CCTV Code of Practice

Effective Date:	**28/04/2021**
Date Reviewed:	**28/02/2024**
Contact Officer(s):	**Mr R Munby, Premises Manager** **Mr M Evans, Assistant Headteacher**

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

The Education Alliance 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
- 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

Building	Camera Number	Floor	Location	Line of Site	Fixing	Risk indicator
West	West 1	Ground	Boys toilets, towards rear	Boys WC cubicle doors & basins	Static	Damage & Behaviour
West	West 2	Ground	Boys toilets, towards front	Boys WC cubicle doors	Static	Damage & Behaviour
West	West 3	Ground	Girls toilets, towards rear LHS	Girls WC cubicle doors, basins & dryers	Static	Damage & Behaviour
West	West 4	Ground	Girls toilets, towards front	Girls WC dryers and corridor	Static	Damage & Behaviour
West	West 5	Ground	Girls toilets, towards rear RHS	Girls WC cubicles & basins	Static	Damage & Behaviour
West	West 6	Ground	West rear corridor, towards HoY office	Corridor	Static	Behaviour
West	West 7	Ground	West corridor, towards rear stairwell	Corridor and stairwell doors	Static	Behaviour
West	West 8	Ground	West corridor exit, outside WB2	External gated area	Static	Behaviour & Security
West	West 9	Ground	Outside, rear of WB2	Playground, towards AstroTurf fencing	Static	Behaviour & Security
West	West 10	Ground	Outside, WB2 towards DT Block	Across playground towards DT entrance	Static	Behaviour & Security
West	West 11	Ground	Outside, playground from WB3	Across playground towards SHC	Static	Behaviour & Security
West	West 12	Ground	Rear entrance, towards West Playground	Across playground towards AstroTurf	Static	Behaviour
West	West 13	Ground	Rear Corridor	IT corridor and outdoor area	Static	Behaviour
West	West 14	Ground	Entrance foyer	Front foyer and foot of stairwell	Static	Behaviour
West	West 15	Ground	Entrance Foyer	Entrance foyer	Static	Behaviour & Security
West	West 16	Ground	Front Entrance to Foyer	Front entrance and carpark area	Static	Behaviour & Security
West	West 17	Ground	Canteen	West canteen seating area	Static	Behaviour
West	West 18	Ground	West carpark	West carpark	Static	Behaviour & Security
West	West 19	Ground	Finance office entrance	Finance office entrance & entrance to the canteen	Static	Behaviour & Security
West	West 20	Ground	West Hall	West hall seating area and gym doors	Static	Behaviour
West	West 21	Ground	MFL corridor, towards Disabled WC	From hall entrance covering length of corridor to internal doors	Static	Behaviour
West	West 22	Ground	MFL corridor, towards external door	From internal corridor doors to external door (side exit)	Static	Behaviour

West	West 23	Ground	Gym corridor, towards external door	From internal corridor doors to external door (playground exit)	Static	Behaviour
West	West 24	Ground	Outside, MFL Entrance	Driveway towards MFL side entrance	Static	Behaviour & Security
West	West 25	Ground	Outside, West Picnic Area	Grassed seating area	Static	Behaviour & Security
West	West 26	Ground	Outside, west gym corner	Playground towards leisure centre gates	Static	Behaviour & Security
West	West 27	Ground	Outside, west playground 1	PE entrance LHS	Static	Behaviour & Security
West	West 28	Ground	Outside, west playground 2	PE entrance RHS	Static	Behaviour & Security
West	West 29	Ground	Outside, Main Entrance	Entrance barrier for vehicles	Static	Security
East	East 1	Ground	Mixed gender toilets, LHS	Basins & dryers	Static	Damage & Behaviour
East	East 2	Ground	Mixed gender toilets, rear	Cubicle doors	Static	Damage & Behaviour
East	East 3	Ground	Mixed gender toilets, RHS	Cubicle doors, basins & dryers	Static	Damage & Behaviour
East	East 4	Ground	Corridor	The Link entrance area and corridor towards history entrance	Static	Damage & Behaviour
North	North 1	Ground	Toilets, entrance corridor	Entrance area and girls basins & dryers	Static	Damage & Behaviour
North	North 2	Ground	Boys toilet, RHS	Cubicle doors & basins	Static	Damage & Behaviour
North	North 3	Ground	Boys toilet, LHS	Cubicle doors, basins & dryers	Static	Damage & Behaviour
North	North 4	Ground	Girls toilet, LHS	Cubicle doors, basins & dryers	Static	Damage & Behaviour
North	North 5	Ground	Girls toilet, RHS	Cubicle doors, basins & dryers	Static	Damage & Behaviour
North	North 6	Ground	Outside, NB1 towards playground	Playground and seating area	Static	Behaviour & Security
North	North 7	Ground	Outside, toilet and biology entrance/exit	External gated area	Static	Behaviour & Security
North	North 8	Ground	Outside, playground towards Performing Arts	Playground and side of performing arts	Static	Behaviour & Security
North	North 9	Ground	Outside, playground towards ICT	Covered seating area outside PA	Static	Behaviour & Security
North	North 10	Ground	Entrance foyer, towards canteen	Foyer, main doors and canteen entrance	Static	Behaviour
North	North 11	Ground	Outside, entrance to foyer	Front entrance area (external)	Static	Behaviour & Security
North	North 12	Ground	Entrance foyer, towards main entrance	Foyer and main entrance	Static	Behaviour

