CCTV Code of Practice

Effective Date:	**26/11/2019**
Date Reviewed:	**26/11/2021**
Contact Officer:	**Sue Marshall**

1. Definitions for the Purposes of this Code

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

System Manager – the person with day to day responsibility for making decisions about how the cameras are used and the processing of images captured, including maintaining the relevant code of practice.

Overt surveillance - means any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act (RIPA) 2000.

2. Identified Key Risk Factors

Brough Primary School as data controller have identified the following risk factors.

Fraud / Theft / Wilful Damage / Breaches of Security / Use of Violence / Instances of Crime.

3. Purpose of the System

- Prevent, investigate and detect crime
- Help reduce the fear of crime
- Assist with the apprehension and prosecution of offenders
- Enhance the safety of employees and the public
- To safeguard vulnerable adults and children
- Provide evidential material for court or committee proceedings
- Reduce incidents of public disorder and anti-social behaviour

- Evidence in investigations of gross misconduct (including protecting employees from allegations)
- Protect property
- Process Subject Access Requests

4. Camera Locations and Associated Coverage Linked to Perceived Risk Factors.

Ref	Location	Line of Site	Fixing	Risk indicator
1	Lower school main entrance	Main door	Static	Theft / Damage / Violence / Breaches of Security
2	Upper school water tower	Exit doors	Static	Theft / Damage / Violence / Breaches of Security
3	Upper school camera pole	Car park	Static	Theft / Damage / Violence / Breaches of Security
4	Upper school	Dining hall doors	Static	Theft / Damage / Violence / Breaches of Security
5	Link Building	Slate area	Static	Theft / Damage / Violence / Breaches of Security
6	Camera pole	Main gate and driveway	Static	Theft / Damage / Violence / Breaches of Security
7	Upper school KS 2 playground	KS 2 playground gate	Static	Theft / Damage / Violence / Breaches of Security
8	Reception/office	Main entrance door	Static	Theft / Damage / Violence / Breaches of Security
9	Currently out of order		Static	Theft / Damage / Violence / Breaches of Security
10	Reception/library area	Entrance door	Static	Theft / Damage / Violence / Breaches of Security
11	Lower school	KS1 playground	Static	Theft / Damage / Violence / Breaches of Security
12	Gym external	Children's Centre	Static	Theft / Damage / Violence / Breaches of Security

13	Gym external	Children's Centre	Static	Theft / Damage / Violence / Breaches of Security
14	Upper school back view	Path leading down the side of the school alongside KS 2 field	Static	Theft / Damage / Violence / Breaches of Security
15	Camera pole	Main drive gate	Static	Theft / Damage / Violence / Breaches of Security
16	Upper school back view	Path at the back of the school	Static	Theft / Damage / Violence / Breaches of Security

5. Control of Access to System and Images

Cameras are monitored through a terminal which is located in a locked cupboard the upstairs resource room along with the recording equipment.

Screens should be switched off at all times unless the camera is to be used for the purpose for which it was designed; this will avoid 'unintentional' viewing of unrelated imagery.

The Headteacher shall be the system manager and will hold the administrators password and the right to allocate passwords to users of the system if necessary.

The named persons with associated levels of access rights to surveillance system are:

Ref	Officer Name	Access Level
1	Headteacher	Full
2	Deputy Headteacher	Full
3	Site Manager	Full
4		
5		

All authorised users of the system must be trained in the use of the system and must have read the Code of Practice and procedures in relation to its use. Once training is complete, each authorised user will sign a training register to verify that they understand how to use the system. The training register is kept in the CCTV cupboard.

6. Camera System Checks and Maintenance

A weekly assessment of the system will be carried out by the site manager to ensure that all cameras are receiving an image (basic functionality) and that the time and date shown on the images are correct. All instances of camera malfunction must be reported as soon as possible, to Exell for repair.

Image capture quality must also be tested on a weekly basis. 10% of the functioning cameras are to be selected (on a rotational basis) and the images produced tested for clarity (in case of the need for production of images for use, in cases of criminal prosecution).

Records of the tests are to be recorded in the system log book located in the locked CCTV cupboard.

7. Retention of Recorded Images

Images recorded onto the hard drive of the CCTV systems shall be retained for a period of no more than 30 days (unless images are being used for an ongoing investigation).

At the end of the 30 day period, images are overwritten automatically (by earliest date of recording first) or can be saved by an authorised named person if an investigation is ongoing.

This action must be recorded in the system log book, detailing date period, by whom and why the images are being retained.

Any images that may have been saved must be deleted after a period of 6 calendar months of retention, unless a specific request has been received stating otherwise.

8. Reference Tables in Use

Not in use

9. Disclosure of Images

Any request by an outside organisation or individual (SAR), for access to recorded or real time CCTV images must be passed to the schools Data Protection Officer for logging and authorisation.

Should the request be a 'simple', unobtrusive request, this may be dealt with on site by Headteacher (authorised person).

Imagery must be reviewed by the authorised named person, taking into account any possible third party inclusion in images. Every effort should be made to protect third party privacy.

Should the authorised named person feel that any third party would not have their basic right to privacy infringed, they may offer the individual/organisation requesting sight of the imagery, the opportunity to 'view' the recorded data.

Should the individual then go on to request a copy of the imagery, this must be referred to the school's Data Protection Officer for authorisation. The appropriate request form must be completed and a record made within the system log book.

Should the school receive a request for CCTV footage from the Police the following Police requests do not require prior authorisation. However the member of staff dealing with the request must be confident that there is a need to share the information and a log must be kept:

- Police requests relating to an immediate danger to the public/staff.
- Requests which relate to crimes the school has reported to the Police.

Once completed, details must be logged as with any other request.

If the request cannot be dealt with immediately, copied images must be held securely on the hard drive as outlined in section 6.

10. Signage

Signage shall be displayed at all entrances to the school and appropriate areas of the external building.

11. References

Human Rights Act 1998
Data Protection Act 2018
General Data Protection Regulation
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Protection of Freedoms Act 2012
Surveillance Camera Code
ICO CCTV Code of Practice - https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf