Adopted by Full Governors on 7.12.23 Agenda Item 7d

Whitley Bay High School

Surveillance Camera Code of Practice

November 2023

Date	November 2023 / Version 1 This code of practice will be reviewed annually
Review date	November 2024
Author	Peter Lilley, WBHS
Approved by	Finance and Premises Committee

SURVEILLANCE CAMERA CODE OF PRACTICE

1. SURVEILLANCE CAMERA CODE OF PRACTICE

1.1 The purpose of this Code of Practice is to regulate the management, operation and use of the surveillance camera system in operation at the school.

1.2 The system is a school owned internal system comprising of fixed and dome cameras only and does not record audio. The system is monitored onsite by nominated staff.

1.3 This Code of Practice will be subject to review annually, or if there is a change in legislation affecting the operation of surveillance cameras. The specific use of cameras on the school site will be reviewed on an annual basis via completion of a Data Protection Impact Assessment to ensure that use of the system remains justified and reasonable.

2. LEGISLATION

2.1 The use of a surveillance camera system is covered by a number of different laws and codes of practice.

2.2 The **Protection of Freedoms Act 2012** introduced a Surveillance Camera Code of Practice[1] and the appointment of a Surveillance Camera Commissioner[2] to promote the code and review its operation and impact. Local authorities and organisations responsible for public spaces must have regard for the Surveillance Camera Code of Practice (SCCP). It is recommended that other operators of surveillance camera systems, including schools, adopt the code voluntarily and the school has followed this approach.
The Surveillance Camera Commissioner, (latterly the Biometrics and Surveillance Camera Commissioner) has issued 12 principles to achieving compliance with the Surveillance Camera Code of Practice, with a self-assessment tool provided to allow organisations to assess compliance. The school completes this self-assessment on an annual basis.
At the time of writing, the Biometrics and Surveillance Camera Commissioner was due to resign at the end of October 2023, with no replacement appointed. Furthermore, the Data Protection and Digital Information Bill are due to be approved by parliament in early 2024. The Bill will see the functions of the Biometrics and Surveillance Camera Commissioner subsumed by the Investigatory Powers Commissioner and will remove the need for the government to publish a Surveillance Camera Code of Practice. The school has opted to follow the published Code of Practice at this time and will review future policy and direction when the situation becomes clearer.

2.3 The **Data Protection Act 1998** included the first Code of Practice[3] issued by the Information Commissioner's Office[4] regarding the use of Closed Circuit Television. This has since been updated to cover the broader area of Surveillance Cameras. The Information Commissioner's Office Code of Practice has then been formally replaced by the Surveillance Camera Code of Practice.

2.4 The **Regulation of Investigatory Power Act 2000** requires that when public authorities, such as the police or government departments, need to use covert techniques to obtain

[1] Surveillance Camera Code of Practice 2021 referred to throughout this document as 'SC Code of Practice'

[2] Surveillance Camera Commissioner referred to throughout this document as 'SCC'

[3] Information Commissioner's Office Code of Practice 2017 (Version 1.2) referred to throughout this document as 'ICO Code of Practice'

[4] Information Commissioner's Office referred to throughout this document as 'ICO'

covert information, they do so in a way that is necessary, proportionate and compatible with human rights. Although the school does not meet the criteria of those to which the Act applies, it notes the information contained within it and complies with Government [1] guidelines regarding any use of covert surveillance systems.

2.5 In addition to the above, this Code of Practice also accounts for our obligations in relation to the **Freedom of Information Act 2000** and the **Human Rights Act 1998** when using a surveillance system.

3. ASSESSING THE NEED FOR USE OF SURVEILLANCE CAMERAS

3.1 The school has surveillance cameras to facilitate two key aims:
1) Ensuring the safety and security of students, staff, and visitors by monitoring gated entry and exit points;
2) To deter acts of anti-social behaviour, vandalism and criminal behaviour in potentially vulnerable areas of the school and to assist with investigations should they occur.

