Burlington Junior School

Shaping Positive Futures

Achieving Our Full Potential

Date adopted	05/12/2019
Date approved by chair of Committee	05/12/2019
Review date	05/12/2020

CCTV and Code of Practice Policy December 2019

Contact details
Email:- burlington.juniors@eastriding.gov.uk
Telephone:- 01262 674487

1. Background

Surveillance cameras are used by Burlington Junior School in a number of areas and are a valuable tool to assist in areas such as public and employee safety, enhancing security and in protecting property.

The camera installations are owned by Burlington Junior School and are operated in line with data protection legislation, the Human Rights Act 1998 and guidelines, such as those issued by the Information Commissioner's Office (ICO) and the Surveillance Camera Commissioner, to ensure, for example, that the need for public protection is balanced with respect for the privacy of individuals.

2. Definitions for the Purposes of this Code

For the purposes of this policy, the following definitions apply in relation to Data Protection.

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.

Covert surveillance - is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place.

Surveillance camera systems - is taken to include: (a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c).

3. Policy Statement

This policy applies to all overt surveillance cameras controlled by Burlington Junior School as a data controller.

Surveillance cameras are a valuable resource, which help the school in areas such as protecting the public and its employees, enhancing security, crime prevention and protecting property. Burlington Junior School recognises that whilst there is a high level of public support for surveillance camera schemes, there are also increasing concerns about the role of cameras and their impact upon the privacy of members of the public, employees, parents and students.

To help address these concerns Burlington Junior School is committed to ensuring compliance with data protection legislation, the Human Rights Act 1998 and all relevant guidelines issued by the ICO and Surveillance Camera Commissioner. Burlington Junior School regards the lawful use and correct installation of surveillance cameras as essential to its successful operations and to maintaining confidence between the School and those with whom it carries out business. The School fully endorses the twelve guiding principles set out in the Surveillance Camera Code of Practice (see section 7) and is committed to privacy by design and default.

4. Identified Key Risk Factors

Burlington Junior School as data controller have identified the following risk factors.

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

5. 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

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

Ref	Location	Line of Site	Fixing	Risk indicator
1	Back door	Entrance to school	Static camera	Theft / Damage / Violence / Breaches of Security/Safeguarding
2	Rear playground	Playground and canteen	Static camera	Theft / Damage / Violence / Breaches of Security/Safeguarding
3	Climbing Wall	Walk way between front and rear of school	Static camera	Theft / Damage / Violence / Breaches of Security/Safeguarding
4	Car park	Main staff car park	Static camera	Theft / Damage / Violence / Breaches of Security/Safeguarding
5	Gazebo	Towards School vehicle entrance/exit	Static camera	Theft / Damage / Violence / Breaches of Security/Safeguarding

7. Control of Access to System and Images

The viewing of live time imagery captured on overt cameras that duplicate what is in general public view is acceptable. However, caution and discretion is advised at all times. Where possible, display screens should be placed in locations away from public view.

Cameras are monitored through a terminal which is located in the staff room and the recording equipment is located in the staff room.

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 IT technician shall be the system manager and will hold the administrators password and the right to allocate passwords to users of the system.

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

Ref	Officer Name	Access Level
1	Headteacher	Full View
2	School Business Manager	Full View
3	ICT Technician	Full View
4	DPO	Full View
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 Business Manager's office.

8. Camera System Checks and Maintenance

A termly assessment of the system will be carried out by an IT technician 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 the systems maintenance providers for repair.

Image capture quality must also be tested on a termly basis. Four 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 School Business manager's office.

9. Retention of Recorded Images

Images recorded onto the hard drive of the CCTV systems shall be retained for a period of less 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 1 calendar month of retention, unless a specific request has been received stating otherwise.

10. Reference Tables in Use

Not in use

11. 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 the IT technician and DPO.

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 Confidential drive.

12. Signage

Appropriate signage shall be displayed on all external doors and walls.

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
ICO CCTV Code of Practice - https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf