CCTV Policy

Contents

1. Introduction

Futura Learning Partnership (the trust) uses closed circuit television (CCTV) images to monitor the conduct of site users in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to trust property.

2. Policy aims and objectives

The trust's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV, and the associated images and any sound recordings is covered by GDPR under which the trust has a legitimate interest to use CCTV. This policy outlines the trust's use of CCTV and how it complies with the Act.

The aims of the policy are:

2.1 To describe the balance between the legitimate interest of the trust and the right to privacy that must be struck.

2.2 To ensure that the trust recognises that data subjects have a right to privacy in appropriate situations.

3. Responsibilities

The trust Chief Operating Officer is responsible for monitoring and updating the policy.

3.1 The trust Head of IT Services is responsible for ensuring that that CCTV systems are compliant with this policy.

3.2 Principals/Headteachers and trust central support managers are responsible for ensuring that their staff use CCTV systems in compliance with this policy.

3.3 All authorised operators and members of staff with access to images must be aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the in their responsibilities under the CCTV Code of Practice. All members of staff are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

This policy will be kept under review in order to take account of changes to law and/or practice and changes to the trust's circumstances.

4. Statement of Intent

The trust complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

4.1 CCTV warning signs will be clearly and prominently placed at all external entrances to schools where CCTV is in operation, including school gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV (see appendix A). In areas where CCTV is used, the school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

4.2 The planning and design has endeavoured to ensure that the scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

5. Existence of CCTV systems

5.1 Where the trust is considering introducing a CCTV system, it will determine if its use is a proportionate response to the identified problem by means of a Data Protection Impact Assessment. It should objectively assess:

- the nature of the problem it is seeking to address;
- whether a CCTV system is justified and is likely to be an effective solution,
- whether a better solution exists,
- what effect its use may have on individuals.

The ICO provides a Code of Practice which should be considered at this stage: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

5.2 In the case of existing CCTV systems, the trust should regularly evaluate whether it is necessary and proportionate to continue using it by reviewing the previous Data Protection Impact Assessment.

6. Siting of Cameras

6.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated.

6.2 Each school will make every effort to position cameras so that their coverage is restricted to its premises, which may include outdoor areas.

6.3 Schools should generally avoid having CCTV cameras situated in learning spaces without good cause (for example for teachers' professional development or to monitor an on-going vandalism issue). Areas which have communal usage such as halls and external sports areas are exempt from this recommendation.

6.4 Cameras will not be sited in changing areas, toilet cubicles, interview rooms and other areas which are reasonably expected to be private.

6.5 Each school will maintain an inventory of where its cameras are situated, with the exception of cameras placed for the purpose of covert monitoring. This inventory will be made available to all data subjects upon request.

7. Covert Monitoring

7.1 The trust may in exceptional circumstances set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct

- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

7.2 In these circumstances authorisation must be obtained from the school's Headteacher or Principal, or the trust's Chief Executive Officer.

7.3 Covert monitoring must cease following completion of the investigation.

7.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, as defined in 6.4, except in extreme circumstances such as to investigate a potential serious crime with the agreement of appropriate law enforcement agencies. Any such deployment must have the authorisation of the trust Chief Executive, or if the monitoring involves the trust Chief Executive, the authorisation of the Trust Board Chair.

8. Storage and Retention of CCTV images

8.1 Recorded data will not be retained for more than 6 months or to support an ongoing investigation (whichever is greater). While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

8.2 All recorded data will be stored securely.

8.3 When recorded data is exported from the CCTV system as part of an ongoing investigation, a named authorised user will be responsible for that data and for deleting it when the investigation is concluded.

9. Access to CCTV images

9.1 Access to live and recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

9.2 The list of authorised staff will be maintained by the school's Headteacher or Principal. It is recommended the list is restricted to the school's or trust's senior management.

9.3 CCTV images should only be viewed in a restricted area, such as a designated secure office within the site. Trust CCTV systems do not transmit images beyond the local site.

9.4 The CCTV system should be configured to log automatically all access of live images where the system supports this.

9.5 A CCTV access log will be maintained, to include:

- the purpose of any searches and whether the search was successful or not,
- who carried out search,
- who requested the search (if different),
- persons present (particularly when reviewing),
- date, start and end time of the incident,
- date and time of the review,
- any other relevant information.

9.6 Some trust sites with CCTV cameras contain more than one trust school. On such sites, there may be situations when CCTV images include pupils from a second school on the same site. In such cases, the authorised staff from the second school should request access to the CCTV images from the Headteacher or Principal of the first school. If these requests are regularly occurring, the two schools may opt to move from case by case basis to a permanent arrangement.

9.7 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

9.8 Trust CCTV systems make no use of automated processing for facial recognition.

10. Access to and Disclosure of Images to Third Parties

10.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the police and service providers to the school where these would reasonably need access to the data.

10.2 Requests should be made in writing to the school's Headteacher or Principal, or the trust's Chief Executive Officer.

10.3 The data may be used within the trust's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

11. System Management

11.1 The CCTV systems will be the responsibility of the Head of IT Services and managed by the IT Services Team on a day-to-day basis.

11.2 The IT Services Team will necessarily have access to the CCTV system in order to operate and support the CCTV system.

11.3 The CCTV system will be operated 24 hours each day, every day of the year other than during maintenance periods.

11.4 The IT Services Team should regularly check that the system is properly recording and that cameras are functional. The regularity of the checks should depend on the recent reliability of the system and whether normal usage of the system has implicitly demonstrated that the system is functioning (e.g. requests to access recorded material).

11.5 If the IT Services Team is asked to download records images from the CCTV system by a member of staff, they must satisfy themselves of the legitimacy of the request:

- the identity of the person requesting this action
- that they are an authorised user
- that the request itself is reasonable.

Where any doubt exists access should be referred to the Headteacher or Principal for confirmation.

12. Other Recording Devices

12.1 Other video transmission devices may be used within schools such as webcams, tablet or phone cameras, video conferencing facilities and telepresence robots. Such systems have the same ability to record footage as a CCTV system but also, in some cases, allow the footage to be transmitted in real time beyond the physical boundaries of the site.

12.2 All such systems are subject to the siting requirements as described in section 6.

12.3 Where such systems are used to transmit footage in real time beyond the site, it is essential to ensure that such footage can only be accessed by approved viewers.

13. Complaints

13.1 Complaints and enquiries about the operation of CCTV within a school should be directed to the Headteacher or Principal in the first instance. For corresponding complaints within other trust buildings, these should be directed to the trust Chief Operating Officer. If this doesn't satisfy the enquirer, they should contact the trust Chief Executive.

14. Further Information

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- www.ico.gov.uk
- Regulation of Investigatory Powers Act (RIPA) 2000
- GDPR 2018

Appendix A – CCTV Signage

It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV protected rea that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded.
- The purpose of using CCTV.
- The name of the school.
- The contact telephone number or address for enquiries.