

Awel y Môr Primary School



CCTV Policy

1. Introduction

1.1 The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Awel y Môr Primary School

1.2 The system comprises a number of fixed and dome cameras located around the school site. All cameras are monitored from a Central Site Office and are only available to designated staff – members of the ICT Technician Staff, Caretakers and members of the Senior Leadership Team. Other significant staff can have access through one of the aforementioned designated staff.

1.3 This Code follows Data Protection Act guidelines.

1.4 The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties.

1.5 The CCTV system is owned and maintained by the school.

2. Objectives of the CCTV scheme

- 2.1
- (a) To increase personal safety of staff students and visitors and reduce the fear of crime
 - (b) To protect the school buildings and their assets
 - (c) To support the Police in a bid to deter and detect crime
 - (d) To assist in identifying, apprehending and prosecuting offenders
 - (e) To protect members of the public and private property
 - (f) To settle disputes between pupils
 - (g) To assist in managing the school

3. Statement of intent

3.1 The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

3.2 The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

3.3 Cameras will be used to monitor activities within the school and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well being of the school, together with its visitors.

3.4 Staff have been instructed that static cameras are not focused on private homes, gardens and other areas of private property.

3.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. CD images/disks will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. CD images/disks will never be released to the media for purposes of entertainment.

3.6 The planning and design has endeavoured to ensure that the 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.

3.7 Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the school CCTV.

4. Operation of the system

4.1 The system will be administered and managed by the Headteacher, in accordance with the principles and objectives expressed in the code.

4.2 The day-to-day management will be the responsibility of the Senior Leadership Team (SLT) during the day.

4.3 The CCTV system will be operated 24 hours each day, every day of the year.

5. Control Room

5.1 The ICT Technicians will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

5.2 Access to the CCTV Recording will be strictly limited to the SLT & the ICT Technicians. The DVD recording is password protected.

5.3 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the Headteacher or the deputy and must be accompanied by them throughout the visit.

5.4 Emergency procedures will be used in appropriate cases to call the Emergency Services.

6. Liaison

6.1 Liaison meetings may be held with all bodies involved in the support of the system.

7. Monitoring procedures

7.1 Camera surveillance may be maintained at all times.

7.2 Access to the recordings is only available via Password protection.

8. Image storage procedures

8.1 Images are stored electronically and sent directly to the Quays, an LEA building. If images are required for evidential purposes, the following procedures for their use and retention must be strictly adhered to:

- i. The images need to be transferred to a disk which must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence disk store until collected.
- ii. Each disk must be identified by a unique reference number.
- iii. The disk should be new or cleaned of any previous recording.
- iv. If the disk is archived at a later date, the reference number must be noted.
- v. Any section copied will be placed on the T Drive and restricted to nominated persons.

8.2 Disks may be viewed by the Police for the prevention and detection of crime, authorised officers of NPTC for supervisory purposes, authorised demonstration and training.

8.3 A record will be maintained of the release of disks to the Police or other authorised applicants.

8.4 Viewing of disks by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.

8.5 Should a disk be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (i) of this Code. Disks will only be released to the Police on the clear understanding that the disk remains the property of the school, and both the disk and information contained on it are to be treated in accordance with this code. The school also retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained thereon. On occasions when a Court requires the release of an original disk this will be produced from the secure evidence disk store, complete in its sealed bag.

8.6 The Police may require the school to retain the stored disks for possible use as evidence in the future. Such disks will be properly indexed and properly and securely stored until they are needed by the Police.

8.7 Applications received from outside bodies (e.g. solicitors) to view or release disks will be referred to the Headteacher. In these circumstances disks will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

9. Breaches of the code (including breaches of security)

9.1 Any breach of the Code of Practice by school staff will be initially investigated by the Headteacher, in order to take the appropriate disciplinary action.

9.2 Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

10. Assessment of the scheme and code of practice

10.1 Performance monitoring, including random operating checks, may be carried out by the ICT Technicians under the guidance of the Headteacher.

11. Complaints

11.1.1 Any complaints about the school's CCTV system should be addressed to the Headteacher.

11.2 Complaints will be investigated in accordance with Section 9 of this Code.

12 Access by the Data Subject

12.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

12.2 Requests for Data Subject Access should be made to the Headteacher.

13. Public information

Copies of this Code of Practice will be available to the public from the School Office and the Headteacher.

Summary of Key Points

- This Code of Practice will be reviewed every two years.
- The CCTV system is owned and operated by the school.
- The Control Room is not open to visitors except by prior arrangement and good reason.
- Liaison meetings may be held with the Police and other bodies.
- The Hard Drive may only be viewed by Authorised School Officers, Control Room staff and the Police.
- Images required as evidence will be properly recorded on a disk from the Hard Drive, witnessed and packaged before copies are released to the police.
- Disks will not be made available to the media for commercial or entertainment.
- Disks will be disposed of securely by incineration.
- Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with academy policies and procedures and be authorised by the Headteacher. The Data Protection Co-ordinator for Schools, Education Department, provides additional information if required.
- Any breaches of this code will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the Headteacher

S.J. Greasley

Approved: Feb 2020

Review Date: Feb 2022

