Code of practice 4 – CCTV

1. Introduction

The use of CCTV systems across the sites of HE institutions to ensure site security and personal safety has become common practice. As a user of such systems the College has to comply with the provisions of the Data Protection Act 1998. Compliance with this Code of Practice, notably with those standards that are directly based on the Data Protection Principles and the Act, will aid the users of CCTV systems and similar surveillance equipment in meeting their legal obligations.

2. Initial assessment procedures

Before installing and using CCTV and similar surveillance equipment or, retrospectively for systems already in operation, users will need to establish the purpose or purposes for which they intend to use the equipment, as the First Data Protection Principle requires Data Controllers to have a legitimate basis for processing personal data, in this case images of individuals. Hence the following procedures should be carried out:

1. Assess the appropriateness of, and reasons for, using CCTV or similar surveillance equipment and document this process.
2. Establish the purpose of the scheme.
3. Establish the person or persons responsible for ensuring the day-to-day compliance with this Code of Practice.
4. Establish the associated security and disclosure policies.
5. Obtain the approval of the College Data Controller or his/her nominee for this activity.

3. Siting the cameras

It is essential that the location of the equipment is carefully considered, because the way in which images are captured will need to comply with the First Data Protection Principle. The following standards should be met:

1. The equipment should be sited in such a way that it monitors only those spaces which are intended to be covered by the scheme.
2. The user should consult with owners of adjacent spaces if images from those spaces might be recorded.
3. Operators must be aware of the purpose(s) for which the scheme has been established.
4. Operators must be aware that they are permitted to use the equipment only to achieve that purpose for which it has been installed.
5. If cameras are adjustable by the operators, this should be restricted so that operators cannot adjust them to overlook spaces which are not intended to be covered by the scheme.
6. If it is not possible physically to restrict the equipment to recording images from those spaces intended to be covered by the scheme, then operators should be trained in recognising the privacy implications of such spaces being covered.

7. Signs should be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment.

8. The signs should be clearly visible to members of the public.

9. The signs should be of an appropriate size.

10. The signs should contain the following information:
   a. the identity of the person or organisation responsible for the scheme,
   b. the purposes of the scheme,
   c. details of who to contact regarding the scheme.

11. Where covert surveillance is carried out to obtain evidence of a specifically identified criminal activity and the use of signs would prejudice the success of obtaining such evidence, they need not be displayed, but the information so obtained must only be for the prevention or detection of criminal activity and should not be retained for any other purpose.

12. When the purpose of a particular surveillance operation has ceased that surveillance must be discontinued.

4. Quality of the images

   It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. The following standards should therefore be observed:

1. Carry out an initial check on installation to ensure that the equipment performs properly.

2. Ensure that, where tapes are used they are of good quality.

3. Images should be retained for no longer than 30 days.

4. Media should not continue to be used once it becomes clear that the quality of the images has begun to deteriorate.

5. If the system records features such as the location of the camera and/or the date and time reference, these should be accurate and there should be a documented system for ensuring their accuracy; where the date and time are not recorded automatically this must be done manually.

6. Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established.

7. Users should assess whether it is necessary to carry out real time recording, or whether the activity or activities about which they are concerned occur at specific times.

8. Cameras should be properly maintained and serviced to ensure that clear images are recorded and a maintenance log kept.

9. Cameras should be protected from vandalism in order to ensure that they remain in working order.
10. If a camera is damaged there should be clear procedures for defining the person responsible for getting it repaired and for ensuring that the camera is fixed within a specific time period.

