



# Whitby School

## Closed Circuit Television Policy

### Governance Status

This policy was first issued in May 2013 and was adopted by the Governing Body on 25.06.13. It will be renewed in light of any new legislation or guidance, as required, or every three years.

Review dates	By Whom	Approval dates
November 2013	Staff and Governors	2 December 2013
September 2015	Staff and Governors	21 September 2015
April 2017	Staff and Governors	22 June 2017
October 2020	Staff and Governors	20 October 2020
December 2024	Staff and Governors	4 February 2023

**Signed by the Chair:**

## **1. Introduction**

1.1 The purpose of this Policy ("the Policy") is to regulate the management, operation and use of closed circuit television ("CCTV") at Whitby School ("WS") on both the Prospect Hill Site and Airy Hill Site.

1.2 The CCTV systems ("the Systems") comprise a number of fixed and dome cameras located around the School sites. All cameras are monitored by selected staff, for the reasons stated in section 2 below,. These staff are as follows:

### **1.2.1 Head of School/Head Teacher**

Deputy Head Teacher

Senior Leadership Staff

Business Manager

ICT Network Staff

Site Management Staff

Office and Reception Staff

Pastoral Staff

Kitchen Managers (Kitchen only)

Office staff under the direction of the Senior Office Administrator and the ICT Team under the direction of the Network Manager.

1.2.2 Staff responsible for operating the systems – 'Operator' (ensure the cameras are correctly maintained and working) are as follows:

ICT Network Staff

Site Management Staff

Business Manager

1.2.3 Staff responsible for controlling the systems – 'Controller' (ie, to use the reviewing station and extracting footage, as per this policy) are as follows:

ICT Network Staff

Site Management Staff

Pastoral Staff

1.2.4. Staff who can view the extracts:

Named persons in 1.2.1

Senior Leadership Team

1.3 The Policy will be reviewed as required by the Governing Body and interested parties will be consulted.

1.4 The Systems are owned by Whitby School.

## **2. Objectives of the Systems**

- a) To increase the personal safety of School site users and their property, by deterring vandalism and ensuring that unauthorised visitors do not enter the site and students do not leave either site, without permission.
- b) To protect WS's buildings and assets and alongside this aim, to support the School and, if necessary, the Police, in the prevention and detection of crime, including damage to property.
- c) To assist WS in identifying, apprehending and disciplining offenders after an event has occurred.

## **3. Statement of intent**

- 3.1 The Systems 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 WS will treat the Systems and all information, documents and recordings obtained and used as data which is protected by the Act.
- 3.3 Cameras will be used for the objectives set out in paragraph 2 hereof.
  - 3.4.1 Static cameras will not focus on private homes, gardens or other areas of private property.
  - 3.4.2 Unless an immediate response to events is required, staff will not direct CCTV cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained in accordance with the Regulation of Investigatory Powers Act 2000 as amended.
- 3.5 Materials or knowledge secured through the Systems will not be used for any commercial purpose. Recorded materials will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Recorded materials will never be released to the media for purposes of entertainment.
- 3.6 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 Systems.

## **4. Operation of the System**

- 4.1 The Systems will be administered and managed by the Head of School and ICT Network Manager, in accordance with the principles and objectives expressed in the Policy.
- 4.2 The day-to-day operation of the Systems will be the responsibility of the staff named in section 1.2.2 above in this policy, during the day, out of hours and at weekends.
- 4.3 The Systems will be operated 24 hours each day, every day of the year.

## **5. Operational Control**

- 5.1 The Network Manager will check the efficiency of the Systems regularly (or ask another member of staff named in section 1.2.2 to do this in his absence) - in particular that the equipment is properly recording and that cameras are functional.
- 5.2 If an emergency arises out of hours, verbal permission must be obtained from the Head of School for an appropriate named person, from section 1.2.2 above, to view or process recorded material, with a completed CCTV Footage Review form to support this permission.
- 5.3 Other operational functions will include maintaining recorded materials and hard disk space, filing and maintaining occurrence and systems maintenance logs.

## **6. Liaison**

- 6.1 Liaison meetings will be held, as required, with all staff involved in the support of the Systems.

## **7. Monitoring procedures**

- 7.1 Pictures will be continuously recorded or when activated by movement.
- 7.2 If covert surveillance is planned, this must be authorised in accordance with paragraph 3.4.2.

## **8. Recorded material procedures**

- 8.1 In order to maintain and preserve the integrity of the recorded material used to record events from the hard drive, and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:
  - (i) each item of recorded material must be identified by a unique mark
  - (ii) before use, each item on which images will be recorded must be cleaned of any previous recording
  - (iii) the person making the recording shall register the date and time of recorded material, including a recorded material reference
  - (iv) any recorded material required for evidential purposes must be sealed, witnessed, signed by The Controller, dated and stored in a separate, secure recorded material store. If recorded material 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 Controller, dated and returned to the evidence material store.
- 8.2 Recorded materials may be viewed by the Police for the prevention and detection of crime.

- 8.3 A record will be maintained of the release of recorded materials to the Police or other authorised applicants. A register will be available for this purpose.
- 8.4 Viewing of recorded materials by the Police must be recorded in writing and logged. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998 as amended.
- 8.5 Should a recorded material be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (iv) of this Policy. Recorded materials will only be released to the Police on the clear understanding that the recorded material remains the property of WS, and both the recorded material and information contained in it are to be treated in accordance with this Policy. WS also retains the right to refuse permission for the Police to pass to any other person the recorded material or any part of the information contained thereon. On occasions when a Court requires the release of an original recorded material, this will be produced from the secure recorded material store, complete in its sealed bag.
- 8.6 The Police may require WS to retain the stored, recorded materials for possible use as evidence in the future. Such recorded materials will be properly indexed and properly and securely stored until they are needed by the Police.
- 8.7 Applications received from outside bodies (eg, solicitors) to view or release recorded materials will be referred to the Head of School (or Acting Head of School/Deputy). In these circumstances, recorded materials will normally be released where satisfactory documentary evidence is produced, supporting 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 WS staff will be initially investigated by the Head of School (or Acting Head of School/Deputy), in order for them 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 an 'Operator' (see section 2.1.2 above).

## **11. Complaints**

- 11.1.1 Any complaints about the Systems should be addressed to the Head of School

11.2 Complaints will be investigated in accordance with paragraph 9 of this Policy.

## **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 in writing to the Head of School.

## **13. Public information**

Copies of this Policy will be available from Whitby School Office and it will also be accessible from the school website.