Surveillance Management Procedure

Title	Surveillance Management Procedure
Author/Owner	Senior Management Team
Status	Approved
Version	1
Date Approved	27/03/18
Approved by	Full Governing Body
Review Date	Summer 2019
Security Classification	Sensitive

1. Contents

1. Introduction

1.1. This procedure covers all matters relating to the use of video and audio recording equipment for overt surveillance in all buildings where the Organisation's employees work and which members of the public utilise. Covert surveillance under the Investigatory Powers Act (2016) is not covered by this document.

2. Policy References

2.1. This procedure is a requirement of the following policies:

- Data Protection Policy

3. Surveillance Management Procedures

3.1. Responsibility

Within the Organisation responsibility for Data Protection issues resides with the Data Protection Officer (DPO).

Responsibility for approving and reviewing this policy rests with the DPO, but responsibility for implementation of these procedures and for reporting performance issues under the policy rests with all employees who have involvement in the management of equipment. Responsibility for managing the deployment and use of cameras rests with identified members of staff with the appropriate authority to ensure procedures are adhered to.

3.2. Impact Assessments

3.2.1. **Scope and Review**: The siting of each CCTV camera that falls within the scope of this policy will be subject to an Impact Assessment (Annex A) before it is commissioned or a retrospective Impact Assessment where it was already operational before policy and this procedure was approved. Each site will be subject to a review against the Impact Assessment criteria every two years, or sooner should there be any relevant change to the building use.

3.2.2. **Ownership**: Each site will have an identified owner who will take responsibility for the operation of all CCTV equipment on that premises or location. Where premises are shared with another organisation and

control of CCTV equipment does not rest with the Organisation, or where operation of equipment is contracted out to a service provider, the Impact Assessment will still record the Organisation's DPO as a point of contact who will be able to redirect queries to the relevant person outside of the Organisation.

3.2.3. **Purpose**: The Impact Assessment will establish whether or not there is a need for CCTV cameras in the first instance by recording the aims and benefits that the camera is meant to deliver and assessing whether there is any other solution that could achieve this.

3.2.4. **Quality**: The level of detail required of CCTV recordings will be assessed according to a categorisation scheme approved by the Home Office. The four quality levels of Monitoring, Detecting, Recognising and Identifying explain the various level of detail that is required for cameras to meet their stated purpose.

3.2.5. **Wider Use:** Consideration will be given as to whether or not there is any wider use that CCTV cameras serve other than the stated purpose. If there is then communicating this additional purpose will be considered.

3.2.6. **Feedback:** Signage and explanatory publications will make building users aware of the purpose of the cameras and how to register feedback. Any complaints or concerns raised about the siting or usage of cameras will be captured and considered in a review. The outcomes of reviews will be communicated to those who have raised concerns, and to a wider audience if deemed appropriate

3.3. Signage & explanatory publications

3.3.1. **Signage.** Signs explaining that CCTV recording is operational in the vicinity shall be clearly visible and legible in accessible areas of the building. They will state who operates the equipment, what their purpose is and provide a contact number of the DPO for those with queries about usage and who wish to access recordings

3.3.2. **Explanatory Publications.** At each building there will be an appropriate supply of an approved leaflet which gives summary details of the policy and procedure including advice about how to make a formal request to view recordings.

3.4. Retention, Security & Access

3.4.1. **Retention of Recordings.** The Organisation commits to retaining recordings for security from CCTV cameras under its control for [31 days]. Cameras managed by partner organisations (not contracted service providers) are responsible for defining and publicising their own retention timescales. This period of time is based on the recommended range of 12-31 days and our experience of the need for authorised usage. When this time period has expired, the data on the recorded tape or server will either be recorded-over, degaussed (deleting magnetic storage content) or disposed of – in any event deleted beyond the ability to reconstitute the content.

3.4.2. **Security:** Once a recording is complete, the tape or other storage medium will be held in a secure container or on a secure server to which only authorised persons trained specifically in the policy and procedures have access.

