CCTV Policy

Author / Responsible Person	**Chief Information Officer**
Ratified by	**Chief Executive Officer**
Date Ratified	**September 2023**
Next Review Date	**September 2024**
Review Cycle	**Annual**

1.0 Context Future Academies (the Trust) know the public expect CCTV to be used responsibly with proper safeguards in place and has developed this CCTV policy to comply with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) to inspire confidence that it is using CCTV responsibly.

Images of people are covered by the Data Protection Act and General Data Protection Regulation (GDPR) and so is information about people which is derived from images, for example, vehicle registration numbers.

2.0 Introduction

The Trust is fully committed to the safety of its staff, students/pupils and visitors and to this extent has invested in the security of its buildings and facilities. The purpose of this policy is to regulate the management, operation and use of CCTV within the Trust.

Under the Protection of Freedoms Act 2012 the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the Data Protection Act, General Data Protection Regulation (GDPR) and the Information Commissioner's Office (ICO) has issued a code of practice on compliance with legal obligations under that Act. The use of CCTV by schools is covered by the Act, regardless of the number of cameras or how sophisticated the equipment is.

All cameras may be monitored and are only available for use by approved members of staff. The CCTV system is owned by the Trust and will be subject to a review annually.

3.0 Persons Responsible

3.1 System Controller

Each Principal is herein named the System Controller at each academy and is responsible for the implementation and enforcement of this policy within their respective academies.

3.2 System Manager

The System Controller may name an individual System Manager for the day-to-day management of the CCTV systems.

3.3 System User

The System Controller has the authority to grant access to specific individuals (System User) to view and access recordings. Each individual will be given a separate account for accessing the system when that feature is available.

3.4 User Responsibilities

All users of the CCTV system have the following responsibilities:

- To uphold the arrangements of this policy.
- To handle images/data securely and responsibly, within the aims of the policy. Staff need to be aware that they could be committing a criminal offence if they misuse CCTV images.

- To uphold the recorded procedure for subject access requests.
- To attend training/refresher sessions as required.
- To report any breach of this policy or procedure to the System Controller.

4.0 Objectives of the CCTV System

The Trust uses CCTV equipment to provide a safer, more secure environment for students/pupils, staff and visitors, to prevent bullying, vandalism and theft. Essentially the system is used to:

- Protect the Trust's buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption.
- Support the police in a bid to deter and detect crime.
- Assist in identifying, apprehending and prosecuting offenders.
- Safeguard students/pupils, staff and the public.
- Monitor behaviour where there is cause for concern.
- Assist in the usage and management of Trust buildings on a day-to-day basis.

The Trust does not have hidden cameras.

5.0 Location

Cameras are located in those areas where each academy has identified a need. The academies' CCTV systems are solely used for the purposes identified above.

Changing areas and toilets would not normally be covered, but open shared toilet areas may be, if deemed necessary by local management

Classrooms would not normally be covered and would only be for security reasons, not to monitor the performance of the teachers. The exception being those classes with expensive assets within the class, such as ICT suites, where the protection of the assets is the driver.

6.0 Identification

In areas where CCTV is used the Trust will ensure that there are prominent signs placed at the entrance of the CCTV zone. The signs will be:

- Clearly visible.
- Contain details of the organisation operating the scheme and who to contact about the scheme.

7.0 Image Storage and Retention

Recorded images will be stored in a way that ensures their integrity and in a way that allows specific times and dates to be identified. Access to live images is restricted to a list of approved users unless the monitor displays a scene which is in plain sight from the location

of the monitors. Recorded images can only be viewed in a restricted area by those staff authorised by the System Manager. The recorded images are viewed only when there is a clear reason for this to happen.

The Trust reserves the right to use images captured on CCTV where there is activity that the Trust cannot be expected to ignore such as potential criminal activity, safeguarding, gross misconduct or behaviour which puts others at risk. Images retained for evidential purposes will be retained in a locked area accessible by the System Controller or System Manager only. Where images are retained, the System Controller will ensure the reason for its retention is recorded, along with where it is kept, any use made of the images and finally when it is destroyed.

Neither the Data Protection Act nor the Information and Records Management Society prescribe any specific minimum or maximum periods which apply to CCTV recorded images. CCTV images are usually retained for a period of between 7-28 days depending on the resolution of the footage and the capacity of the storage device. All CCTV will be deleted automatically after 28 days, with the exception of recordings taken offline for evidence/investigation.

8.0 Disclosure

Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

8.1 Academy Staff

Viewing of recorded images by members of staff can only be authorised by the System Controller or those with delegated access. Disclosure will only be granted if it is consistent with the objectives of the CCTV system.

