CCTV Policy

Date approved: 8th February 2019

Review cycle/date: Every 3 years

Party responsible: Finance & Premises Committee

PURPOSE OF POLICY

At The Swanage School we take great pride in the behaviour of our staff and students and our ethos of relationships being at the heart of the school. We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff, students and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy and as such this policy is intended to address such concerns.

The 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 use of CCTV and its associated technology in the monitoring of both the internal and external environments of the premises under the remit of The Swanage School, hereafter referred to as 'the school'.

1. **The CCTV system comprises of the following: -**

1.1 The system comprises of a number of cameras located internally and externally around the school site. Camera data is stored centrally and only available to the Site Manager, the IT Manager and members of the Senior Leadership Team. Access by other parties is controlled by the Senior Leadership Team or Site Manager.

1.2 The CCTV system is owned by the school.

2. **Scope**

2.1 This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. Where classes and activities are carried out in rented premises, the Swanage School will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this policy.

2.2 This policy covers all employees, workers, contractors, agency workers, consultants, directors, members, governors, trustees, past or present students and will also be relevant to visiting members of the public.

3. Objectives of the CCTV policy

The two main objectives of CCTV at the school are to act as a deterrent and where appropriate to be used to investigate events that occur within the school grounds. These objectives will help to achieve the following:

- Protect the school buildings and assets
- Increase personal safety for students, staff and visitors and deter incidents of crime and anti-social behaviour (including theft and vandalism)
- 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
- Assist in managing the school
- Deter bullying

4. Statement of intent

4.1 The CCTV system will be registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

4.2 The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

4.3 Cameras will be used to record activities within the school and its car park and other public areas to identify criminal and antisocial activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school, together with its visitors.

4.4 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.

4.5 The system will not cover or detect every single incident taking place in the areas of coverage.

4.6 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.

5. Operation of the system

5.1 The CCTV system will be operational 24 hours a day, every day of the year.

5.2 The system will be administered and managed in accordance with the principles and objectives expressed in this policy.

5.3 The day-to-day management will be the responsibility of both the Senior Leadership Team and the Site Manager.

5.4 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.

6. Storage and Retention

6.1 Section 2(1)(c)(iv) of the Data Protection Acts states that data "*shall not be kept for longer than is necessary for*" the purposes for which it was obtained. CCTV footage will be stored for a minimum of 30 days subject to storage availability, after which they are automatically deleted except where the images identify an issue such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

7. Day-to-day Management

7.1 The Site Manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

7.2 Access to the CCTV system will be strictly limited to the Senior Leadership Team, the Site Manager and the IT Manager (where appropriate).

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

7.4 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.

7.5 It is vital that operations are managed with the minimum of disruption. Casual access to CCTV data will not be permitted. Any other staff, Governors or third parties requesting to view CCTV footage must first obtain permission from a member of the Senior Leadership Team or Site Manager and must be supervised during this time.

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

7.7 CCTV data will be stored on a dedicated server which operates alongside the rest of the school's IT systems. Day-to-day management of this server will be undertaken by the IT Manager.

7.8 Physical access to this server is restricted to authorised staff only and the server room is kept locked at all times.

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

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

8. Liaison

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

9. Covert surveillance

9.1 The Swanage School will not engage in covert surveillance.

9.2 The only exception is a Police request to carry out covert surveillance on school premises (such covert surveillance may require the consent of a judge). Accordingly, any such request made by the Police will be requested in writing and the school will seek legal advice.

10. Safeguarding

10.1 If there is a need for images to be viewed by authorised personnel then no individual may view the footage alone. Any review of footage will be facilitated by two authorised members of staff.

11. Viewing by and release of stored images to outside bodies

11.1 Stored images may be viewed by the Police for the prevention and detection of crime.

11.2 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.

11.3 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.

11.4 Should a digital copy be required as evidence, a copy may be released to the Police under the procedures described in paragraph 9.2 of this policy. 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 policy. 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.

11.5 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.

11.6 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, a subject access request, or in response to a Court Order.

12. **Breaches of the CCTV policy (including breaches of security)**

12.1 Any breach of this policy by school staff will be initially investigated by the Headteacher, in order for him/her to take the appropriate disciplinary action.

12.2 Any serious breach of this policy will be reported to the Chair of Governors, and an investigation carried out to make recommendations on how to remedy the breach.

13. **Complaints**

13.1 Any complaints about the school's CCTV system should be addressed to the Headteacher.

14. **Access by the Data Subject**

14.1 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.

14.2 Subject Access Requests (SARs) should be made by letter addressed to the school's Data Protection Officer.

15. **Public information**

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

16. **Summary of Key Points**

- This policy will be reviewed every three years.
- 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.
- Recordings and stored images will be properly indexed, stored and securely destroyed after appropriate use.
- Stored images may only be viewed by the Senior Leadership Team, Site Manager, IT Manager, the Police, and staff, Governors and third parties authorised by the Senior Leadership Team.
- 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 purposes.
- Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with the with policy.

- Breaches of the policy and remedies will be reported to the Headteacher.
- Any breaches of this policy will be investigated by the Headteacher. Serious breaches will be handled in accordance with the school disciplinary or other relevant policy and reported to the Chair of Governors.
- Contact the school's Data Protection Officer if you require more information.

Arrangements for monitoring and evaluation

The Finance & Premises Committee will monitor the impact of this policy at least annually by receiving and reviewing reports of:

- The number and type of incidents which have been investigated using images recorded the CCTV system
- The number of breaches of the CCTV policy reported to the Headteacher
- The number of complaints made to the Headteacher about the CCTV system