3.4.3. **Access:** Instances of access to recordings will be recorded in a log which can be produced on demand to the DPO, an authorised manager or Auditor/ Regulator and will be a complete record of access activity (Annex C). This log should state:

- Dates of access,
- the period and location covered by the recording,
- the reason for access and
- Name, position and authority of those who have accessed recordings.
- Whether or not copies were made.

3.4.4. There must be a single point within premises where a record of acceptance forms is stored. These will record signatures on approved forms of those who have had access and will support full auditability.

3.5. Usage

3.5.1. **The Organisation's Usage:** We will only use recorded CCTV images for the purposes which we have identified in our Impact Assessments and communicated through signage and explanatory leaflets.

3.5.2. **Usage by other Organisations:** We will ensure that where recordings are accessed by or copies are provided to other organisations, this will also fall within these stated purposes, or otherwise within the law. Where copies are provided, the organisation requesting the material will be required to agree to manage the data in accordance with the Data Protection Act/ General Data Protection Regulations (Annex D). Where regular general information sharing with a partner takes place we will

have in place an Information Sharing Protocol under the Whole Essex Information Sharing Framework.

3.5.3. **Recording:** Where use is made of recordings by us or access granted or copies provided to other organisations, these instances will be recorded and kept up to date in a central log available for inspection by anyone with the authority to do so wishing to monitor compliance with this policy. The reasons for use will be recorded and approved (Annex C).

3.6. Handling Access Requests

3.6.1. **Rights.** Employees and members of the public whose images are captured by surveillance equipment have a right in law to access such recordings.

3.6.2. **Data Protection Law**. The Data Protection Act and the General Data Protection Regulations (from May 2018) provide statutory rights for individuals (employees and members of the public) to have access to information held by organisations about themselves. By the very nature of surveillance images there is likely to be information present on recordings that identifies not just the requesting Data Subject but other persons who had been present. This will require an assessment of whether or not third parties can be identified and if so what method and level of redaction may be necessary.

3.6.3. **Freedom of Information Act.** The Freedom of Information Act provides general statutory rights of access to information held by Public Authorities. In practice, the rules governing this access regime will be applied where a requestor is asking for information about a person or persons other than themselves.

3.6.4. **Handling a Request.** Employees and members of the public will see signage and explanatory guidance at the locations where recordings are made that directs them to the appropriate contact to receive formal requests. Such requests should be directed to Headteacher

3.7. Equipment not managed by the Organisation

3.7.1. **Shared or leased premises.** There may be instances of buildings where our employees are based where surveillance equipment is not directly controlled by us. Some of these buildings are used by the public to access our services. Any equipment present in such circumstances is not managed by us and responsibility under Data Protection law therefore falls to the organisation in charge and they are the Data

Controller. Such organisations should have in place the same provisions as described in this document including basic signage providing a contact point for queries and access requests. We have a responsibility to have appointed employees who will have limited responsibility for or oversight of the building and who are aware of the partner organisation's provisions for surveillance recordings and can redirect enquires to the appropriate contact.

3.7.2. **Security Contractors.** Private companies may undertake surveillance recording and data handling on our behalf. Where this occurs, we have a responsibility to ensure that personal data is being managed according to the provisions in this policy or where there is any difference in practice, this is recorded, explained and noted in the policy.

4. Advice and Support

4.1. If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact A member of the senior management on 01206 570231

5. Breach Statement

5.1. A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Annex A: Surveillance Equipment Impact Assessment Forms

5A. Surveillance Equipment Impact As:

Annex B: Surveillance Equipment Register

5DB. CCTV Register.xlsx

Annex C: Recordings Access Log

5DC. Recordings Access Log.xlsx

Annex D: Subject Access Request Forms

Data Subjects:

5DA. Access Request Form - DS.dc

Investigators (e.g. The Police):

5DB. Access Request Form - INV v2.docx