MR07 - CCTV Policy and Procedure

Purpose

- To comply with the Data Protection Act 1998.
- Taking into account:
  - The CCTV Code Of Practice produced by the Information Commissioner;
  - The Human Rights Act 1998;
  - The Mental Capacity Act 2005;
  - The Regulation of Investigatory Powers Act 2000;
  - Caldicott Report 1997.

Scope

- This policy will cover all employees of , persons providing a service (voluntary or paid) to the organisation, Service Users, visitors and all other persons whose image(s) may be captured by the system at 's premises.

Guidance to the Service Provider

- This policy is for the guidance of the Service Provider.

Policy

- must, before deploying any CCTV system, modifying an existing system, or on first introduction of this Policy, conduct a written impact assessment which must include:
  - An examination of the effects which the deployment has on the privacy of employees of ; persons providing a service (voluntary or paid) to the organisation; Service Users; visitors and all other persons whose image(s) may be captured by the system.
  - Who will be using the CCTV images? Who will take legal responsibility under the Data Protection Act?
  - What is the organisation’s, Service User's, or their families purpose for using CCTV? What are the problems it is meant to address? These could include:
    - Prevention or detection of crime or disorder;
    - Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings);
    - Interest of public and employee Health and Safety;
    - Protection of public health;
    - Protection of property and assets;
    - To provide evidence in support of misconduct.
  - What are the benefits to be gained from its use?
  - Are the images to be used concurrently i.e. the monitor manned permanently in order to identify and deal with incidents such as unauthorised or dangerous ingress or egress of people, or are images to be made and stored only for review if past incidents are to be reviewed?

MR07 - CCTV Policy and Procedure

- Can CCTV technology realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Do you need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?
- Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will you address these?
- What are the views of those who will be under surveillance?
- What could you do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?

- Where the system will be operated by or on behalf of a public authority, the authority will also need to consider wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life). The surveillance must also comply with The Regulation of Investigatory Powers Act 2000 (RIPA). This will include:
  - Is the proposed system established on a proper legal basis and operated in accordance with the law?
  - Is it necessary to address a pressing need, such as public safety, crime prevention or national security?
  - Is it justified in the circumstances?
  - Is it proportionate to the problem that it is designed to deal with?
- If this is not the case then it would not be appropriate to use CCTV.
- The impact assessment must be written, and stored for future reference, including auditing the system to ensure that it meets the assessed parameters.

Policy application

- must designate a Data Controller to take the legal responsibility for the operation and compliance of the CCTV system and resulting data. If the organisation is a legal entity e.g. a limited company, then the Data Controller can be the limited company, it does not need to be a person.

Procedure

Siting the cameras

- It is essential that the location of the equipment be carefully considered, because the way in which images are captured will need to comply with the Data Protection Act.
- All cameras will be located in prominent positions within Service User, public, and staff view and do not infringe on living, circulating (corridors etc) areas.
- All CCTV surveillance will be automatically recorded and any breach of these Codes of Practice will be detected via controlled access to the system and auditing of the system.
- Signs need to be erected on all entrance points to premises and throughout the site to ensure staff and visitors are aware they are entering an area that is covered by CCTV surveillance equipment. The signs must include details on the purpose, organisation and contact details.
- Use of Covert CCTV (Directed) surveillance if required should be considered only with consultation with the

MR07 - CCTV Policy and Procedure

Police, whose advice and requirements must be met.

- Siting a camera within a Service User's place of care provision must be carried out in consultation with Service Users and their families.

- Consultation with these people is the best way to understand their privacy concerns. The privacy concerns that are identified during consultation must be given due consideration in line with Regulation 17(2)(d) Health and Social Care Act 2008 (Regulated Activities) Regulations 2014.

KEY POINTS

- Covert and overt surveillance can have legitimate uses. The benefits should be weighed against the impact on the person's privacy.

- The use of surveillance in places where people are receiving health and social care is likely to raise greater privacy concerns than in any other kind of business - especially where the care is being provided in the Service User's personal space.

- Transparency and openness are vital in order to meet legal requirements, and to maintain the trust of people who use the services and of the care staff. However there may be limited circumstances where the legitimate use of covert surveillance prevents such openness for a short time.

DEFINITIONS

- Surveillance - This is the monitoring of place, person, group or on-going activity to gather information.