5. Processing the images

To maintain the integrity of the images and to protect the rights of the individual, the following standards should be maintained:

1. Monitors displaying images from areas in which individuals would have an expectancy of privacy should not be viewed by anyone other than the staff authorised to use the equipment.
2. Access to recorded images should be restricted to the person responsible for managing the scheme (the Data Owner) or his/her nominee who will decide whether to allow requests for access by third parties in accordance with the College's documented disclosure policies (i.e. in its Data Protection notification to the ODPC).
3. Viewing of recorded images should take place in a restricted area to which other staff do not have access.
4. Removal of the medium for the viewing of recorded images within the College should be documented to record the person removing the images, the person viewing them, the reason for viewing, the outcome, if any, of the viewing and the date and time the images were returned to the system.
5. All operators and other employees with access to images should be made aware of the procedures to be followed when accessing recorded images.
6. All operators should be trained in their responsibilities under this Code of Practice and they should be aware of the security and disclosure policies pertaining to the scheme and the rights of individuals in relation to their recorded images.
7. Where images are retained, it is essential that their integrity be maintained, whether to ensure their evidential value or to protect the rights of the people whose images may have been recorded.
8. Images should not be retained for longer than is necessary; once the retention period has expired, the images should be removed or erased.
9. If the images are retained for evidential purposes, they should be kept in a secure place to which access is controlled.
10. On removing the medium on which images have been recorded for use in legal proceedings, the operator should ensure that s/he has documented the date on which the images were removed from the general system for such use, the reason for doing so, any crime incident number to which the images may be relevant, the new location of the images and the signature of the person collecting the images.
6. Access to and disclosure of images to third parties

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of the individual are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Staff should maintain the following standards:

1. Access to recorded images should be restricted to those staff who need to have access in order to achieve the purpose(s) of using the recording equipment.
2. All access to the medium on which images are recorded should be documented.
3. Disclosure of recorded images to third parties, whether members of the College or not, should only be made in limited and prescribed circumstances.
4. All requests for access or for disclosure should be recorded and, if access is denied, the reason should be documented.
5. If access to or disclosure of images is allowed, then the following should be recorded:
   a. the date and time access was allowed or disclosure made.
   b. the identification of any third party who was allowed access or to whom disclosure was made.
   c. the reason for allowing access or disclosure.
   d. the extent of the information to which access was allowed or which was disclosed.

6. Access to and disclosure of images to third parties

The Data Protection Act 1998 gives data subjects rights to access any personal data held on them by employers and other agencies, including visual data collected by CCTV cameras and other surveillance equipment. The following standards should be maintained:

1. Staff involved in operating CCTV and other surveillance equipment should be aware of the College procedures for dealing with subject access requests and with the rights of the individual concerning subject access under the DP Act.
2. Data Subjects who wish to view images of themselves that they believe have been captured on CCTV should submit a standard subject access request form. In order to enable the College to locate the relevant images, Data Subjects will need to provide certain information in order to identify themselves (a photo of themselves, the date, time and location when a particular image might have been captured, and a description of what they were wearing at the time). Giving the reason for their request would also assist the College to locate the image requested. Blanket requests will be considered unreasonable and will not be complied with.
3. The Data Owner responsible for the system which captured the images should determine whether disclosure to the individual requesting access would entail disclosing images of third parties and if so whether images of third parties might need to be obscured.
4. If third party images are not to be disclosed, the data owner shall arrange for the third party images to be disguised or blurred.
5. If the data owner decides that a subject access request is not to be complied with, he/she should document the identity of the individual making the request, the date of the request, the reason for refusing to comply with the request and the name and signature of the person making the decision.

8. Monitoring compliance with this code of practice

1. A record of the number and nature of complaints or enquiries received should be maintained by the manager responsible for any scheme, together with an outline of the action taken in each case.

2. A report on those numbers should be made available to the College Data Protection Officer, acting on behalf of the College Data Controller.

3. The College Data Protection Officer should undertake regular reviews of the documented procedures to ensure that the provisions of this Code are being complied with and a report on these reviews submitted to the College Data Controller to ensure that compliance with legal obligations is being maintained.

4. College Authorised Officers should carry out regular assessments to evaluate the effectiveness of the scheme being operated in light of the stated purpose for that scheme. If the scheme is not achieving its purpose it should be discontinued or modified.