



CCTV Policy

2024-2027

Statutory Policy			Website	
Yes – as part of Data Protection Policy			Yes	
Date Written:	Written by:	Ratified by:	Ratified on:	Review:
January 2024	Adrienne Hatfield, Data Tools for Schools & Kirklees	Full Governors	January 2024	January 2027



1. Aims

This policy has been partially adopted from Kirklees School CCTV Policy and written with support from the school's Data Protection Officer, Data Tools for Schools. This policy should be read alongside the statutory Fixby J&I School Data Protection Policy, Records' Management Policy. This policy follows the guidance contained in the UK Government's Surveillance Camera Code of Practice, updated in November 2021, pursuant to The Protection of Freedoms Act 2012

- 1.1 Fixby J&I School 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 CCTV is not for surveillance use.
- 1.2 The system comprises of 16 dome cameras.
- 1.3 The system has sound recording capability.
- 1.4 The CCTV system is owned and operated by the school with support from Harford's Security Ltd, First Class ICT Support Ltd and the deployment of which is determined by the school's Senior Leadership Team
- 1.5 The CCTV is monitored centrally from within Fixby J&I School Office.
- 1.6 The school is a registered data controller with the Information Commissioner's Office under the terms of the UK GDPR and the Data Protection Act 2018. The use of CCTV, and the associated images and any sound recordings, is covered under the UK GDPR and the Data Protection Act 2018. This policy outlines the school's use of CCTV and how it complies with the Act.
- 1.7 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. Breaches of the code of practice by staff may lead to disciplinary action and possible criminal proceedings.

2. Statement of Intent

- 2.1 The school complies with the 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. Further information can be obtained directly from the ICO's website <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/>
- 2.2 CCTV warning signs are clearly and prominently placed, including at all external entrances to the school, including school gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV (see appendix B). 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.
- 2.3 CCTV is included in the school's privacy notice on the school website to be transparent to parents and students about the collection of CCTV images.

- 2.4 The planning and design ensure that the CCTV 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.

3. Siting the Cameras

- 3.1 Cameras are 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 UK GDPR and the Data Protection Act 2018. These are located in the following areas:
- Entry/Exit gates and doors.
 - External communal areas including playground and car park.
 - Internal communal areas including foyer and corridors.
- 3.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.
- 3.3 CCTV will **not** be used in toilets, staffroom or classrooms.
- 3.4 Members of staff should have access to details of where CCTV cameras are situated.

4. Covert Monitoring

- 4.1 The school does not undertake or permit covert monitoring.

5. Storage and Retention of CCTV images

- 5.1 Recorded data will not be retained for longer than is necessary, and will usually be deleted after four weeks, unless it is recognised that it is needed for the purpose of an investigation, in which case it is retained until completion of that investigation. 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.
- 5.2 All retained data will be stored securely. When the retention period has passed, the data will be removed or erased and documented.

6. Access to CCTV images

- 6.1 Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available, unless authorised and documented by the Headteacher, stating the reason for the authorisation (to be recorded as per form attached at Appendix D). In Fixby J&I School only the following staff have authorisation to access CCTV images with good reason to do so: these staff have received appropriate training and been issued with the school's CCTV policy:

Name	Role	Date
Claire Allen	Headteacher	January 2024
Saima Ahmed	Deputy Headteacher	January 2024
Adrienne Hatfield	School Business Manager	January 2024
First Class ICT Support Ltd	IT Support Provider	January 2024
Harford's Security Ltd	Security System Provider	January 2024

7. Subject Access Requests (SAR)

- 7.1 Individuals have the right to request access to CCTV footage relating to themselves under the UK GDPR and the Data Protection Act 2018.
- 7.2 All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location. All requests and action to be recorded on form attached at Appendix D.
- 7.3 The school will respond to requests within 1 calendar month of receiving the request and any relevant fee.
- 7.4 All requests will be documented, including whom the request was from, the response received and date of response.
- 7.5 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

8. Access to and Disclosure of Images to Third Parties

- 8.1 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 (e.g. investigators).
- 8.2 Requests should be made in writing to the Headteacher.
- 8.3 The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.
- 8.4 The data may also be used and shown to students and/or parents as appropriate, in relation to student disciplinary and/or suspension processes and parental complaints.

9. Complaints

- 9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance in writing to:

Claire Allen
Headteacher
Fixby J&I School
Lightridge Road
Fixby
Huddersfield
HD2 2HB

office@fixby.org

Further Information

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

- Surveillance Camera Code of Practice
- www.ico.gov.uk
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 2018

Appendix A - Checklist

This CCTV system and the images produced by it are controlled by Claire Allen, Headteacher, 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 under the UK GDPR and the Data Protection Act 2018).

Fixby J&I School has 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 stakeholders. The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures. We conduct a three-year annual review of our use of CCTV.

	Checked (Date)	By	Date of next review
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.			
Staff named as CCTV authorised users have received appropriate training and received a copy of the school's CCTV Policy			
A system had 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.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
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).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
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.			
Images will only be shared with those who fit the criteria outlined in the text.			
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.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix B – CCTV Signage

It is a requirement under the UK General Data Protection Regulation 2018 and the Data Protection Act 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that images are recorded. The school ensures that this requirement is fulfilled by displaying the minimum required information as outlined on the example sign below.



Appendix C – UK General Data Protection Regulation 2018 & Data Protection Act 2018 Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is not a full explanation of the principles, for further information refer to the

UK GDPR and the Data Protection Act 2018

Appendix D – Requests

Subject Access & Third-Party Request Disclosure Log

Date request received and from whom (name & organisation)	Date referred to DPO	Subject Access Request or Third Party Request	State the reason (if third party)	Date & nature of disclosure (viewing or copy of image)	Images viewed/sent (state location, date,time of original image/s and internal image reference)	The outcome if applicable