

SOLIHULL MBC CCTV IMPLICATIONS – DATA PROTECTION ACT 1998

1 DATA PROTECTION IMPLICATIONS

1.1 It is intended to provide guidance as to good practice for users of CCTV (closed circuit television) and similar surveillance equipment.

Initial Assessment Procedures

1.2 Before installing and using CCTV and similar surveillance equipment, users will need to establish the purposes for which they intend to use the equipment. This equipment may be used for a number of different purposes; for example, prevention, investigation and detection of crime, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings), public and employee safety, monitoring security of premises etc.

Siting the Cameras

1.3 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 standards to be met under this Code of Practice are set out below.

Standards

- (a) Identity of the person or organisation responsible for the scheme.
- (b) The purposes of the scheme.
- (c) Details of whom to contact regarding the scheme.

(First Data Protection Principle)

1.4 In exceptional and limited cases, if it is assessed that the use of signs would not be appropriate, the user of the scheme must ensure that they have:

- (a) Identified specific criminal activity.
- (b) Identified the need to use surveillance to obtain evidence of that criminal activity.
- (c) Assessed whether the use of signs would prejudice success in obtaining such evidence.
- (d) Assessed how long the covert monitoring should take place to ensure that it is not carried out for longer than is necessary.
- (e) Documented to above.

1.5 Information so obtained must only be obtained for prevention or detection of criminal activity, or the apprehension and prosecution of offenders. It should not be retained and used for any other purpose. If the equipment used has a sound recording facility, this should not be used to record conversations between members of the public (First and Third Data Protection Principles).

Quality of the Images

1.6 If a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

Standards

- (a) Upon installation an initial check should be undertaken to ensure that the equipment performs properly.
- (b) If tapes are used, it should be ensured that they are good quality tapes (Third and Fourth Data Protection Principles).
- (c) The medium on which the images are captured should be cleaned so that images are not recorded on top of images recorded previously (Third and Fourth Data Protection Principles).
- (d) The medium on which the images have been recorded should not be used when it has become apparent that the quality of images has deteriorated. (Third Data Protection Principle).
- (e) If the system records features such as the location of the camera and/or date and time reference, these should be accurate (Third and Fourth Data Protection Principles).
- (f) If their system includes such features, users should ensure that they have a documented procedure for ensuring their accuracy.
- (g) Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established (Third Data Protection Principle)
- (h) If an automatic facial recognition system is used to match images captured against a database of images, then both sets of images should be clear enough to ensure an accurate match (Third and Fourth Data Protection Principles).
- (i) If an automatic facial recognition system is used, procedures should be set up to ensure that the match is also verified by a human operator, who will assess the match and determine what action, if any, should be taken (First and Seventh Data Protection Principles).
- (j) The result of the assessment by the human operator should be recorded whether or not they determine there is a match.
- (k) When installing cameras, consideration must be given to the physical conditions in which the cameras are located (Third and Fourth Data Protection Principles).
- (l) Users should assess whether it is necessary to carry out constant real time recording, or whether the activity or activities about which they are concerned occur at specific times (First and Third Data Protection Principles)

- (m) Cameras should be properly maintained and serviced to ensure that clear images are recorded (Third and Fourth Data Protection Principles)
- (n) Cameras should be protected from vandalism in order to ensure that they remain in working order (Seventh Data Protection Principle)
- (o) A maintenance log should be kept.
- (p) If a camera is damaged, there should be clear procedures for:
 - (i) Defining the person responsible for making arrangements for ensuring that the camera is fixed.
 - (ii) Ensuring that the camera is fixed within a specific time period (Third and Fourth Data Protection Principle).
 - (iii) Monitoring the quality of the maintenance work.

Processing the images

1.7 Images, which are not required for the purpose(s) for which the equipment is being used, should not be retained for longer than is necessary. While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the 1998 Act. The Seventh Data Protection Principle sets out the security requirements of the 1998 Data Protection Act. The standards required by this Code of Practice are set out below.

Standards

- (a) Images should not be retained for longer than is necessary (Fifth Data Protection Principle)
- (b) Once the retention period has expired, the images should be removed or erased (Fifth Data Protection Principle).
- (c) If the images are retained for evidential purposes, they should be retained in a secure place to which access is controlled (Fifth and Seventh Data Protection Principles).
- (d) On removing the medium on which the images have been recorded for the use in legal proceedings, the operator should ensure that they have documented:
 - (i) The date on which the images were removed from the general system for use in legal proceedings.
 - (ii) The reason why they were removed from the system.
 - (iii) Any crime incident number to which the images may be relevant.
 - (iv) The location of the images.
- (e) The signature of the collecting police officer, where appropriate (Third and Seventh Data Protection Principles).
- (f) Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised employees of the user of the equipment (Seventh Data Protection Principle).
- (g) Access to the recorded images should be restricted to a manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the user's documented disclosure policies (Seventh Data Protection Principle).