3.2 In addition to facilitating one or both of the above aims, an assessment of whether to install a camera in a specific area will be carried out and this will consider:

- The nature of the problem we are addressing and whether the use of a surveillance camera is justified and likely to be an effective solution;
- Whether alternative solutions may be more effective than the use of a camera;
- The effect the use of a camera may have on individuals, and whether in light of this, the use is a proportionate response to the issue.

This assessment will be summarised in a Data Protection Impact Assessment which shall be carried out by a senior member of staff, with assistance and information from colleagues. The Assessment will use the template provided by the Surveillance Camera Commissioner therefore the school's Data Protection Officer will take an integral role in this process.

This assessment will be carried out:

- When a new camera is being installed
- When the location of an existing camera is being changed
- On an annual basis as part of a routine review of the necessity of the existing surveillance camera provision.

As per the guidance in the template, the school shall consult the ICO if we cannot adequately mitigate a high risk identified within the assessment.

4. GOVERNING THE USE OF SURVEILLANCE CAMERAS

4.1 Following completion and review of the Data Protection Impact Assessment, the Headteacher shall authorise the use of surveillance cameras on the school site.

4.2 The Headteacher has set out in this code of practice the specific staff members who shall have access to the system and the situations in which recordings will be shared with external agencies.

4.3 The Headteacher has delegated responsibility for ensuring that this Code of Practice is in place to the Data Protection Officer. Please see point 14 for an outline of the reviewing processes that will be completed to ensure that our system complies with the Surveillance Camera Code of Practices and continues to meet our legal obligations.

---

[1] Government guidelines regarding monitoring staff at work: https://www.gov.uk/data-protection-your-business/monitoring-staff-at-work

4.4 The school is registered with the ICO as a Data Controller and maintains this registration on an annual basis.

4.5 In line with Article 6 of GDPR, the school uses surveillance cameras lawfully to ensure it meets its legal obligation and public task of providing a safe and secure working and learning environment for staff, students and visitors.

4.6 Anyone wishing to make a complaint regarding the operation of the system or an apparent failure to comply with the requirements of the code must do so in writing to the Headteacher.

4.7 Where a staff member is believed to have committed a breach of this Code of Practice then the matter shall be investigated in line with standard school procedures. Further information on this process is available from the Headteacher's PA.

5. SELECTING AND SITING SURVEILLANCE CAMERAS

5.1 The location and type of camera to be installed will be finalised in line with the findings of the Data Protection Impact Assessment and the purpose for which the camera is being installed. This process will be co-ordinated between the School Business Leader, the Facilities Manager, and the IT Technical Co-ordinator. The school was provided with HIK Vision equipment for our CCTV solution as part of a new school build – this includes cameras and network video recorders. All equipment has been supplied and installed by MRM Solutions. Moving forward, the equipment will be maintained by IDS Fire & Security. In addition, the following key points will also be considered:

- That a 'privacy by design' approach will be followed, meaning that the equipment installed in a specific location will only collect the necessary information to meet the purpose for which it was installed;
- That a camera does not view areas which are not of interest and not intended to be the subject of the surveillance, such as individuals' private property;
- That if a camera is installed in response to a specific issue then the system is set up, where possible, to only record during the time when the issue usually occurs, or only records when movement occurs in a defined area;
- That the system is of the appropriate standard to ensure recorded images are of a useable quality (size, resolution and frames per second) to satisfy their intended purpose – this includes factoring in the camera's technical capability, the environment in which it is being placed and risk of vandalism.

5.2 The use of cameras in areas where there would be a heightened expectation of privacy, such as changing rooms, will only be authorised in the most exceptional circumstances where it is necessary to address a very serious concern. In these cases, the school will ensure that those under surveillance are aware that they are being recorded and that any requests to view images from these cameras are approved by the Headteacher.

5.3 A list of the location of each camera shall be maintained by the IT Technical Co-Ordinator and available on request. This list is included as Appendix 4 of the Data Protection Impact Assessment and will be designed to meet the needs of that document.

