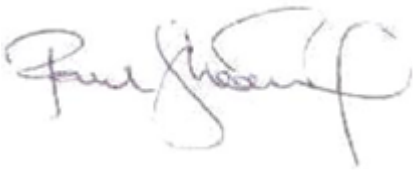
WATFORD GRAMMAR SCHOOL FOR BOYS

CCTV POLICY

Headmaster's signature 12/9/17

Chair of Governors' signature 12/9/17



POLICY FOR CLOSED CIRCUIT TELEVISION CAMERA SECURITY (CCTV)SYSTEM

1. INTRODUCTION

1.1. The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at Watford Grammar School for Boys, hereafter referred to as 'the school'.

1.2. The system comprises a number of fixed, dome and PTZ (pan-tilt-zoom) cameras located in and around the school site. All cameras are monitored from the Server or the computers of the Site Manager or the IT Manager and images are only available to SLT.

1.3. This Policy follows Data Protection Act guidelines.

1.4. The School Policy will be subject to review bi-annually to include consultation as appropriate with interested parties.

1.5. The CCTV system is owned by the school.

2. OBJECTIVES OF THE CCTV SYSTEM

2.1. To protect pupils, staff and visitors.

2.2. To increase personal safety and reduce the fear of crime.

2.3. To protect the school buildings and assets.

2.4. Without prejudice, to protect the personal property of pupils, staff and visitors.

2.5. To support the police in preventing and detecting crime.

2.6. To assist in identifying, apprehending and prosecuting offenders.

2.7. To assist in managing the school.

3. STATEMENT OF INTENT

3.1. The CCTV system will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

3.2. The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under 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 activity actually occurring, anticipated, or perceived. It will be used for the purpose of securing the safety and wellbeing of the pupils, staff and school together with its visitors.

3.3.1. The system has been designed to deny observation on adjacent private homes, gardens and other areas of private property.

3.4. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

3.4.1. Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police.

3.4.2. Images will never be released to the media for purposes of entertainment.

3.5. The planning and design 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.

3.6. Warning signs have been placed at strategic places around the site.

4. SYSTEM MANAGEMENT

4.1. The system will be administered and managed by the Site Manager in accordance with the principles and objectives expressed in the policy.

4.2. The day-to-day management will be the responsibility of both the Site Manager and the IT Manager.

4.3. The system and the data collected will only be available to the SLT on request, the Site Manager and the IT Manager.

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

4.5. The IT 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.

4.6. Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

4.7. Control operators must satisfy themselves of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists access will be refused.

4.8. Details of **ALL** visits and visitors will be recorded in the system log book including time/data of access and details of images viewed.

4.9. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

4.10. If out of hours emergency maintenance arises, the Control operators must be satisfied as to the identity and purpose of contractors before allowing access.

4.11. When not manned the facility must be kept secured.

5. LIAISON

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

6. DOWNLOAD MEDIA PROCEDURES

6.1. In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures: -

6.1.1. Each download media must be identified by a unique mark.

6.1.2. Before use, each download media must be cleaned of any previous recording.

6.1.3. The Site Manager or IT Manager will register the date and time of download media insertion, including its reference.

6.1.4. Download media required for evidential purposes must be sealed, witnessed and signed by either the Site Manager or the IT Manager, then dated and stored in a separate secure evidence store. If a download media 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 and signed by the Site Manager or the IT Manager, then dated and returned to the evidence store.

6.1.5. If download media is archived the reference must be noted.

6.2. Images may be viewed by the police for the prevention and detection of crime.

6.3. A record will be maintained of the release of any download media to the police or other authorised applicants.

6.4. Viewing of images by the police must be recorded in writing and in the log book.

6.5. Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that

the download media (and any images contained thereon) remains the property of the school, and download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

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

6.7. Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the Headmaster. In these circumstances, 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.

7. ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

7.1. Performance monitoring, including random operating checks, may be carried out by the Headmaster or another member of SLT.

8. BREACHES (including breaches of security)

8.1 Any breach of the Code of Practice by school staff will be initially investigated by the Headmaster, in order for him to take the appropriate disciplinary action.

8.2 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.

9. COMPLAINTS

9.1. Any complaints in relation to the school's CCTV system should be addressed to the Headmaster.

9.2. Complaints will be investigated in accordance with Section 8 above.

10. ACCESS BY THE DATA SUBJECT

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.

10.1. Requests for Data Subject Access should be made in writing to the Headmaster.

11. PUBLIC INFORMATION

11.1. Copies of this policy will be available to the public from the school office and the Headmaster.

12. SUMMARY OF KEY POINTS

12.1. This Policy will be reviewed every two years.

12.2. The CCTV system is owned and operated by Watford Grammar School for Boys.

12.3. The CCTV system and images are not available to visitors except under circumstances as outlined in this policy.

12.4. Liaison meetings may be held with the police and other bodies if required.

12.5. Downloaded media will be used properly indexed, stored and destroyed after appropriate use, in accordance with the Data Protection Act.

12.6. Images may only be viewed by authorised School officers and the police.

12.7. Downloaded media required as evidence will be properly recorded witnessed and packaged before copies are released to the police.

12.8. Downloaded media will not be made available to the media for commercial or entertainment purposes.

12.9. Any breaches of the Code will be investigated by the Headmaster. An independent investigation will be carried out for serious breaches.

12.10. Any breaches of the Code and remedies will be reported to the Headmaster.