- (h) Viewing of the recorded images should take place in a restricted area, for example, in a manager's or designated member of staff's office. Other employees should not be allowed to have access to that area when a viewing is taking place (Seventh Data Protection Principle).
- (i) Removal of the medium on which images are recorded, for viewing purposes, should be documented as follows:
 - i. The date and time of removal
 - ii. The name of the person removing the images
 - iii. The name(s) of the person(s) viewing the images. If this should include third parties, this should include the name of the organisation of that third party
 - iv. The reason for the viewing
 - v. The outcome, if any, of the viewing
 - vi. The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes
- (j) All operators and employees with access to images should be aware of the procedures that need to be followed when accessing the recorded images (Seventh Data Protection Principle).
- (k) All operators should be trained in their responsibilities under this Code of Practice i.e. they should be aware of:
 - i. The user's security policy e.g. procedures to have access to recorded images.
 - ii. The user's disclosure policy.
 - iii. Rights of individuals in relation to their recorded images.

(Seventh Data Protection Principle)

Access to and disclosure of images to third parties

1.8 Users of CCTV will also need to ensure that the reason(s) for which they may disclose copies of the images are compatible with the reason(s) or purpose(s) for which they originally obtained those images.

Standards

1.9 All employees should be aware of the restrictions set out in this code of practice in relation to access to, and disclosure of, recorded images.

- (a) 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 equipment (Seventh Data Protection Principle).
- (b) All access to the medium on which the images are recorded should be documented (Seventh Data Protection Principle).
- (c) Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances (Second and Seventh Data Protection Principles).

For example - if the purpose of the system is the prevention and detection of crime, then disclosure to third parties should be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry

- Prosecution agencies
- Relevant legal representatives
- The media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

(d) If access or disclosure is denied, the reason should be documented

(Seventh Data Protection Principle)

(e) If access to or disclosure of the images is allowed, then the following should be documented:

(f) The date and time at which access was allowed or the date on which disclosure was made

(i) The identification of any third party who was allowed access or to whom disclosure was made

(ii) The reason for allowing access or disclosure

(iii) The extent of the information to which access was allowed or which was disclosed

(g) Recorded images should not be made more widely available - for example they should not be routinely made available to the media or placed on the Internet (Second, Seventh and Eighth Data Protection Principles).

(h) If it is intended that images will be made more widely available, that decision should be made by the manager or designated member of staff. The reason for that decision should be documented (Seventh Data Protection Principle).

(i) If it is decided that images will be disclosed to the media, the images of individuals will need to be disguised or blurred so that they are not readily identifiable (First, Second and Seventh Data Protection Principles).

(j) If the system does not have the facilities to carry out that type of editing, an editing company may need to be hired to carry it out.

(k) If an editing company is hired, then the manager or designated member of staff needs to ensure that:

(i) There is a contractual relationship between the data controller and the editing company.

(ii) That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images.

(iii) The manager has checked to ensure that those guarantees are met

(iv) The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the manager or designated member of staff.

(v) The written contract makes the security guarantees provided by the editing company explicit.

(Seventh Data Protection Principle)

(l) If the media organisation receiving the images undertakes to carry out the editing, then (a) to (e) will still apply (Seventh Data Protection Principle)

Access by data subjects

1.10 This is a right, which is provided by section 7 of the 1998 Act. The standards of this Code of Practice are set out below.