6. DEFINING THE BASIS ON WHICH STAFF ACCESS SURVEILLANCE CAMERAS

6.1 A live feed of the Surveillance Cameras will be accessible to the Front Office. This is to allow Front Office staff and members of the Site Team to monitor gated entry and exit points. The feed is also used to monitor the safety of staff, students and visitors with

cameras in corridors and open spaces. This feed is monitored by one to three staff at a time and can only be viewed from the Front Office.

6.2 We outline below, the three categories of staff who will be able to access the system along with key reasons as to why this access is required. All users are inducted in the use and operation of the system in line with the guidelines listed in this Code of Practice.

6.3 Facilities Manager

- To assist the School Business Leader with management of the safety, security and wellbeing of those onsite;
- To investigate incidents of anti-social behaviour, vandalism, accidents and criminal behaviour;
- To ensure the cameras are in working order.

6.4 IT Technical Co-ordinator

- To gather recordings as part of investigations into incidents of anti-social behaviour, vandalism and criminal behaviour;
- To prepare recordings that are to be provided to external agencies;
- To ensure the system is functioning, recording, retaining and deleting data in line with this Code of Practice.

6.5 Front Office Staff

- Ensuring the safety, security and welfare of students and visitors by monitoring the entry and exit points in real time;
- Providing access to recordings to pastoral staff where there is a concern regarding student welfare or when clarifying the circumstances of an incident involving students.
- To gather recordings as part of investigations into incidents of anti-social behaviour, vandalism and criminal behaviour;
- To prepare recordings that are to be provided to external agencies;

6.6 To ensure the correct use of the system, Reference Document A lists the procedures that have been produced for all three named user groups to assist them in accessing the cameras and recordings appropriately. Furthermore, all users shall use a log, (please see Reference Document B), to document when they access the system. Logs are stored on SharePoint with access only available to the named users and the Data Protection Officer. The Data Protection Officer will monitor use of the system and logs on a periodic basis to ensure staff are accessing and documenting system use appropriately, and that the system is being used for the intended purposes.

7. SECURE ACCESS, STORAGE & RETENTION OF INFORMATION

7.1 All user accounts for accessing our system are password protected. Management of user accounts is the responsibility of the IT Technical Co-ordinator.

7.2 The recordings are held on a specific school server with hard drives stored on a secure area of the school site. The hard drives are also password protected to further secure the data.

7.3 The system is set to store data for a period of 30 days before it is automatically deleted. This time period has been selected based on school experience of the length of time in which requests to view footage are made.

8. ACCESS PROCEDURES

8.1 Any of the school's designated users may access and save images or recordings from the system. Prior to accessing the system, the designated user must determine that the purpose of the request aligns with the key aims outlined in point 3.1. Should an individual request access and the school's delegated user determines that the purpose does not align with the key aims outlined in point 3.1, the designated user will refer the request to the Headteacher, who will make the final determination. If an image or clip is extracted from the system, this will be shared with the requestee only (unless there is a clear need for others, e.g. senior or pastoral manager, to see the information). This will be shared via the School's SharePoint system within a dedicated folder setup for recordings. Recordings will be named in the format or 'yymmdd overview of incident' to allow them to be easily identifiable.

8.2 Designated users will be responsible for regularly checking the log and ensuring that any saved images or clips are routinely deleted from the OneDrive folder after 30 days. Images will only be retained for a longer period when required as part of an ongoing investigation. This will be recorded in the log.

9. DISCLOSURE TO EXTERNAL AGENCIES

9.1 The Criminal Procedure and Investigations Act 1996 places a statutory obligation on the Police to record and retain material that may be relevant to an investigation. In addition, the Police and Criminal Evidence Act 1984 allows the Police to seize evidence, and this can be achieved via a formal search warrant. Additional rules for the processing and sharing of recorded images is covered by UK GDPR and the Data Protection Act 2018.

9.2 The school will disclose images to the Police only on request and where use of the images is thought to be of significant benefit for the prevention and detection of crime, to safeguard children or to protect the welfare of the individuals involved and/or others. Should the school be unsure of the appropriateness of releasing information, then a formal legal request will be required before any images are provided.

