Revised 2023

Brecknock and Torriano Schools Federation

GDPR CCTV Policy 2023-24

Committee	Resources
Last reviewed	Summer 2023
To be reviewed	Summer 2024
Changes from 21-22 to 22-23	Both policies were previously the same, however, there is now a template policy available and both policies have been merged into one new policy. Where relevant, the document now includes 'The Brecknock and Torriano Federation'. Reference to the school/schools remains as referring to separate camera systems.

Brecknock Primary School, Cliff Villas, London, NW1 9AL
Ph. 020 7485 6334 Email. admin@brecknock.camden.sch.uk

Torriano Primary School. Torriano Avenue, London, NW5 2SJ
Ph. 020 7424 0202 Email. admin@torriano.camden.sch.uk

Contents

1. Aims

This policy aims to set out the Federation'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
- Protect members of the school community from harm to themselves or to property
- Deter criminality in the school
- Protect school assets and buildings
- Determine the cause of accidents
- Assist in the effective resolution of any disputed which may arise in the course of disciplinary and grievance proceedings
- To assist in the defence of any litigation procedures

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.

The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

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). Cameras are located on the outside of the school buildings and in the foyer entrance of the building.

Appropriate signage is in place to warn members of the school community that they are under surveillance.

Cameras are not and will not be aimed off school grounds into public spaces or people's private property. Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

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.

5.2 The Executive Headteacher

The Executive Headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV 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 Federation is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection

- 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

The data protection officer (DPO) will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Train all staff to recognise a subject access request
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Monitor compliance with UK data protection law
- Advise on and assist the Federation with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office
- Conduct data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the Federation, what their rights are, and how the Federation will endeavour to protect their personal information
- 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
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- 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 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 annually, or sooner if required (appendix 1)
- Ensure the data and time stamps are accurate annually, or sooner if required

6. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year. The system will not record audio.

Recordings will have date and time stamps.

7. Storage of CCTV footage

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.

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.

The DPO will carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period.

8. Access to CCTV footage

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

8.1 Staff access

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

- The Executive Headteacher
- The Head of School
- The Director of Business Operations
- Anyone with express permission of the Executive Headteacher

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.

8.2 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 Executive Headteacher and the DPO.

The Federation will comply with any court orders that grant access to the CCTV footage. The Federation 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.

9. Data protection impact assessment (DPIA)

The Federation follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

A new DPIA will be done whenever cameras are moved or new cameras are installed.

If any security risks are identified in the course of the DPIA, the Federation will address them as soon as possible.

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 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. Complaints

Complaints should be directed to the Executive Headteacher or the DPO and should be made according to the Federation's complaints policy.

12. Monitoring

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

Appendix One: CCTV Checklist

Item	Checked (Date)	By
There is a named individual who is responsible for the operation of the system.	25.05.2023	Lisa Hallinan Director of Business Operations
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.	25.05.2023	Lisa Hallinan Director of Business Operations
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.	25.05.2023	Lisa Hallinan Director of Business Operations
Cameras have been sited so that they provide clear images.	25.05.2023	Lisa Hallinan Director of Business Operations
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	25.05.2023	Lisa Hallinan Director of Business Operations
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).	25.05.2023	Lisa Hallinan Director of Business Operations
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	25.05.2023	Lisa Hallinan Director of Business Operations
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	25.05.2023	Lisa Hallinan Director of Business Operations
Except for law enforcement bodies, images will not be provided to third parties.	25.05.2023	Lisa Hallinan Director of Business Operations
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.	25.05.2023	Lisa Hallinan Director of Business Operations
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.	25.05.2023	Lisa Hallinan Director of Business Operations
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	25.05.2023	Lisa Hallinan Director of Business Operations