Isle of Wight Education Federation

The Governing Board of the Isle of Wight Education Federation

CCTV Policy

Author	Mark Overy Josh Collins
Approved by	Full Governing Board
Approval date	January 2023
Review frequency	Bi-Annually
Next review	January 2025

Revision History

Revision	Change	Date
2.0	Initial CCTV Policy version 2.0	03/01/2023

1. Introduction

The purpose of this policy is to regulate the management, operation, and use of the closed-circuit television (CCTV) system at the Isle of Wight Education Federation (IWEF). The system comprises almost 200 cameras located across the three Federation sites. All cameras are centrally monitored and the footage is available to senior staff, Head of Years and the ICT Support team.

This policy follows the Data Protection Act and GDPR guidelines. The policy will be subject to review to include consultation as appropriate with interested parties. The CCTV system is owned by the Federation.

2. Objectives of the CCTV scheme

- To increase personal safety of staff, children and visitors and reduce the fear of crime
- To protect the Federation buildings and their assets
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property

3. Statement of Intent

The CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements and implementation of the General Data Protection Regulation (GDPR) and the Commissioner's Code of Practice. The Federation will treat the system, and all information, documents and recordings obtained and used, as data which are protected by the Act. Cameras will be used to monitor activities within the Federation grounds to identify adverse activity occurring, anticipated or perceived, and for the purpose of securing the safety and well-being of the Federation's children and staff, together with its visitors.

Staff have been advised that static cameras do not focus on private homes, gardens and other areas of private property. The cameras are only located at strategic points throughout the Federation premises, principally at the entrance and exit points and the play areas around the Federation. No camera focuses, or will focus, on toilets, shower facilities, changing rooms, staff rooms or private offices. There are signs that clearly communicate that the site is covered by CCTV.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Recordings will never be released to the media for purposes of entertainment. 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. Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the Federation CCTV.

4. Operation of the system

The CCTV system will be administered and managed by the Federation in accordance with the values and objectives expressed in the policy. The day-to-day management will be delegated by the Executive Headteacher to the ICT Support Team. Viewing of recorded images must take place in the ICT Office at an appropriate time, arranged via the Federation's Helpdesk via the ticketing system. The CCTV system will be operational 24 hours each day, every day of the year, recording all activity. All operators and others with access to images must be aware of the access procedures that are in place. The CCTV system records images only and there is no audio recording. Therefore, conversations are not recorded by the CCTV system.

5. Control and Liaison

The ICT Support Team will check and confirm the efficiency of the system regularly, in particular that the equipment is properly recording and that cameras are functional. This includes the digital video recorder (DVR) units across the sites and their storage capacity, firmware versions and physical condition.

6. Monitoring procedures

Camera surveillance may be maintained at all times and footage continuously recorded and held on system memory for a retention period of 14 days. Beyond the retention period the footage is automatically overwritten by the DVR unit.

7. Recording and retention of images

Images produced by the CCTV equipment are as clear as possible so that they are effective for the purposes for which they are intended. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high quality images. Images may be recorded either in constant real-time (24 hours a day throughout the year), or only at certain times, as the needs of the business dictate.

As the recording system records digital images, any CCTV images that are held on the hard drives of the video recorder units are deleted and overwritten on a recycling basis and are not held for more than 30 days. Once a hard drive has reached the end of its use, it will be erased and then destroyed to ISO 27001 standards . Images that are stored on, or transferred on to, removable media such as CDs are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of one week. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

8. Access to and disclosure of images

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

The images that are filmed are recorded centrally on a DVR at each site and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those line managers who are authorised to view them in accordance with the purposes of the system. Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented.

Disclosure of images to other third parties can only be made in accordance with the purposes for which the system is used and will be limited to:

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness
- Prosecution agencies, such as the Crown Prosecution Service
- Relevant legal representatives
- Line managers involved with Federation disciplinary processes
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).
- The Executive Headteacher (or another authorised person acting in their absence) is the only person who is permitted to authorise disclosure of information to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented on the Federation Helpdesk ticketing system, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

Requests by the Police can only be authorised under section 29 of the Data Protection Act 1998. Should a USB export of footage be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.4 of this policy. USBs will only be released to the Police on the clear understanding that the USB remains the property of the Federation, and both the USB and information contained on it are to be treated in accordance with this policy. The Federation also retains the right to refuse permission for the Police to pass to any other person the USB or any part of the information contained thereon. On occasions when a Court requires the release of an original USB this will be produced from the safe, complete in its sealed bag. The Police may require the Federation to retain the stored USBs for possible use as evidence in the future. Such USBs will be properly indexed and properly and securely stored in a safe until they are needed by the Police.

Applications received from outside bodies (e.g. solicitors) to view or release footage will be referred to the Headteacher. In these circumstances footage will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. This must be provided within 30 calendar days of receiving the required fee and the request. If the decision is taken not to release the images, then the image in question should be held and not destroyed until all legal avenues have been exhausted.

9. Individuals' access rights

Under the GDPR individuals have the right on request to receive a copy of the personal data that the Federation holds about them, including CCTV images if they are recognisable from the image.

If you wish to access any of your CCTV images, you must make a written request to the Headteacher. Your request must include the date and time when the images were recorded and the location of the particular CCTV camera, so that the images can be located and your identity can be established as the person in the images. The Federation will always check the identity of the person making the request before processing it. The footage itself is only available for up to 30 days, therefore footage requests outside of this timeframe from the specified date is not possible.

The Headteacher will first determine whether disclosure of your images will reveal third party information as you have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

If the Federation is unable to comply with your request because access could prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders, you will be advised accordingly.

10. Training

IWEF will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the GDPR with regard to that system.

11. Breaches of the policy (including breaches of security)

Any breach of the CCTV policy by Federation staff will be initially investigated by the Headteacher, in order for the Headteacher to take the appropriate disciplinary action. Complaints will be dealt with in accordance with the Federation Complaints Policy.

12. Assessment of the policy

Performance monitoring, including random operating checks, may be carried out by the Operations Manager (Systems) with direction from the Director of Facilities and ICT..

13. Complaints

Any complaints about the Federation's CCTV system should be addressed to the Headteacher. Complaints will be dealt with in accordance with the Federation complaints policy.

14. Public information

Copies of this policy will be available to the public on request and can be found on the Federation website:

https://www.iwef.org.uk/iwef/policies/

15. Summary of Key Points

- This policy will be reviewed every three years.
- The CCTV system is owned and operated by the Federation.
- Liaison meetings may be held with the Police and other bodies.
- Recording USBs used will be properly indexed, stored and destroyed after appropriate use.
- Footage may only be viewed by authorised Federation staff and the Police.
- Exported footage required as evidence will be properly recorded, witnessed and packaged before copies are released to the police.
- Footage will not be made available to the media for commercial or entertainment.
- Exported footage will be disposed of securely to ISO 27001 standards.
- Any breaches of this policy will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches.
- Breaches of this policy and remedies will be reported to the Headteacher.