CCTV Policy

Reviewed September 2017

1. Introduction

- The purpose of this Policy is to regulate the management, operation and use of the monitored Closed Circuit Television (CCTV) system owned by Cedar Lodge School hereafter referred to as 'the school'.

- The system comprises of fourteen cameras located around the exterior/ and interior* of the school building.

2. Objectives of the CCTV system

- To protect pupils, staff and visitors
- To increase personal safety and reduce the fear of crime
- To protect the school buildings and assets
- Without prejudice, to protect the personal property of pupils, staff and visitors.
- To support the police in preventing and detecting crime
- To assist in identifying, apprehending and prosecuting offenders
- To assist in managing the school

3. Statement of intent

- The CCTV system 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.
- The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.
- Cameras will be used to monitor activities within the school grounds and buildings to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well being of the pupils, staff and school, together with its visitors.
- The system has been designed to deny observation on adjacent private homes, gardens and other areas of private property.

- Materials or knowledge secured as a result of use of the CCTV system will not be used for any commercial purpose.
- Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police.
- The planning and design has endeavoured to ensure that the system 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.
- Warning signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas covered by the school CCTV system.
- This System Policy follows Data Protection Act guidelines.

4. On Site System Management

- The organisation, which is the school, is the Data Controller under the Act. The system will be administered and managed by AMEY FM in accordance with the principles and objectives expressed in the policy.
- The Data Controller will inspect all records relating to 'On Site Management' on a monthly basis. The date and time of each inspection together with signature will be inserted on each individual record. In addition the Data Controller may carry out additional random checks to ensure that the system is being managed correctly.
- The day-to-day management will be the responsibility of the AMEY FM Site Manager who will act as the responsible to the Data Controller.
- The system and the data collected will only be available to the Data Controller, the Senior Management Team and the On Site System Manager.
- The CCTV system will be operated and recorded 24 hours each day, every day of the year.
- Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

5. Responsibilities of the On Site Manager

- To check and confirm the efficiency of the system daily i.e. that cameras are functional the system is recording properly and that the date and time on the recorder are correct. The results will be logged on the appropriate sheet and any defects reported to the appropriate person to initiate repair.
- To satisfy him/her self of the identity of any person wishing to view images and the legitimacy of the request. Where any doubt exists access will be refused.
- If out of hours emergency maintenance arises, he/she must be satisfied of the identity and purpose of contractors before allowing access to the system.

6.Liaison

- Liaison meetings will be held as required with all bodies involved in the support of the system.

7. Digital media viewing and download procedures

- In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events must be prepared in accordance with the following procedures: -
    - Download media must be identified by a unique mark.
    - Before use, download media must be cleaned of any previous recording.
    - The On Site System Manager will register the date and time of download media insertion, including its reference.
    - A download media required for evidential purposes must be sealed, witnessed, signed by the appropriate System Manager, dated and stored in a secure store. If download media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the System Manager, dated and returned to the secure store.
    - If download media is archived the reference must be noted.

- A record will be maintained of the release of download media to the police or other authorised applicants. A register will be available for this purpose.
- Viewing of images by the police must be recorded in writing and in the log book.
- Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the download media (and any images contained thereon) remains the property of the school, and both the download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of an original downloaded media this will be produced from the secure store, complete in its sealed bag.
- The police may require the school to retain the stored downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and properly and securely stored until they are needed by the police.
- Copyright of all images and recordings will remain the property of the school.
- Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the Data Controller. In these circumstances downloaded media 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.

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

- Any breach of the System Policy by school staff will be initially investigated by the Data Controller, in order for him/her to take the appropriate action.
- Any serious breach of the System policy will be the subject of an immediate independent investigation by the Education Authority Belfast Region's Security Advisor. The investigation will also make recommendations on how to remedy the breach.

9. Complaints

- Any complaints about the school's CCTV system should be addressed to the Data Controller.

10. Access by the Data Subject

- 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.
- Requests for Data Subject Access should be made on an application form available from the Data Controller.

11. Public information

- Copies of this System Policy will be available to the public by applying to the Data Controller.

12.Policy Review

- This System Policy will be subject to annual review including consultation with all interested parties; e.g. Board of Governors. The review will as well as assessing the need for retention of the Monitored CCTV system ensure that all parts of the policy are up to date and relevant and that any relevant changes to the Law or Codes of Practice are reflected in the document. A page will be attached to this document giving the date of the review what parties were consulted and details of any decisions and changes made. The review sheet will be signed by the Data Controller.

_____ Date _____

'Data Controller'

_____ Date _____

'On Site System Manager'