9.3 All requests to disclose images shall be approved by a member of the Senior Leadership Team and co-ordinated with one of the designated system users who will process and log the request as detailed above.

9.4 Any other external requests for images will be approached with extreme care as wider disclosure may be deemed unfair to the individuals concerned. In some limited circumstances it may be appropriate to release information to a third party, where their needs outweigh those of the individuals whose information is recorded. All such requests shall be evaluated on a case-by-case basis by the Headteacher and, if authorised, recorded in the same manner as detailed above. The Headteacher will evaluate the validity of the request and whether there is a risk to the safety and data security of others involved.

9.5 As per point 8.2, images shall be retained by the school where they are part of an ongoing investigation.

10. SUBJECT ACCESS REQUESTS

10.1 Under data protection legislation, individuals have the right to request access to information that is held about them. This is requested through a process called 'Subject Access Request' (SAR) and are dealt with in line with established procedure. Further information, and a copy of this procedure, is available from the Data Protection Officer.

10.2 Where a subject access request is approved and involves providing information from our surveillance cameras, this will be completed in line with guidance provided by the ICO. Should a decision be made to extract and transfer images on a permanent basis to facilitate a request, then the process detailed above in point 8 will be followed.

11. FREEDOM OF INFORMATION REQUESTS

11.1 The Freedom of Information Act 2000 provides public access to information held by public authorities.
It does this in two ways:

- Public authorities are obliged to publish certain information about their activities;
- Members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland.

Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

The Act does not give people access to their own personal data (information about themselves) as this is covered by Subject Access Requests.

As our surveillance cameras allow individuals to be identified, it is unlikely that this information can be disclosed in response to a Freedom of Information request. Requests for information on the operation, siting and cost of the system may not be appropriate to disclose depending on the nature and specifics of the request. Further information on Freedom of Information requests is available from the Data Protection Officer.

12. SYSTEM MAINTENANCE

12.1 The school has entered into a maintenance contract with IDS Fire & Security who will co-ordinate system wide standards and adjustments with our Facilities Manager and IT Technical Co-ordinator. Maintenance checks will include ensuring that:

- All cameras are operating as intended;
- The system is producing good clear quality information which is maintained throughout the recording process;
- That high-level compression is not leading to low picture quality on playback;
- That the recording process is not leading to inadvertent system corruption;
- That recordings include an accurate date and time stamp (taking into account changes between GMT/DST);
- That the system is not vulnerable to, or being the victim of unauthorised access;
- That any software updates provided by Avigilon have been processed onto the school system and that all cameras remain compatible with the updated software.

13. HIGHLIGHTING THE USE OF SURVEILLANCE CAMERAS ON THE SCHOOL SITE

13.1 Signage highlighting the use of surveillance cameras will be displayed at the main entrance points to the site. If cameras are discreet, or in locations where people may not expect to be under surveillance, then the signage will be of a more prominent nature. As all signs are on the school site and, it can be assumed are the property of the school, the signage will state the following ‘You are currently in an area monitored by surveillance cameras. Please contact 0191 731 7070 if you require further information.’

13.2 The school reserves the right to use covert surveillance cameras in exceptional circumstances – please refer to point 2.4 for further information on the use of such systems.

14. REGUARLY ASSESSING THE APPROPRIATENESS OF OUR SURVEILLANCE CAMERAS

14.1 The Data Protection Officer shall complete the following actions on an annual basis:

- Surveillance Camera Commissioner's Data Protection Impact Assessment for use of Surveillance Cameras;
- Surveillance Camera Commissioner's Self-Assessment Tool to ensure compliance with Surveillance Camera Commissioner's 12 principles.

The Data Protection Officer will then meet with the School Business Leader to review the information in the two assessments, and, utilising the Data Protection Officer's ability to review the user logs for accessing the system, confirm that the use of surveillance cameras remains appropriate and justified. Should any issues or non-compliance with procedures be identified then action will be taken to rectify this as appropriate. Once this is complete, the documents with be dated and signed, with the next review to be completed within 12 months of that date.

