TRINITY COLLEGE
CAMBRIDGE CB2 1TQ

Code of Practice for CCTV

in

Trinity College

June 2013

1. Introduction

The aim of this Code of Practice is to ensure that members of the College and College staff, particularly those members of the College staff involved in running the CCTV system, understand the principles which govern the operation of CCTV cameras in the College and how they will be used.

The purpose of CCTV cameras within the College is to address the needs to improve security, to provide additional protection for all members of College and staff who live and work at Trinity College and to deter and detect crime. (See further below)

The day-to-day management, maintenance and security of the CCTV systems within College will be the responsibility of the following Responsible Officers, under the overall direction of the Junior Bursar:

Head Porter
Deputy Head Porter
College Porters

The Junior Bursar, with assistance from the Head Porter, will be responsible for:

- ensuring that all Responsible Officers and any other staff who either manage or use the CCTV systems or use or process the images and information obtained have the necessary skills and knowledge; and
- reviewing, from time to time, the system and its operation, including the siting of cameras, the purposes of the system and its effectiveness in meeting those purposes.

2. Legislation

CCTV operations are subject to legislation, including the Acts referred to below.

It is important that the operation of all College run CCTV systems complies with these Acts and the guidelines contained within this Code of Practice.

When clarification is required, the Junior Bursar will contact the College's Solicitors for advice and guidance. The College's Solicitors should be contacted in all cases when a RIPA request is received.

2.1 The Data Protection Act 1998 (DPA)

All Cambridge City Colleges' CCTV systems are registered under the Data Protection Act: all enquiries regarding Data Protection should be directed to the Junior Bursar on (01223) 338400.

Data Protection principles must be observed by all staff involved with the CCTV systems and the data collected. See the College's Data Protection Policy

2.2 The Human Rights Act 1998 (HRA}.

2.3 The Freedom of Information Act 2000 (FOIA}.

2.4 The Regulation of Investigatory Powers Act 2000 (RIPA}.

It will be rare for small building CCTV systems to be required to respond to requests for assistance under RIPA.

3. Purpose Statement

It is important that all staff, and particularly those charged with operating the system understand exactly why the system has been introduced and what it will and will not be used for.

The key objectives of the CCTV cameras within College are:

To enhance premises security.

To protect members of College and staff in areas used by the public.

To deter and detect crime.

To assist in the identification of offenders leading to their arrest and successful prosecution.

To discourage aggressive or violent behavior towards members of College and staff.

To reduce members of College and staff's fear of crime or aggressive behavior.

To provide evidence in cases of alleged disciplinary offences by members of staff (see section 9). But the system will not be used to monitor flexi time or absences.

4. Privacy

The College respects and supports an individual's entitlement to go about their lawful business and their right to a private life. These are primary considerations in the operation of the system.

Although there is inevitably some loss of privacy when CCTV cameras are installed, cameras will not be used to monitor individuals in the ordinary course of lawful use of the area under surveillance.

Individuals will only be continuously monitored if there is reasonable cause to suspect an offence has been, or may be, about to be committed.

5. Cameras

Most cameras are sited so that they are clearly visible and publicity will normally be given to the system by clear signing. This will ensure that both the maximum deterrent value is achieved and that the public, members of the College, visitors and staff are clearly aware when they are in a monitored area.

However, concealed and unsigned cameras may be used in areas of high security where there is no legitimate public access and only limited/restricted/controlled staff access. Where concealed cameras are used in areas other than these, College staff who normally work in those areas or others who can be identified as likely to make substantial use of the area will normally be informed of the location of the cameras and of the position of the monitors. Where there is a pressing need, a concealed and unsigned camera may be installed but it will only remain concealed and unsigned while the need is a pressing one.

The College will sometimes utilise non-functioning or "dummy cameras" to increase the deterrence value of the College's CCTV system if there is specific need. The decision to use non-functioning or "dummy cameras" will be taken by the Junior Bursar.

The system does not record sound.

6. Monitoring

Monitoring of the systems will be carried out by persons authorised by the Junior Bursar in consultation with the Head Porter.

7. Digital Recording Systems and staffing

7.1 The system

The College's CCTV systems use a digital recording system.

The recording system links its cameras to a digital recording machine normally controlled through a computer. The basic features are the same as an analogue system except that it records its cameras onto a computer hard drive and all images are stored on a central server, which is maintained by the Computer Department.

Where images are required for investigatory or evidential purpose (see Section 9 below), Compact Discs are used to make copies of the images available to investigating officers instead of using traditional videotapes.

All cameras are recorded 24 hours a day.

Recording equipment will be kept in secure accommodation and no access will be granted to unauthorised staff.

7.2 Staffing

Only authorised staff may operate or manage CCTV equipment, recorded images or data. All such staff shall receive training in the use and management of the equipment and of the images and data and must conform to this Code of Practice at all times. Levels of authorized access may differ depending on the role of the staff member.

Before being allowed to access or to process the images, authorised staff will be required to sign a 'Confidentiality Statement' (see example at annex 'A'), which prohibits them from making any material available for purpose other than those stated in the Code of Practice. Any other staff having access to the equipment will also sign a confidentiality statement. Once signed, the confidentiality statement should be placed in that person's personal file.