8.2 Third Parties

Disclosure of the recorded images to third parties can only be authorised by the System Controller. Disclosure will only be granted if either:

- Its release is fair to the individuals concerned; or
- There is an overriding legal obligation (e.g. information access rights); or
- It is consistent with the purpose for which the system was established.

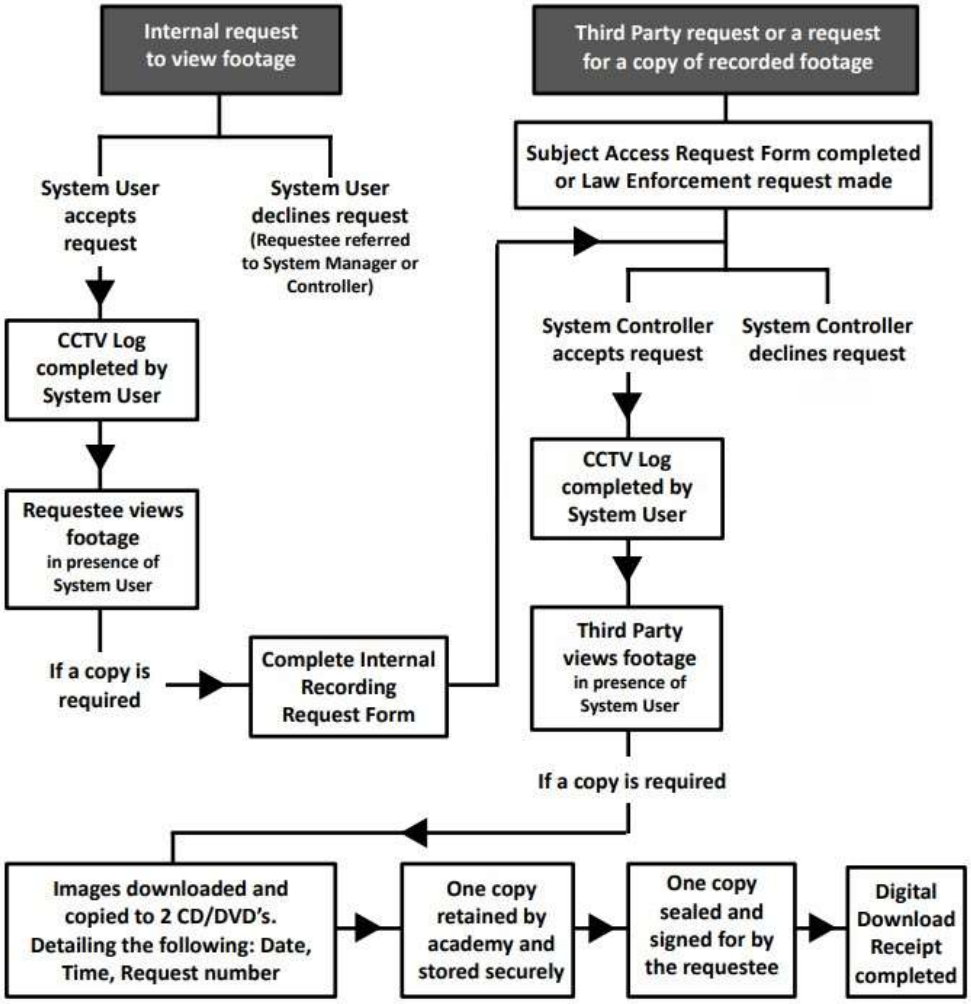
9.0 Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom “personal data” relate) with a right to data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made in writing to the academy’s Data Protection Co-ordinator (see Subject Access Request form, Appendix 1) and will be dealt with in accordance with the Trust’s Data Protection policy. All data for subjects not part of the SAR will be anonymised or redacted. The Subject has a right to see their own images, but not that of others.

Specialist software and skills may be required to redact other subjects in the footage.

9.1 The Request Procedure

Initial request for disclosure:



A log should be kept of viewings to include:

- Date and time of viewing
- Name/s of the person/s viewing the images.
- The reason for the viewing
- The outcome, if any, of the viewing

10.0 System Maintenance and Monitoring

The Trust undertakes regular audits to ensure that the use of CCTV continues to be justified. The audit includes a review of:

Its stated purpose.

- The location of cameras.
- The images recorded and the length of time they may be stored for.
- CCTV policy and procedure.

The CCTV systems are owned by the Trust.

11.0 Complaints

Any complaints about an academy's CCTV system should follow the Future Academies Complaints policy.

---END---