KLB School CCTV System
Code of Practice and Operational Procedures
Version 1.2
January 2016

1. Introduction

KLB School has a CCTV system installed for the purposes of site security and pupil management. The school has a joint venture called Sport Wotton for the management of its sports facilities outside normal school hours and the coverage of the school system also includes the playing surfaces on the New Road site belonging to the Wotton Community Sports Foundation (WCSF).

The system and scheme are referred to in the School's Data protection registration with the office of the Data Protection Commissioner.

The purpose of this document is to provide guidance on how the school will address the various legal requirements and operation of the CCTV system.

Nominated KLB staff will manage the scheme. Selected KLB staff and staff of the sports facility management organisation will be authorised and receive adequate training and guidance to ensure that their use of the system falls within the requirements of the necessary legislation.

It should be noted that the images/data from the CCTV System fall under the School's Freedom of Information and Data Protection Act procedures.

2. Ownership

The **Scheme Manager** is the Facility Manager. This person will oversee

- the management and implementation of the Code of Practice, procedure, installation of new system and audits of the scheme;
- the day to day operation of the CCTV system within the school;
- the operation and compliance with the Code of Practice by authorised users;
- the general operation of the scheme (including registration of the system with the ICO) and arrange for the necessary maintenance of the system.

Authorised Users are nominated individuals, who, as part of their duties may be required to view footage from the CCTV system. Specific access, training and guidance will be provided.

3. Overview of legal Requirements

The oversight of the CCTV system will ensure that the requirements contained in the legislation below are adhered to:

Data Protection Act principles– As detailed in the KLB Data Protection Policy document

Human Rights Act – Article 8 on the right to respect for private and family life, and Article 14 on prohibition of discrimination.

Freedom of Information Act 2000.

4. Aims and Purpose of the System

The School CCTV system has been installed to ensure that issues relating to pupil management and site security can be addressed for the benefit of those who work and attend the school and the associated sports facilities. The objective of the system will be to:

- protect the School / Trust buildings and their assets.
- increase personal safety for staff, students, contractors and the general public.
- assist in identifying, apprehending and prosecuting offenders.
- support the Police in a bid to deter and detect crime.
- assist other agencies in justifiable (to Scheme Manger) incidents in need of investigations
- assist in managing and monitoring behaviour and vandalism on campus.

The system therefore will:

- assist in the identification of individuals involved in crime and public order offences on the school site
- assist in the identification of individuals breaching the school rules on the school site and WCSF grounds
- assist the Site Team in monitoring the school site when the intrusion alarm is activated or issues relating to trespass/unapproved use of the school facilities
- assist in the effective management of vehicle movements on the school premises
- assist in the detection of crime on both the school site and the WCSF property

The CCTV system is not continually monitored but there is continuous and motion detection recording. It should be noted that there is no audio monitoring associated with the KLB School CCTV system.

5. System Review

The school will conduct an annual audit of its CCTV system. This will be compiled by the end of September each year. The scope of this will be to:

- Confirm who has access and their levels of access
- Ensure that required maintenance has been carried out
- Review any necessary changes to the operational of the system and associated operational procedures
- Review system coverage
- Review download usage
- Review storage time
- Review public awareness of the system
- Ensure compliance with the ICO Code of Practice
- Ensure renewal of the notification to the ICO of the CCTV system
- Ensure that the system is not being used or abused.

6. Operational Practices

The following requirements shall be complied with:

1. All users shall sign to confirm that they have read the guidance contained in this document and that they will comply with the necessary requirements
2. All users should familiarise themselves with the requirements on the School's FOI and Data Protection Policies
3. The system shall only be used by authorised users
4. No images/data shall be distributed
5. No images/data shall be released for external use unless approved under the school's FOI process and any enquirer should be directed to this process / procedure when requesting information. All releases shall be recorded
6. Internal requests for images/data shall be considered by the authorised user to ensure that the viewing / exporting of any images/data is in compliance with the requirements contained in this document.
7. No images from the CCTV system shall be published without the written permission of the Data Controller
8. The destruction of any images/data shall be in a secure manner, e.g. confidential waste /shredded etc.
9. The use of images/data shall be for the purposes described in section 4 of this document
10. Copying of material will only be made for a valid, specific reason and securely destroyed when no longer required.

11. All recording equipment shall be secured in a locked room and be password protected
12. Any images / data exported from the system shall be stored securely. The system shall record what has been exported and users may be required to provide justification as to why the images / data have been exported.
13. Any faults to the system should be reported to the Scheme Manager.
14. Signage shall be provided to inform users of the site that a CCTV system is operational and provide the contact details of the school should there be any queries or requests for information.

Please note that it is a criminal offence to give access to, or disclose recorded data / images to person(s)/organisations other than allowed within the procedures and by the process as directed by this policy/operational procedure ("The Data Protection Act 1988").

7. Camera Location and Maintenance

The following point shall be complied with in setting up / changes / maintenance of the system:

- The operational requirements of every camera shall be recorded in accordance with BSEN50132 including details on intended duration of use, conditions at the site, signage and privacy issues etc
- Wherever possible, CCTV equipment shall be sited to prevent undue or unnecessary intrusion to the privacy to users of the school site and the WCSF facilities.
- The School CCTV system shall not be used to observe private land around the school
- To unnecessarily monitor or zoom into a person/vehicle/office is viewed as an invasion of privacy
- Images shall be held only for as long as necessary – this shall be for a 10 day period so that the opportunity to review issues is available. The digital information will be overwritten by current imagery. This shall apply except in exceptional circumstance such as seizure by police, when provided to enforcement agencies or for reasons of disciplinary action etc.
- Following installation, all equipment shall be suitably maintained either using internal resources or covered by a maintenance agreement. The maximum period between inspections of the system should be no longer than 12 months.
- Routine checks of the camera/system function shall be under taken by the Scheme Manager. These checks shall take place on a weekly basis to ensure that the system is operating as intended. This shall include the functioning of the system as well as ensuring that the date and time on the system are correct.

8. System Access

Requests for access to the system shall be via the Scheme Manager.

When granting users access to the system, restrictions based on need shall be applied to their account by the Scheme Manager. This may for example include restricting:

- access to certain cameras
- times of access
- images / data download capability etc.

Training will be provided to all new users.

Approved by Governors' Health and Safety Committee: 5 February 2016