form is included in Appendix 1.

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 Trust's data protection officer should be made aware. The Trust's Data Protection Officer is: SchoolsDPO@veritau.co.uk

Records of Processing

The Trust has a duty under Article 30 of the GDPR to ensure that all instances of data processing activity is recorded for regulatory inspection where required. The Trust maintains an information asset register in order to fulfil this requirement.

The Trust will ensure that the use of surveillance systems is recorded on their information asset register.

Related Documents

Employees who are responsible for planning, maintaining, or reviewing the implementation of a surveillance system are encouraged to read the following related documents prior to implementation:

- ICO Surveillance Code of Practice (External Link)
- The School's Data Protection Impact Assessment (DPIA) Template (available through Veritau)

Date of Last Approval/Revision	June 2026
Review interval (years)	1 yearly
Responsible Officer	Director of Operations
Approval/review body	CET/ Trust Board approval 30 June 2026
Date of next review	June 2027
Public File location	Atomix Educational Trust Sharepoint/ Websites/Staff Handbook

Appendix 1 – CCTV System Review Log Atomix Educational Trust

CCTV review Log

Reference number	Name of person reviewing CCTV	Date of Review	Camera location	Start time of review	End time of review	Reason for review	CCTV Downloaded? (Yes/No)	Reason for download	Footage passed on to outside agencies? (Yes/No)	Agencies names the data was shared with	Reason for data being shared with