

Horley Town Council

Closed Circuit Television (CCTV) Policy and Code of Practice

1. CCTV POLICY

- 1.1. The purpose of this policy is to regulate the management and use of the closed circuit television (CCTV) systems operated by Horley Town Council.
- 1.2. All cameras are monitored from the Town Council Offices which are streamed wirelessly from separate control units held at each secure location.
- 1.3. This CCTV scheme and policy is operated within the Information Commissioner's Code of Practice for CCTV 2008 and Surveillance Camera Code of Practice 2013 published by the Home Office.
- 1.4. This policy will be subject to annual review, which will include a review in respect of the effectiveness and necessity of the system.
- 1.5. The CCTV systems are owned wholly by the Town Council.

2. OBJECTIVES OF THE CCTV SCHEME

Along with a range of measures, the CCTV system will be used to:

- reduce the fear of crime
- deter crime and criminality
- aid the detection of crime and the prosecution of offenders
- reduce instances of nuisance and vandalism
- promote a sense of safety to park users
- provide safety and security to all vulnerable members of the community

3. STATEMENT OF INTENT

- 3.1. The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements of the Data Protection Act and the Commissioner's Code of Practice, as well as the Surveillance Camera Code of Practice 2013 published by the Home Office.
- 3.2. Horley Town Council will treat as data all CCTV recordings and relevant information.
- 3.3. Cameras will be used to monitor activities within the Council and its recreation grounds in line with the objectives of the scheme.
- 3.4. Static cameras are set as to not focus on private homes, gardens and other areas of private property.
- 3.5. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained in writing for directed surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

- 3.6. Materials or knowledge secured as a result of CCTV will not be released to the media, or used for any commercial purpose, or for the purpose of entertainment. Recordings will only be released under the written authority from the Police, or in respect of a subject access request.
- 3.7. The planning and design has endeavoured to ensure that the scheme will give maximum effectiveness and efficiency. It is not possible, however, to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.
- 3.8. 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 Council's CCTV.

4. OPERATION OF THE SYSTEM

- 4.1. The system will be administered by the Town Clerk and other Council staff, in accordance with the principles and objectives expressed in the code.
- 4.2. The CCTV system will be in operation 24 hours each day, for every day of the year.
- 4.3. Systems will be checked on a daily basis to ensure that the system is operating effectively and in particular that the equipment is properly recording and that cameras are functional. The system will be regularly serviced and maintained. Defects will be reported to the servicing company at the earliest convenient opportunity.

5. CONTROL OF SOFTWARE & ACCESS TO THE SYSTEM

- 5.1. Access to the CCTV software will be strictly limited to authorised operators with a password.
- 5.2. Operators must satisfy themselves that all persons viewing CCTV material will have a right to do so.
- 5.3. The main control facilities must be kept secure.
- 5.4. Other administrative functions will include controlling and maintaining downloaded digital materials, and maintenance and system access logs.

6. MONITORING PROCEDURES

- 6.1. Images from these cameras are to be shared with Surrey Police by allowing access through the existing police run CCTV control room at Reigate Police Station. Access to monitors must be restricted to staff where those areas being monitored are not in public view.
- 6.2. If covert surveillance is planned or has taken place, copies of the Authorisation Forms, including any Review, must be completed and retained.

7. DIGITAL IMAGES: PROCEDURES

- 7.1. Live and recorded materials may be viewed by authorised operators investigating an incident.
- 7.2. Recorded material may be downloaded from the system in line with the objectives of the scheme.
- 7.3. Images (stills and footage) may be viewed by the Police for the detection of crime.
- 7.4. A record will be maintained of the release of images to the Police or other authorised applicants. A register will be available for this purpose.
- 7.5. Viewing of images by the Police must be recorded in writing and in the log book. Requests by the Police are allowable under section 29 of the Data Protection Act (DPA) 1998.
- 7.6. Should images be required as evidence, a digital copy may be released to the Police.
- 7.7. The Police may require the Council to retain images for possible use as evidence in the future. Such images will be securely stored until they are needed by the Police.
- 7.8. Applications received from outside bodies to view or release images will be referred to the Town Clerk. 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. A fee may be charged appropriate for subject access requests.
- 7.9. Retention: Images will be retained for only as long as these are required. The system will automatically delete all recordings held on the main control unit after approximately one month.

8. BREACHES OF THE CODE (including breaches of security)

Any breach of the CCTV Code of Practice will be investigated by the Town Clerk, in order for him/her to take any appropriate disciplinary action

9. COMPLAINTS

Any complaints about the CCTV system should be addressed to the Town Clerk

10. SUBJECT ACCESS AND FREEDOM OF INFORMATION

- 10.1. The Data Protection Act (DPA) provides Data Subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV
- 10.2. Requests for Data Subject Access should be made in writing to the Town Clerk
- 10.3. A request for Subject Access will be charged at £10, which is the maximum allowable under the DPA
- 10.4. A request under the Freedom of Information Act 2000 will be accepted, where such a request is appropriate

CCTV Code of Practice

1. Introduction and Accountability

The Horley Town Council has a comprehensive closed circuit television (CCTV) surveillance system for the purpose of the prevention and detection of crime and the safety and welfare of staff, and park users.

The system is owned by Horley Town Council and images from the system are strictly controlled and monitored by authorised personnel.