- Overt Surveillance - This is where the individual being monitored would reasonably be aware of the surveillance occurring. For example, visible CCTV camera with clear signs stating they are in use.

- Covert Surveillance - This is surveillance where the individual being monitored would not reasonably be aware of the surveillance occurring. For example, the use of hidden CCTV for a time limited specific purpose.

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. This is why it is essential that the purpose of the scheme be clearly identified. For example, if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

- All camera installations and service contracts should be undertaken by NACOSS approved security companies where the equipment is placed in or on the site of s premises. Upon installation, all equipment is tested to ensure that only the designated areas are monitored and high quality pictures are available in live and play back mode. All CCTV equipment should be serviced and maintained on an annual basis by a NACOSS approved company.

- The system can consist of cameras recording to digital recorders. These recorders must be located in secure locations, with access control at two levels (a) access to the location available only to authorised persons (b) access to images must be password protected and limited to persons authorised to view them.

Processing the images

- 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.

- All images that are digitally recorded in or on site of s premises must be stored securely within the system’s hard drives for up to 30 days when they are then automatically erased. Located within the ’s premises there may

MR07 - CCTV Policy and Procedure

be sub monitors which display images of public areas, however these must be located within enclosed areas and only accessible to ‘s authorised employees.

- Where the images are required for evidential purposes in legal or disciplinary proceedings, a DVD disc recording is made and placed in a sealed envelope signed and dated and held by the Registered Manager until completion of the investigation. Viewing of images must be controlled by the Data Controller or a person nominated to act on their behalf. Only persons trained in the use of the equipment and authorised by the Data Controller can access data. For images taken by equipment belonging to a Service User or their family, these can be shared with the police, adult services or other relevant party.

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. This will ensure that the rights of individuals are preserved, but also to ensure that the continuity of evidence remains intact should the images be required for evidential purposes e.g. a Police inquiry or an investigation being undertaken as part of the disciplinary procedure.

- Access to the medium on which the images are displayed and recorded must be restricted to such parties and persons as the Data Controller may decide, subject to the restrictions of legislation and good practice.
For Service User equipment, the Data Controller may be themselves or their appointed family member.

- Access and disclosure to images is permitted only if it supports the purpose of the scheme. Under these conditions, the CCTV images record book and the appropriate view / release form (see Appendix) must be completed for images taken on or in company premises.

Access to images by individuals

- Section 7 of the 1998 Data Protection Act gives any individual the right to request access to CCTV images.

- Individuals who request access to images taken on or in company premises must be issued an access request form (see appendix). Upon receipt of the completed form, the Registered Manager and Provider’s representative will determine whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties. If the duty of care cannot be discharged then the request can be refused.

- A written response must be made to the individual, giving the decision (and if the request has been refused, giving reasons) within 40 days of receipt of the enquiry. If disclosure is appropriate a payment in advance of £10.00 may be required.

Enforcement

- The Information Commissioner has the power to issue Enforcement Notices where they consider that there has been a breach of one or more of the Data Protection Principles. An Enforcement Notice will set out the remedial action that the Commissioner requires of to ensure future compliance with the requirements of the Act. The ICO should be notified prior to installation of any CCTV. When informing the ICO you will be required to identify what the data you are recording will be used for.

- The Data Protection Guide - https://ico.org.uk/for-organisations/guide-to-data-protection/

MR07 - CCTV Policy and Procedure

Appendix

Access to view or copy images	
Name of person making the request:	
Organisation (if appropriate):	
Address:	
Telephone number:	
Details of image to be viewed:	
Date:	
Reason:	
Signed:	Date of signature:
Request granted	
Request denied (state reason(s))	
To be completed if images are to be copied and removed from storage	
Images issued to:	
Case reference (e.g. Police crime number, or disciplinary file reference):	
Date issued:	
Issued by:	
Return date:	
I acknowledge receipt of the DVD containing the images referred to above	
Signed:	Date:
Designation:	

MR07 - CCTV Policy and Procedure

Key Lines of Enquiry Table

Key Line of Enquiry	Primary	Supporting	Mandatory
R.C3 - How is peoples privacy and dignity respected and promoted?	✓		✓

Note: All QCS Policies are reviewed annually, more frequently, or as necessary.