All authorisations will be by the Junior Bursar or Head Porter.

8 Control of Images

8.1 Ownership and Copyright

All images will remain the property and copyright of Trinity College.

8.2 Viewing

Viewing of any of the recorded digital images (however they are stored) is only permitted to persons authorised to do so by the Head Porter or the Junior Bursar.

Viewing must be carried out in an area which is appropriate and secure.

Details of viewing of images (see example at annex 'B'), will be logged in a Viewing Register, which will be maintained by the Head Porter.

8.3 Use

Images must not be copied in whole or in part except for evidential and investigatory purposes in accordance with Section 9 below. Images will not be sold or used for commercial purposes or the provision of entertainment or other unauthorised use.

Images may be used in disciplinary procedures where appropriate.

8.4 Issue

Images may from time to time be released on request to the police or other enforcement or investigatory person or body (see Section 9 below). The release will be on the basis that at no time can the images be used for anything other than the purpose for which they were originally released.

8.4 Quality and accuracy

Recorded materials may need to be submitted as evidence in criminal proceedings or at internal disciplinary hearings and therefore must be of good quality, and accurate in content. All material provided as evidence will be treated in accordance with clearly defined procedures either under the Police And Criminal Evidence Act (PACE) or this Code of Practice to ensure a clear audit trail.

8.5 Retention and Deletion

Routine recordings will be retained for up to a maximum of 14 days on the CCTV server and will then be erased and over-written. The Junior Bursar or the Head Porter may change this period either generally or in specific instances where necessary.

Specific images and data may be retained on CD-Rs for the period of internal disciplinary or external investigation and proceedings. Once the specific images are no longer needed, they will be deleted in accordance with Section 9.3 below.

9 Requests to View, Release of Images and Issue of CD-R Discs for investigation and evidential purposes

9.1 Requests

Requests to view or release evidence will normally come from the police or other enforcement body or from another College department conducting an investigation into criminal or other activities or disciplinary issues.

Any requests from the police, other law enforcement body or other third party must be referred to the Head Porter or in his absence, the Deputy Head Porter.

Any viewing of images or release of evidence in response to such a request must have the prior written authorisation of the Head Porter or in his absence, the Deputy Head Porter. Requests from the police and law enforcement bodies will normally be granted but any from a third party will only be granted where the needs of the third party outweigh those of the persons whose images are recorded. In cases of doubt, the Head Porter shall consult the Junior Bursar.

If the matter concerns a member of staff, a request to view or for the release of evidence must be made to the Junior Bursar who may liaise, where appropriate, with the Head Porter or Deputy Head Porter, Head of Personnel and/or the member of staff's Head of Department.

Any subject access request must be made in writing addressed to the Junior Bursar, accompanied by a fee of £10 and providing details to enable the College to identify them as the subject of the images and also to locate the images on the system.

If a member of staff receives or becomes aware of a subject access request or

Freedom of Information request or a request relating to data protection, this must be referred immediately to the Junior Bursar.

9.2 Processing of authorised requests

Once authorised, arrangements will be made to enable the investigator to view the images, and if necessary be issued with the recorded CD-R disc or a copy of the recorded material on another CD-R disc.

A record must be made in the CCTV Register of the issue of CD-R discs to the Police or to other authorised applicants. An issue certificate, accepting responsibility for the CD-R, must be completed before it can be released to the authorised applicant (see example at annex 'D'),

When images are released under these circumstances, a copy of the released images must be held on a separate CD-R and a record made in the CCTV Register. This will ensure the completeness of the archive for the specific period.

9.3 Destruction or deletion of CD-R discs

Once the issued CD-R disc and the images on it are no longer required, then the CD-R and any copy discs must, with the prior written consent of the Junior Bursar or the Head Porter, be destroyed

A record of the destruction or deletion must be made in the CCTV Register.

9.4 CCTV Register

A CCTV Register (see Annex C) will be maintained by the Head Porter. Access to this will normally be restricted to the Head Porter or the Deputy Head Porter, although the Junior Bursar may authorize access by other members of staff if required.

10. Disciplinary Offences: Breaches of the Code of Practice

Any breach of the Code of Practice is a serious disciplinary matter.

Any breach of this Code of Practice will be dealt with according to the College's disciplinary procedures – a process which could result in the dismissal of any member of staff responsible for a breach. Serious breaches will be regarded as gross misconduct.

Tampering with cameras, monitoring or recording equipment, images or recorded data or unauthorised accessing or copying or possession of images or recorded data will be regarded as gross misconduct and will lead to disciplinary action, which may result in dismissal or criminal prosecution.
Unless the Junior Bursar decides otherwise, the Head Porter or his Deputy will, in the first instance, investigate all breaches or allegations of breaches of security and

will report his/her findings to the Junior Bursar.

11. Complaints

Any formal complaints about the operation and management of the CCTV system or the management of the images should be made in writing to the Head Porter. Formal complaints will be dealt with in accordance with the College's formal complaints procedure.

Statistical information about the number and nature of any complaints received and how they have been resolved will be kept.