

TCS CCTV Policy

Policy responsible: IT Manager

Approved by: Headteacher

Statutory/Discretionary: Discretionary

Review cycle: Annual

Last reviewed: October 2019

Contents

Introduction

1. *The CCTV system comprises of the following*
 2. *Objectives of the CCTV scheme*
 3. *Statement of intent*
 4. *Operation of the system*
 5. *Day-to-day Management*
 6. *Liaison*
 7. *Monitoring procedures*
 8. *Image capture procedures*
 9. *Breaches of the code (including breaches of security)*
 10. *Assessment of the scheme and code of practice*
 11. *Complaints*
 12. *Public information*
 13. *Summary of Key Points*
-

Introduction

To purpose of this policy is: -

- To enhance the security and safety of all site users and the structure and contents of the buildings.
- To regulate the management, operation and use of the closed-circuit television (CCTV) system at Testbourne Community School, hereafter referred to as 'the school'.

1. The CCTV system comprises of the following:-

1.1 The system comprises several fixed and dome cameras located around the school site. Camera data is stored centrally and only available to selected senior staff, selected Pastoral staff, IT Manager and Site Services.

1.2 This Code follows Data Protection Act and General Data Protection Regulation (GDPR) guidelines.

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

1.4 The CCTV system is owned by the school

2. Objectives of the CCTV scheme

2.1

- (a) To protect the school buildings and their assets
- (b) To increase personal safety and reduce the fear of crime
- (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 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 2018 and GDPR and will seek to comply with the requirements both 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 **and antisocial** activity occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school, together with its visitors.

3.4 To use images to reduce bullying and vandalism where considered appropriate.

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

3.6 Unless an immediate response to events is required, staff must not direct cameras at individuals, their property or a specific group of individuals, without an authorisation being obtained using the appropriate means as set out in the Regulation of Investigatory Power Act 2000.

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

3.8 Planning and design of the system 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.

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

4. Operation of the system

4.1 The Scheme 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 both the Senior Leadership Team, select Pastoral staff and Site Services during the day and Site Services out of hours and at weekends.

4.3 The technical management will be undertaken by the IT Manager, working with the Site Manager. The IT Manager or the Site Manager may choose to delegate maintenance to a suitable third party but will ensure the contents of this policy are adhered to.

4.4 The CCTV system will be operated 24 hours each day, every day of the year. CCTV footage will be stored for a minimum of 30 days and no longer than 90 days, subject to storage availability.

5. Day-to-day Management

5.1 Site Services will check and confirm the efficiency of the system daily and that the equipment is properly recording and that cameras are functional.

5.2 Access to the CCTV system will be strictly limited to the Senior Leadership Team, selected Pastoral staff, Site Services and the IT Manager.

5.3 CCTV footage is not reviewed regularly. However, spot checks may be undertaken to ensure the efficiency and functionality of the system.

5.4 Unless an immediate response to events is required, staff must not direct cameras (through use of zoom or motorised camera mount – where this exists) at an individual or a specific group of individuals.

5.5 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual access to CCTV data will not be permitted. Any third parties requesting to view CCTV footage must first obtain permission from the Headteacher or Site Manager and must be supervised during this time.

5.6 If out of hours emergency maintenance arises, the system operators must be satisfied of the identity and purpose of contractors before allowing access.

5.7 CCTV data will be stored on a Network Video Recorder (NVR) which operates alongside the rest of the school's IT systems. Day-to-day management of this NVR will be undertaken by the IT Manager.

5.8 Physical access to this NVR is restricted to authorised staff only and the server room is always kept locked.

5.9 Other administrative functions will include maintaining video/images stored, hard disk space, filing and maintaining occurrence and system maintenance logs.

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

6. Liaison

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

7. Monitoring procedures

7.1 Camera surveillance may always be maintained.

7.2 If covert surveillance is planned or has taken place copies of the Authorisation Forms, including any Review, or Cancellation must be returned to the Corporate Monitoring Officer, Hampshire County Council, Chief Executive's Department, Elizabeth II Court, The Castle, Winchester, Hampshire. SO23 8UJ.

The corporate policy and procedures can be obtained from Hampshire County Council

8. Image capture procedures

8.1 Stored images may be viewed by the Police for the prevention and detection of crime, authorised officers of Hampshire County Council for supervisory purposes, authorised demonstration and training.

8.2 A record will be maintained of the release of stored images to the Police or other authorised applicants. A register will be available for this purpose.

8.3 Viewing of stored images 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 2018.

8.4 Should a digital copy be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (iv) of this Code. Stored images will only be released to the Police on the clear understanding that the data remains the property of the school, and that the data is 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 data or any part of the information contained therein. On occasions when a Court requires the release of the original hard drive this will be produced and placed in a sealed evidence bag.

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

8.6 Applications received from outside bodies (e.g. solicitors) to view or release stored images will be referred to the Headteacher. In these circumstances stored images will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, or in response to a Court Order.

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, for him/her 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

Performance monitoring, including random operating checks, may be carried out by the Site Manager at any time.

11. Complaints

11.1 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. Public information

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

13. Summary of Key Points

- This Code of Practice will be reviewed annually.
- The CCTV system is owned and operated by the school.
- The CCTV system will be operational 24 hours a day, every day of the year.
- Access to CCTV data is not available to visitors except by prior arrangement and with good reason.
- Liaison meetings may be held with the Police and other bodies.

- Recording stored images will be used properly indexed, stored and destroyed after appropriate use.
- Stored images may only be viewed by Authorised School Officers, and the Police.
- Stored images required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Stored images will not be made available to the media for commercial or entertainment.
- Stored images will be disposed of securely.
- Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with the corporate policies and procedures. Schools must use these procedures and comply with the requirements set out in the procedure documentation available from Hampshire County Council
- Contact the school's Data Protection Officer if you require more information.
- 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.

Change History

Date	Author	Version	Details
14/09/2016	J Worth	0.1	Initial Draft
10/10/2016	J Worth	0.1.1	Updated Corporate Policies URL
11/10/2016	J Worth	0.2	Minor changes and specification of how long footage is stored for
03/11/2016	J Worth	0.3	5.3 added. 12.2 revised.
15/11/2016	J Worth	1.0	Ratification by Governors
12/04/2019	J Worth	1.1	2019 Annual Review. Updated DPA1998 to 2018 and GDPR
14/10/2019	J Worth	1.1.1	Revise 4.4