North	North 13	Ground	Rear corridor	Corridor, internal doors and external doors to hall/PE	Static	Behaviour
North	North 14	Ground	Science corridor, covering biology entrance/exit	Corridor and entrance/exit doors	Static	Behaviour
North	North 15	Ground	Outside, area to North Hall/canteen	External area outside hall and changing room entrance	Static	Behaviour & Security
North	North 16	Ground	Canteen	North canteen seating area	Static	Behaviour
ACE	ACE 1	Ground	Reception	Reception front desk, main entrance and student seating area	Static	Behaviour & Security
ACE	ACE 2	Ground	Outside, corner of ACE building	ACE car park and pedestrian gate	Static	Behaviour & Security

5. 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. There are no display screens that show the real-time CCTV. All imagery is accessed through iVMS software, which is installed on specific PCs of the staff listed below, and can only be viewed in their private office. The viewing of real-time imagery on iVMS is a duplicate of what is in general public view; however, caution and discretion is advised at all times.

All camera monitoring is actioned through the iVMS software. Each user has a unique account to access the iVMS software; the account permissions set to the appropriate level for the purpose of each user.

The iVMS software will only be used for the purpose for which it was designed; this will avoid 'unintentional' viewing of unrelated imagery.

The IT Network Manager shall be the system manager and will hold the administrators password and the right to allocate passwords to users of the system. New users must be authorised by either the Premises Manager or Assistant Headteacher.

The named persons with access rights to surveillance system are:

Staff Name, Job Role	Access Level
Robin Munby, Premises Manager	Full access (administrator)
Andrew Moorhouse, IT Network Manager	Full access (administrator)
Tom Fisher, Assistant Headteacher	View live and remote playback
Mike Evans, Assistant Headteacher	View live and remote playback
Rose Baker, IT Heldesk Technician	View live and remote playback

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, a record if kept of when each authorised user has received this training. The training register is kept on MS Teams: CCTV

6. Camera System Checks and Maintenance

A weekly check of the system will be carried out by the IT Network Manager to ensure that all cameras are receiving an image (basic functionality), that the time and date shown on the images are correct and the image quality is sufficient. All instances of camera malfunction must be reported as soon as possible, to the Premises Manager who will organise maintenance/repair on the system.

Image capture quality must also be tested on a monthly basis. Five 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 on the system check log on MS Teams: CCTV.

7. Retention of Recorded Images

Images recorded onto the hard drive of the CCTV systems shall be retained for a period of less than 28 days (unless images are being used for an ongoing investigation).

At the end of the 28 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.

Any retained images/footage must be recorded on the system access log (MS Teams: CCTV), 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 six 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 school's Data Protection Officer for logging and authorisation.

Should the request be a 'simple', unobtrusive request, this may be dealt with on site by the Premises Manager or the IT Network Manager.

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 access log.

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 MS Teams: CCTV.

10. Signage

Appropriate signage shall be displayed at all pedestrian and vehicle entrances to the school. Signage shall also be displayed at an externally visible point mounted on each individual building near its main entrance.

11. Contact Details

Name	Job Title	Contact Details
Robin Munby	Premises Manager	01377 253631 office@driffieldschool.org.uk
Andrew Moorhouse	IT Network Manager	
Mike Evans	Assistant Headteacher	

12. 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
The Education Alliance Surveillance Camera Policy