14.2 This Code of Practice will be reviewed annually.

Reference Document A

Procedure for accessing Surveillance Camera System for named users

Instructions for all users:

- Users must not disclose their login details for the Surveillance Camera System to another member of staff;
- Access to the system must be for a specific purpose (as defined below);
- If you are unsure if a reason for access meets the guidance provided below then users should seek clarification from a member of the Senior Leadership Team before proceeding – Do not access the system until you are satisfied that the request meets our criteria;
- All access to the system must be recorded on the log;
- When accessing the system ensure that your screen is not being viewed by a third party other than the person requesting access;
- Ensure that any images or clips are recorded, uploaded and shared in line with details listed in the School's Code of Practice.

Specific guidance for Facilities Manager regarding appropriate reasons for accessing the system

In addition to the overview statement, examples are given of appropriate reasons for accessing the system:

- 'To assist the School Business Leader in managing the safety, security and wellbeing of those on site'

For example, this may be to investigate health and safety queries regarding overcrowding or crushing at entry / exit points; or to monitor the effectiveness of lighting in the car park

- 'To investigate incidents of anti-social behaviour, vandalism and criminal behaviour'

For example, this may include to investigate alleged trespassing, criminal damage to the site or cars/bikes; or, at the request of the School Business Leader, to investigate allegations of physical violence, theft or misconduct.

- 'To ensure the cameras are in working order'

For example, this may be as part of pre-planned maintenance to ensure that the cameras are in working order; or in response to a report of a damaged camera from another member of staff.

Specific guidance for IT Technical Co-ordinator regarding appropriate reasons for accessing the system

In addition to the overview statement, examples are given of appropriate reasons for accessing the system:

- 'To gather recordings as part of investigations into incidents of anti-social behaviour, vandalism and criminal behaviour'
- 'To prepare recordings that are to be provided to external agencies'
- 'To ensure the system is functioning, recording, retaining and deleting data in line with this Code of Practice'

For example, this may be as part of pre-planned maintenance to ensure that the system is in working order; or in response to a report of a system issue from another member of staff.

Specific guidance for Front Office staff regarding appropriate reasons for accessing the system

In addition to the overview statement, examples are given of appropriate reasons for accessing the system:

- 'Ensuring the safety and security of students and visitors as they move around the site'

For example, concern has been raised regarding a vulnerable student failing to return to lessons after visiting the office or toilet and the system is used to look at corridor feeds to confirm that they did return to their classroom – the requests of this nature must be genuine and where the request comes from a member of staff with a legitimate reason

- 'Providing access to recordings for staff checking on the welfare of a student and clarifying the circumstances of an incident involving students'

For example, a member of the Leadership Team is investigating a physical altercation between students in a location covered by a camera and asks to view footage to help establish the facts. Requests of this nature must come from either a member of the Leadership or Pastoral Teams.

- 'To gather recordings as part of investigations into incidents of anti-social behaviour, vandalism and criminal behaviour'
- 'To prepare recordings that are to be provided to external agencies'

Reference Document B

User logs for accessing Surveillance Camera System

Whitley Bay High School - Surveillance Camera Access Log

All occasions when you access the system must be recorded below

Date of accessing system	Name of staff member accessing system	Name of person making the request	Names of other people viewing the footage with you	Does request reason meet criteria? If not, deny access and seek clarity from SLT	Date & time of footage being viewed, reason for viewing the footage & any action taken with regard to copying or storing image (this should be completed on SharePoint with folder password protected and shared only with staff/agency who have genuine need to view image/recording)	If image shared via SharePoint, list date of deletion below (should be within 30 days of access date) unless otherwise specified in column f
20/10/23	*RPP*	*PEL*	*PEL & SMW*	*Yes*	*20/10/23 - 14.00 to 14.05 - footage of a student accessing staff toilet - print screen of student taken and uploaded to SharePoint folder, then shared with DJL for confirmation of identity and further*	*19/11/2023*
20/10/23	*BDW*	*N/A*	*N/A*	*N/A*	*System maitenance - BDW viewed all cameras to ensure all are operating as intended*	*N/A*