

CANTERBURY COLLEGE POLICY

CCTV IMAGES POLICY

EFFECTIVE DATE: December 2011

LAST REVIEWED: December 2011

REVIEWED BY: Craig Nimmo

NEXT REVIEW: December 2013

POLICY LEAD: Director of Finance & Corporate Services

Estates and Building Services Department

POLICY: CCTVRP2011-12

REVISION: 2

DATE: 30/8/11

OWNER: CN

Procedure for the release of CCTV footage.

Introduction

With the increasing use of Closed Circuit Television cameras throughout the City Centre and Canterbury College and Sheppey College estate, strict procedures must be in place to ensure that cameras and footage are only used for the purpose stated in the Code of Practice.

This will ensure that nobody's right to privacy is denied or encroached upon, whilst fulfilling the main aims of the installation, i.e.: to detect and prevent crime.

All CCTV systems installed have safeguards built in to prevent cameras from looking into areas where they are not authorised to look, such as windows, gardens, conservatories etc. The cameras are all computer controlled, and the system set to prevent this type of intrusive surveillance.

Canterbury College is committed to the rights of privacy, and ensures that all precautions are taken to ensure those rights are not infringed.

1. General Policy

All requests for the release of CCTV footage, (called Data), shall be channelled through the Estates and Building Services Manager, or their representative.

2. Primary requests to view data.

Requests to view data generated by a CCTV system are likely to be made by third parties for any one or more of the following purposes:

- Providing evidence in criminal proceedings.
- Providing evidence in civil proceedings or tribunals.
- The prevention of crime.
- The investigation and detection of crime, including identification of offenders.
- Identification of witnesses.

Third parties are required to show adequate grounds for disclosure of data within the above criteria, and may be any of the following:

- Police Authorities.
- Statutory Authorities with powers to prosecute, (e.g. Customs & Excise, Trading Standards etc.).
- Solicitors, on behalf of clients.
- Claimants in civil proceedings.
- Accused persons or Defendants in criminal proceedings.
- Other Agencies, (as agreed by the Data Controller and notified to the Information Commissioner) according to purpose and legal status.

All requests are to be made in writing by the Third Party and signed by their representative of the highest authority possible.

All requests for data shall be verified before data is released, and the Data Controller shall:

- Not unduly obstruct or delay a third party investigation to verify the existence of relevant data.
- Ensure the retention of data which may be relevant to a request, but for which a completed application, Court Order or Subpoena has not been completed. A time limit shall be imposed on such retention, which will be notified to the inquirer at the time of the request.
- Ensure that all recordings seized are accompanied by a witness statement verifying authenticity, and said footage shall be sealed in an evidence bag, and signed for by the Officer assigned to the investigation.

Where requests fall outside the terms of disclosure and Subject Access legislation, the data controller, or nominated representative, shall inform the inquirer of this in writing within 10 days of receipt of the request. All requests for data shall be treated with the utmost confidentiality.

3. Secondary requests to view data.

A secondary request to view data may be defined as any request being made which does not fall into the category of a primary request. For example, a request made under the Freedom of Information Act (further information can be found under **freedom of information** on this site). Before complying with a secondary request, the data controller shall ensure that the request does not contravene (and compliance with the request would not breach) current relevant legislation, e.g. Data Protection Act 1998, Human Rights Act 1998, Section 163 of the Criminal Justice & Public Order Act 1994, etc.

The data controller shall ensure that any requests:

- Comply with all legislative requirements.
- Due regard has been taken of any known case law, current or past, which may be relevant.
- The request would pass a test of 'disclosure in the public interest.'

If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:

- In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material shall be obtained from a Police Officer, not below the rank of Inspector. The Officer should have personal knowledge of the circumstances of the crime/s to be prevented, and an understanding of the CCTV Code of Practice.
- If the material is to be released under the auspices of 'public well-being, health or safety' written agreement to the release of the material shall be obtained from a senior officer within the local authority, in consultation with the Data Protection Officer. The officer should have personal knowledge of the potential benefit to be gained from the release of the material, and an understanding of the CCTV Code of Practice.
- Recorded material may be used for bona fide training purposes, such as staff training, but under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

4. Individual subject access under Data Protection legislation.

Under the terms of the Data Protection Act 1998, individual access to personal data, of which that individual is the data subject, must be permitted, providing that:

- The request is made in writing.
- A specific fee is paid for each individual search.
- The data controller is supplied with sufficient information to satisfy them as to the identity of the person making the request.
- The person making the request provides sufficient accurate information about the time, date and location to enable the data controller to locate the information sought, (it is recognised that a person making a request is unlikely to know the exact time. Under these circumstances, it is reasonable to expect within one hour accuracy.).
- The person making the request is only shown information relevant to that particular search, and which only contains personal data of themselves, unless all other individuals who may be identified from the same information have consented to the disclosure.

In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable.

The data controller is entitled to refuse an individual request to view data under these provisions, if insufficient or inaccurate information is provided. However every effort will be made to comply with subject access procedures, and every request will be treated on its own merit.

In addition to the principles contained within Data Protection legislation, the data controller will be satisfied that the data is:

- Not currently, and as far as can be reasonably ascertained not likely to become, part of a criminal investigation.
- Not currently, and as far as can be reasonably ascertained not likely to become, relevant to civil proceedings.
- Not the subject of a complaint or dispute which has not been actioned.
- The original data, and that the audit trail has been maintained.
- Not removed or copied without proper authority.
- For individual disclosure only (i.e. to be disclosed to a named subject).

5. **Process of Disclosure**

The data controller will verify the accuracy of the request.

The requestee will be shown the relevant footage only (or authorised person acting on their behalf).

The viewing will take place in isolation from the control room, with adequate supervision.

Only data, which is specific to the request, will be shown.

It must not be possible to identify any other individual from the information being shown (any such information will be blanked-out, either by means of electronic depixelation, or manual editing on the monitor screen).

If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an authorised editing house for processing prior to being sent to the requestee, (an additional fee would be payable for this).

6. **Media Disclosure**

Material will not be released to the media unless prior consent is sought from the Data Controller, and only then for the purpose of identifying suspects in criminal proceedings.

Craig Nimmo

Estates and Building Services Manager

Canterbury College