This policy has been prepared from the standards set out in the Information Commissioner's CCTV Code of Practice 2008 and the Surveillance Camera Code of Practice 2013 published by the Home Office. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff and visitors to the Council Offices and its Recreation Grounds and to ensure that its operation is consistent with the obligations on the Town Council imposed by the Data Protection Act 1998.

In line with the Home Office 12-point code of conduct the use of the system will:

- always be for the purpose specified which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
- take into account its effect on individuals and their privacy
- have as much transparency as possible, including a published contact point for access to information and complaints
- have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
- have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them
- have no more images and information stored than that which is strictly required
- restrict access to retained images and information with clear rules on who can gain access
- consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
- be subject to appropriate security measures to safeguard against unauthorised access and use
- have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with
- be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in pursuit of a legitimate aim
- be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes

2. Operation

The Town Clerk is responsible for the operation of the CCTV system and for ensuring compliance with this policy. Any concerns in respect of the system's use or regarding compliance with this policy should be addressed to the Town Clerk.

3. Location

This code of conduct applies to all CCTV systems operated by the Town Council. Currently CCTV is present at the Council Offices, Horley Recreation Ground, Court Lodge Playing Fields including the Innes Pavilion and Michael Crescent Centenary Park. It will also encompass all other CCTV images that, in due course, are added to the system.

The system is operational and images are capable of being monitored for 24 hours a day throughout the whole year.

Images captured on camera will be recorded on the main CCTV servers which are held in secure locations. Although every effort has been made in the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

For the purposes of the Data Protection Act 1998, the Data Controller is The Horley Town Council and the Council is legally responsible for the management and maintenance of the CCTV system.

No unauthorised access to the system is allowed at any time. Normal access is strictly limited to authorised staff only. Surrey Police will monitor cameras from Reigate Police Station under a separate Memorandum of Understanding.

In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to access the CCTV system.

Before granting access to the CCTV system, controllers must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include their name, department or the organisation they represent, the person who granted authorisation for their visit (if applicable) and the start and finish times of their access to the CCTV system.

It is recognised that the images obtained comprise personal data and are subject to the law on Data Protection. All copies will be handled in accordance with the procedures.

Recorded images will only be reviewed with the authority of the Town Clerk. Copies of digital images will only be made for the purposes of crime detection, evidence in relation to matters affecting safety, evidence for prosecutions, or where otherwise required by law.

All staff involved in the operation of the CCTV system will, by training and access to this Policy, be made aware of the sensitivity of handling CCTV images and recordings.

The Town Clerk will ensure that all staff are fully briefed and trained in respect of all functions; operational and administrative, arising within the CCTV control operation. Training in the requirements of the Data Protection Act and this policy will also be provided.

4. Recordings

The system is supported by digital recording facilities which will function throughout operations in real time. As the images are recorded digitally, the process of identifying retrieval dates and times will be computerised. Images will be cleared automatically after a set time.

Unless required for evidential purposes or for the investigation of crime, recorded images will be retained for no longer than 30 days from the date of recording. However, the Town Council recognises that, in accordance with the requirements of the Data Protection Act, no images should be retained for longer than is necessary. Accordingly, some recorded images may be erased after a shorter period, for example where it can be determined more quickly that there has been no incident giving rise to the need to retain the recorded images. Digital images will be automatically erased after a set period, which will be no longer than 30 days.

In the event of the digitally recorded image being required for evidence or the investigation of crime it will be retained for a period of time until it is no longer required for evidential purposes or any investigation into a crime has been completed.

5. Digital Recording and Access Procedures

All disks containing images to remain the property of the Town Council.

Requests by persons for viewing or copying of disks or obtaining digital recordings will be usually be made by prior authority of the Police.

Requests from the Police will arise in a number of ways, including:

- requests for a review of recordings in order to trace incidents that have been reported
- immediate action relating to live incidents, eg immediate pursuit
- for major incidents that occur when images may have been recorded continuously
- individual Police Officers seeking to review recorded images

It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes. Users of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images. These aspects of the policy reflect the Second and Seventh Data Protection Principles of the Data Protection Act 1998.

All requests for access or disclosure will be recorded. The Town Clerk will make decisions on access to recorded images by persons other than Police Officers. Requests by the Police for access to images will not normally be denied and can be made without the above authority, provided they are accompanied by a written request signed by a Police Officer who must indicate that the images are required for the purposes of a specific crime enquiry.

If access or disclosure is denied, the reasons will be documented.

If access to or disclosure of the images is allowed then the following will be documented:

- the date and time at which access was allowed or the date on which disclosure was made
- the reason for allowing access or disclosure
- the extent of the information to which access was allowed or which was disclosed

Appropriate forms will be used to document routine disclosure to the Police.

6. Photographs and hard copy prints

Photographs and hard copy prints taken from digital images are subject to the same controls and principles of Data Protection as other data collected. They will be treated in the same way as digital images.

At the end of their useful life all computer disks, still photographs and hard copy prints will be disposed of as confidential waste.

This code of practice will be reviewed annually to assess its implementation and effectiveness and it will be promoted and implemented throughout the Academy.

This Policy and Code of Practice was recommended by the F&GP Committee on 17 January 2017 and approved by Full Council on 7 February 2017.

It is subject to annual review