Standards for the Release of Data to Third Parties

1. Introduction

The Information Commissioners Office Code of Practice (2008) for CCTV systems/schemes is followed by Wiltshire Council.

2. General Policy

All requests for the release of data shall be processed in accordance with the Procedures Manual. All such requests shall be channelled through the Corporate Information Team to the System Manager.

Note: The Corporate Information Team report to the Council Data Controller who (either alone or jointly with others) agree what data will be released and the manner in which any personal data will be processed or released, to ensure compliance with the relevant legislation. (DPA, FoIA).

Day to day responsibility for the operation of the CCTV system lies with the System Manager.

3. Primary Request to View Data

a) Primary 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:

- i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.)
- ii) Providing evidence in civil proceedings or tribunals
- iii) The prevention of crime
- iv) The investigation and detection of crime (may include identification of offenders).
- V) Identification of witnesses

b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

- i) Police (see note 1)
- ii) Statutory (enforcing) authorities with powers to prosecute (e.g. Custom & Excise, Trading Standards, etc.)
- iii) Solicitors (see note 2)
- iv) Plaintiffs in civil proceedings (see note 3)
- v) Accused persons or defendants in criminal proceedings (see note 3)
- vi) Other agencies, according to purpose and legal status (see note 4)

c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:

- i) Not unduly obstruct a third party investigation to verify the existence of relevant data.
- ii) Ensure the retention of data which may be relevant to the request, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.

d) In circumstances outlined in note (3) below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative shall:

i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
ii) Treat all such enquiries with strict confidentiality.

Notes:
(1) The release of data to the police is not to be restricted to the civil police but could include (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (Special arrangements may be put in place in response to local requirements)

(2) Aside from criminal investigation, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred.

In all circumstances data will only be released for lawful and proper purposes.

(3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

(4) The data controller shall decide which (if any) 'other agencies' might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this Standard.

(5) The data controller can refuse an individual request to view if sufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest half-hour).

4. Secondary Request to View Data

a) A 'secondary' request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:

i) The request does not contravene and that compliance with the request would not breach current relevant legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.)
ii) Any legislative requirements have been complied with (e.g. the requirements of the Data Protection Act 1998)
iii) Due regard has been taken of any known case law (current or past) which may be relevant (e.g. R v Brentwood BC ex P. Peck) and
iv) The request would pass a test of 'disclosure in the public interest' (see note 1)

b) 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 to place before releasing the material:

i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should 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.

ii) If the material is to be released under the auspices of 'public well being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV Code of Practice.

c) Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale or for entertainment purposes.

Note:
(1) 'Disclosure in the public interest' could include the disclosure of personal data that:

i) provides specific information which would be of value or of interest to the public well being
ii) identifies a public health or safety issue
iii) leads to the prevention of crime
iv) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request (see 3 above).

5. Individual Subject Access under Data Protection Legislation

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

i) The request is made in writing
ii) A specified fee is paid for each search
iii) A data controller is supplied with sufficient information to satisfy him/herself as to the identity of the person making the request.
iv) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks (it is recognised that a person making a request may not know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement)
v) The person making the request is only shown information relevant to that particular search and which contains personal data of hi/herself only, unless all other individuals who may be identified from the same information have consented to the disclosure.

b) 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).

c) 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 should be made to comply with subject access procedures and each request should be treated on its own merits.

d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:
i) Not currently and as far as can be reasonably ascertained, not likely to become part of a 'live' criminal investigation.
ii) Not currently and as far as can be reasonably ascertained, not likely to become relevant to civil proceedings
iii) Not the subject of a complaint or dispute which has not been actioned
iv) The original data and that an audit trail has been maintained
v) Not removed or copied without proper authority
vi) For individual disclosure only (i.e. to be disclosed to a named subject)

6. Process of Disclosure

a) Verify the accuracy of the request

b) Replay the data to the requestee only (or responsible person acting on their behalf)

c) The viewing should take place in a separate room and not in the control room or monitoring area. Only data relevant to the request to be shown.

d) 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 screening or manual editing on the monitor screen

e) 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 editing house for processing prior to being sent to the requestee.

Note: The Information Commissioners Code of Practice for CCTV makes specific requirements for the precautions to be taken when images are sent to an editing house for processing.

7. Media Disclosure

a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:

i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.
ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.
iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System Code of Practice).
iv) The release form shall be considered a contract and signed by both parties (see note 1)
Note: In the well publicised case of R v Brentwood Borough Council, ex parte Geoffrey Dennis Peck, (QBD November 1997), the judge concluded that by releasing the video footage, the Council had not acted lawfully. A verbal assurance that the broadcasters would mask the identity of the individual had been obtained. Despite further attempts by the Council to ensure the identity would not be revealed, the television company did in fact broadcast footage during which the identity of Peck was not concealed. The judge concluded that tighter guidelines should be considered to avoid future accidental broadcasts.
Attention is drawn to the requirements of the Information Commissioners in this respect, detailed in her Code of Practice summarised above.

8. Principles

In adopting this national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the system.

b) Access to recorded material shall only take place in accordance with this standard and the Code of Practice.

c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.