Standards

- (a) All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects (Sixth and Seventh Data Protection Principles).
- (b) Data subjects should be provided with a standard subject access request form which:
 - (i) Indicates the information required in order to locate the images requested.
 - (ii) Indicates the information required in order to identify the person making the request.
 - (iii) Indicates the fee that will be charged for carrying out the search for the images requested. A maximum of £10.00 may be charged for the search.
 - (iv) Asks whether the individual would be satisfied with merely viewing the images recorded.
 - (v) Indicates that the response will be provided promptly and in any event within 40 days of receiving the required fee and information.
 - (vi) Explains the rights provided by the 1998 Act.
- (c) Individuals should also be provided with a leaflet, which describes the types of images that are recorded and retained, the purposes for which those images are recorded and retained, and information about the disclosure policy in relation to those images (Sixth Data Protection Principle).
- (d) This should be provided at the time that the standard subject access request form is provided to an individual (Sixth Data Protection Principle).
- (e) All subject access requests should be dealt with by a manager or designated member of staff.
- (f) The manager or designated member of staff should locate the images requested.
- (g) The manager or designated member of staff should determine whether disclosure to the individual would entail disclosing images of third parties (Sixth Data Protection Principle).
- (h) The manager or designated member of staff will need to determine whether the images of third parties are held under a duty of confidence (First and Sixth Data Protection Principle).
- (i) If third party images are not to be disclosed, the manager or designated member of staff shall arrange for the third party images to be disguised or blurred (Sixth Data Protection Principle).
- (j) If the system does not have the facilities to carry out that type of editing, a third party or company may be hired to carry it out
- (k) If a third party or company is hired, then the manager or designated member of staff needs to ensure that:
 - (i) There is a contractual relationship between the data controller and the third party or company.
 - (ii) That the third party or company has given appropriate guarantees regarding the security measures they take in relation to the images.

- (iii) The manager has checked to ensure that those guarantees are met.
- (iv) The written contract makes it explicit that the third party or company can only use the images in accordance with the instructions of the manager or designated member of staff.
- (v) The written contract makes the security guarantees provided by the third party or company explicit

(Seventh Data Protection Principle)

- (l) If the manager or designated member of staff decides that a subject access request from an individual is not to be complied with, the following should be documented:
 - (i) The identity of the individual making the request
 - (ii) The date of the request
 - (iii) The reason for refusing to supply the images requested
 - (iv) The name and signature of the manager or designated member of staff making the decision.
- (m) All staff should be aware of individuals' rights under this section of the Code of Practice (Seventh Data Protection Principle)

Other rights

1.11 The standards of this Code are set out below.

- (a) All staff involved in operating the equipment must be able to recognise a request from an individual to:
 - (i) Prevent processing likely to cause substantial and unwarranted damage to that individual.
 - (ii) Prevent automated decision taking in relation to that individual.
- (b) All staff must be aware of the manager or designated member of staff who is responsible for responding to such requests.
- (c) In relation to a request to prevent processing likely to cause substantial and unwarranted damage, the manager or designated officer's response should indicate whether he or she will comply with the request or not.
- (d) The manager or designated member of staff must provide a written response to the individual within 21 days of receiving the request setting out their decision on the request.
- (e) If the manager or designated member of staff decide that the request will not be complied with, they must set out their reasons in the response to the individual.
- (f) A copy of the request and response should be retained.
- (g) If an automated decision is made about an individual, the manager or designated member of staff must notify the individual of that decision.
- (h) If, within 21 days of that notification, the individual requires, in writing, the decision to be reconsidered, the manager or designated staff member shall reconsider the automated decision.

- (i) On receipt of a request to reconsider the automated decision, the manager or designated member of staff shall respond within 21 days setting out the steps that they intend to take to comply with the individual's request.
- (j) The manager or designated member of staff shall document:
 - (i) The original decision.
 - (ii) The request from the individual.
 - (iii) Their response to the request from the individual.

Monitoring compliance with this code of practice

1.12 Standards

- (a) The contact point indicated on CCTV signs should be available to members of the public during office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.
- (b) Enquiries should be provided on request with one or more of the following:
 - (i) The leaflet which individuals receive when they make a subject access request as general information
 - (ii) A copy of this code of practice
 - (iii) A subject access request form if required or requested
 - (iv) The complaints procedure to be followed if they have concerns about the use of the system
 - (v) The complaints procedure to be followed if they have concerns about non-compliance with the provisions of this Code of Practice
- (c) A complaints procedure should be clearly documented.
- (d) A record of the number and nature of complaints or enquiries received should be maintained together with an outline of the action taken.
- (e) A report on those numbers should be collected by the manager or designated member of staff in order to assess public reaction to and opinion of the use of the system.
- (f) A manager or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Code are being complied with (Seventh Data Protection Principle).
- (g) A report on those reviews should be provided to the data controller(s) in order that compliance with legal obligations and provisions with this Code of Practice can be monitored.
- (h) An internal annual assessment should be undertaken which evaluates the effectiveness of the system.
- (i) The results of the report should be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, it should be discontinued or modified.
- (j) The result of those reports should be made publicly available.