FERNDOWN UPPER SCHOOL

CCTV
CODE OF PRACTICE

Policy first adopted: Jun 2006

To be reviewed 3-yearly

Reviewed: January 2010

Reviewed: April 2012

Reviewed: Jan 2013

Reviewed: Feb 2016

Reviewed: May 2019

Reviewed: June 2022

Reviewed: January 2023

Reviewed: September 2023

1. Aims

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe and safeguarded – this includes use of CCTV at break and lunch to safeguard students.
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Determine the cause of behaviour incidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defense of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including inside toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

The use of the CCTV is registered under Dorset County Council's Data Protection Notification (Registration No Z5874509) for the purposes of the prevention and detection of crime

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2. Relevant legislation and guidance

This policy is based on:

2.1 Legislation

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

2.2 Guidance

- Surveillance Camera Code of Practice (2021)

3. Definitions

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

4. Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Signs have been placed in the following areas to ensure the public is aware that they are entering a zone covered by CCTV; please see site plan.

5. Roles and responsibilities

5.1 The governing board

The governing board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with. This responsibility is delegated to the Headteacher.

5.2 The Headteacher

The Headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Decide which members of staff will have acess to the system
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

5.3 The data protection officer

- Monitor compliance with UK data protection law
- The data protection officer (DPO) will review the policy as a quality assurance process.
- Act as a point of contact for communications from the Information Commissioner's Office
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- Carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period
- Receive and consider requests for third-party access to CCTV footage

5.4 The behaviour Deputy Head will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Keep accurate records of all data processing activities and make the records public on request
- Ensure that the CCTV system is not infringing on any individual’s reasonable right to privacy in public spaces
- As a viewer follows the same practice as all staff re access permissions.

5.4 The system manager

The system manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly
- Ensure footage is destroyed when it falls out of the retention period
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified

6. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year.
The system is registered with the Information Commissioner's Office (Registration No Z5874509).
The CCTV records visual images only with the exception of the camera in Reception which records sound for the safety and protection of staff, students and the general public.
Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

7. Storage of CCTV footage

Footage will be retained for 21 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

8. Access to CCTV footage

The Headteacher's authorisation must be gained for any viewing of the CCTV system with the following exceptions:

- Use by staff looking for a missing student.
- Use by duty staff at break and lunch time.
- Authorisation of a behaviour incident involving students where authorisation may be granted by the behaviour Deputy Headteacher.

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time – this is recorded online through the system on each occasion.

CCTV footage will be accessed by two members of staff together.

When viewing students, one of the members of staff should be level two safeguarding trained and ideally will be level three trained.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

FUS will use CCTV to support safeguarding of students – it will be accessed when looking for a student. It is used at break and lunch time to ensure student safety.

9.1 Staff access

The following members of staff have authorisation to access the CCTV footage:

- The head teacher
- The behaviour deputy head teacher
- The system manager for technical reasons
- Anyone with express permission of the head teacher or the deputy headteacher for student behaviour incidents
- Duty staff at break and lunch time or on call staff if a student is missing

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

Any member of staff who misuses the surveillance system may be committing a criminal offence, and will face disciplinary action.

9.2 Subject access requests (SAR)

According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the request the school will immediately issue a receipt and will then respond within 30 days during term time. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

All staff have received training to recognise SARs. When a SAR is received staff should inform the DPO in writing. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

9.3 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the head teacher and the DPO.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the DPO.

10. Security

- The system manager will be responsible for overseeing the security of the CCTV system and footage
- The system will be checked for faults once a term
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible
- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use
- Proper cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

11. Staff Monitoring

FUS may wish to monitor its workplace for various reasons, the Data Protection Act does not prevent FUS from monitoring workers, but FUS remembers that workers are entitled to privacy at work.

- Monitoring should not be excessive.

.

CCTV monitoring

Ferndown Upper School uses CCTV to ensure the safety and well-being of all of its staff and students.

CCTV microphones are only ever used in main Reception, which are constantly recording to ensure the safety of staff and students.

Covert monitoring

FUS will not use monitoring from covert cameras but on rare occasions it will use the established CCTV cameras to covertly surveil, either live or via viewing the recordings. This will only occur if FUS suspects that the employee is involved either in an illegal activity or to ensure the safeguarding of its staff or students.

12. Complaints

Complaints should be directed to the headteacher or the DPO and should be made according to the school's complaints policy.

13. Monitoring

The policy will be reviewed annually by the DPO and behaviour Deputy Head to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

14. Links to other policies

- Data protection policy
- Biometric data policy
- Privacy notices for parents, pupils, staff, governors and suppliers
- Safeguarding policy