National and local guidance in relation to the Covid 19 pandemic may over rule aspects of this policy.

CCTV Policy

STATUS: **Approved**

REVIEW DATE: **September 2022**

"The Academy believes that inclusive practice is central to developing quality teaching and learning. As such we endeavour to provide a supportive framework that responds to pupils' needs and overcomes potential barriers for individuals and groups of pupils and to ensure that pupils of all abilities and needs are fully included in the life of the school. The ethos of this statement underpins all Oldbury Academy's policies."

This policy should be read in conjunction with other school policies as/where necessary.

Introduction

The purpose of this Policy is to regulate the review, management, operation, and use, of closed circuit television (CCTV). At Oldbury Academy CCTV is in use to:

- increase personal safety of students, staff and visitors, and reduce the fear of crime
- assist in managing the school
- protect the school buildings and their assets
- support the Police in a bid to deter and detect crime
- assist in identifying, apprehending and prosecuting offenders
- protect members of the public and private property

This Code follows the Data Protection Act guidelines and will be subject to review annually to include consultation as appropriate with interested parties.

1. The system

1.1 There are two CCTV systems in operation on the school site. One is owned and managed by Interserve Facilities Management and the other owned by the school.This policy relates **only** to the CCTV system that is owned by the school as Interserve Facilities Mangement have their own policy and control systems in place.The school CCTV system comprises of 140 fixed cameras located around the school site, 115 internally and 25 externally. The CCTV can be viewed and a remote link access is available to designated members of the Senior Leadership Team or their authorised nominees. Fourteen (14) of the cameras are not on the main DVR system.

2. Statement of intent

2.1 The CCTV Scheme will be registered annually by the school with the Information Commissioner under the terms of the General Data Protection Regulations (GDPR) and will endeavour to comply with these requirements and the Commissioner's Code of Practice.

2.2 The school will treat the system and all information, documents and recordings obtained and used, as data that is protected by the GDPR.

2.3 Cameras will be used to monitor activities within the school and its play and public areas, for the purpose of securing the safety and well-being of the pupils, staff and visitors and to identify criminal activity actually occurring, anticipated or perceived.

2.4 Static cameras are positioned so they do not focus on private homes, gardens or other areas of private property.

2.5 Unless an immediate response to events is required, staff must not direct cameras off site at an individual, their property or a specific group of individuals, without an authorised, documented, instruction from a member of the Senior Leadership Team or by police instruction, endorsed by the Head Teacher, for Directed Surveillance, as set out in the Regulation of Investigatory Power Act 2000.

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

2.7 Planning, design and installation 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.

2.8 Warning signs, as required by the Code of Practice have been placed at all access routes to areas covered by the school CCTV including entrances and recreational spaces.

3. Operation of the system

3.1 The system will be managed by the School Operations Manager and administered by the Data and ICT Development Manager.

3.2 The day-to-day management will be the responsibility of both the Senior Leadership Team (SLT) and the School Operations Manager.

3.3 The CCTV information will only be accessed by SLT members or their authorised nominee, and the School Operations Manager.

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

3.5 The 14 school cameras will be monitored by the School Operations Manager and administered by the Data & ICT Development Manager.

4. System Equipment & Control

4.1 The School Operations Manager, will check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional.

4.2 Access to the CCTV equipment will be strictly limited to the SLT and their nominee, and the School Operations Manager.

4.3 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits to view information will not be permitted. Visitors must first obtain permission from the SLT and must be accompanied throughout the visit.

4.4 A visitor's book will be maintained at school reception. Full details of visitors including time/date of entry and exit will be recorded.

5. Liaison

Liaison meetings may be held with all bodies involved in, or requiring, the support of the system eg Police.

6. Monitoring procedures

6.1 Camera surveillance will be maintained at all times.

6.2 A monitor is installed to which pictures will be continuously recorded. A monitor and recordings for some of the buildings will be captured on the local DVR held in that area.

6.3 Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with school policies and procedures and must be authorised by the Data Controller.

7. Image storage procedures

7.1 The images are stored on the CCTV Hard Drive for a period of 30 days and will be over written as the disk becomes full. If images are required for evidential purposes, the following procedures for their access, use and retention will be strictly adhered to:

7.1.1 The images required will be transferred to an encrypted USB which will be placed in a sealed envelope, dated and stored in a separate and secure place until collected.

7.1.2 Each USB will be identified by a unique reference number.

7.1.3 The USB used will be new or cleaned of any previous recording.

7.1.4 If the USB is archived the reference number will be noted.

7.1.5 All USB'S made will be recorded in the CCTV Log.

7.2 Data on USB'S may be viewed by the Police for the prevention and detection of crime, under part 3 of the Data protection act 2018, which implements an EU directive (directive 2016/680) and is seperate from the GDPR regime.

7.3 A record will be maintained in the CCTV Log of the release of recordings to the Police or other authorised applicants.

7.4 Viewing of footage by the Police will be recorded in writing and in the log book.

7.5 Should footage be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (i) of the Code of Practice. Footage will only be released to the Police on the clear understanding that the USB remains the property of the school, and both the USB and information contained on it are to be treated in accordance with the code of practice. The school also retains the right to refuse permission for the Police to pass to any other person the USB or any part of the information contained thereon. On occasions when a Court requires the release of footage copied from the CCTV system this will be produced and kept secure and made available as required.

7.6 The Police may require the school to retain the stored USB for possible use as evidence in the future. The USB will be properly indexed and securely stored until requested by the Police.

7.7 Applications received from outside bodies to view or release disks will be referred to the Data Controller. Requests from eg solicitors will normally be met 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. Access by or on behalf of the Data Subject

8.1 GDPR provides Data Subjects (individuals to whom "personal data" relate, and their parents or authorised carers) with a right to data held about themselves, including those obtained by CCTV.

8.2 A fee can be charged in such circumstances, this will be : £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

8.3 Requests for Data Subject Access should be made to the Data Controller and still images will be provided as per 8.1.(i) with the images of other pupils and adults obscured to prevent identification and inappropriate disclosure of their personal information.

9. Breaches of GDPR

9.1 Any breach of the GDPR by school staff will be investigated by the Head Teacher or their nominee, and could lead to disciplinary action including dismissal.

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

10. Data Retention

Recordings will be retained for 30 days before being overwritten.

11. Public information

Copies of this policy will be available via the school website.

12. Complaints

12.1 Complaints regarding Data breaches will be investigated in accordance with Section 9 of this Code.