The Federation of

Alver Valley

CCTV Policy

Date written	**June 2024**
FGB	**No approval needed shared June 2024**
Review Date	**June 2027**
Author	**SM – Luke Spence**

Introduction

The Federation of Alver Valley Schools uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property.

- The system comprises a number of fixed and dome cameras.
- The system **does not** have sound recording capability.
- The CCTV system is owned and operated by the school, the deployment of which is determined by the school's leadership team.
- The CCTV is monitored centrally from the school offices by the site manager and the data protection controller.
- The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the school community.
- The school'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 the Data Protection Act 1998. This policy outlines the school's use of CCTV and how it complies with the Act.
- All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

Statement of Intent

The school 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 Template (ico.org.uk)

CCTV warning signs will be clearly and prominently placed at all external entrances to the school, including school gates if coverage includes outdoor areas. 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.

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.

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- 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
- 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 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.

Siting the Cameras

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. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

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

CCTV will not be used in classrooms but in areas within school that have been identified by staff and pupils as not being easily monitored.

Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

Covert Monitoring

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

i) 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;

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

In these circumstances, authorisation must be obtained from a member of the senior leadership team.

Covert monitoring must cease following completion of an investigation.

Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles.

Storage and Retention of CCTV images

Footage will be retained for 30 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.

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

Staff access

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

- The Executive Head Teacher: Jill Roseblade
- The Head of School: Ali Lockwood
- The data protection officer: Mel Chandler
- The system manager: Luke Spence
- Anyone with express permission of the Executive head teacher: James Pritchett

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

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

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

Subject Access Requests (SAR)

According to UK GDPR and Data Protection Act 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.

Access to and Disclosure of Images to Third Parties

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

Complaints

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

Legislation

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights - The European Convention on Human Rights (coe.int)
- 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 - Search (bing.com)
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004

The Equality Act 2010

Guidance

- Surveillance Camera Code of Practice (2021)

Appendix 1 - Checklist for users of limited CCTV systems

This CCTV system and the images produced by it are controlled by the data protection controller who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998)1.

	Checked (Date) By	Date of next review
We have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of pupils, staff and visitors. It will not be used for other purposes. We conduct an annual review of our use of CCTV.	July 2024	July 2027
Notification has been submitted to the Information Commissioner and the next renewal date recorded.		
There is a named individual who is responsible for the operation of the system.	July 2024	July 2027
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.	July 2024	July 2027
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	July 2024	July 2027
Cameras have been sited so that they provide clear images.	July 2024	July 2027
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	July 2024	July 2027
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	July 2024	July 2027
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	July 2024	July 2027
The recorded images will only be retained long enough for any incident to come to light (eg for a theft to be noticed) and the incident to be investigated.	July 2024	July 2027
Except for law enforcement bodies, images will not be provided to third parties.	July 2024	July 2027
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.	July 2024	July 2027
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.	July 2024	July 2027
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	July 2024	July 2027