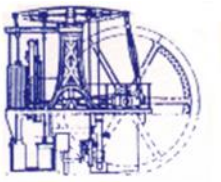
Witham First District IDB

Upper Witham IDB



Witham Third District

North East Lindsey

www.witham3idb.gov.uk

**CCTV Policy**

| | |
|---|---|
| **Background** | This policy provides a framework for the planning, installation, management and maintenance of Closed-Circuit Television (CCTV) systems on sites owned or occupied by Witham and Humber Drainage Boards where there is a building management responsibility. |
| **Statement** | It aims to ensure that appropriate legal requirements are satisfied at each of the above stages and that staff involved in the management and operation of such systems have the necessary information to ensure that they discharge their responsibilities in accordance with the appropriate legislation |
| **Responsibility** | |
| **Dissemination** | Board website |
| **Approval Date** | |
| **Version** | V1 December 2019 |
| **Review Date** | 3 yearly or as and when required |

## 1. Introduction

This policy provides a framework for the planning, installation, management and maintenance of Closed-Circuit Television (CCTV) systems on sites owned or occupied by Witham and Humber Drainage Boards where there is a building management responsibility.

It aims to ensure that appropriate legal requirements are satisfied at each of the above stages and that staff involved in the management and operation of such systems have the necessary information to ensure that they discharge their responsibilities in accordance with the appropriate legislation.

## 2. Aims and Objectives

CCTV surveillance has become a common feature of our daily lives. Whilst the use of CCTV continues to enjoy general public support, it necessarily involves intrusion into the lives of ordinary individuals in the course of their day to day business. The public expect CCTV to be used responsibly with effective safeguards in place.

The Boards operates a number of CCTV systems, within Head office, depots, on its vehicles and machinery as well as wildlife cameras positioned in areas of interest. It is clear that these systems can assist in the prevention, detection and deterrence of crime, the apprehension and prosecution of offenders, and to provide assurance to staff, particularly those who work alone or are required to work during the hours of darkness.

It is essential that the Boards use CCTV in a manner that complies with the law and continues to enjoy the support of staff, visitors and the public.

**3. Legal Requirements**

CCTV systems consist of devices which view and record images of individuals, vehicles, machinery and wildlife. They also cover other information derived from those images that relate to individuals (for example vehicle registration marks). Therefore the use of CCTV systems is covered by UK Data Protection Legislation, with guidance provided by codes of practice issued by the Information Commissioner's Office (ICO).

UK Data Protection Legislation not only creates obligations for organisations, it also gives individuals rights, such as the right to gain access to their details, and to claim compensation when they suffer damage as a result of misuse of data.

The basic legal requirements are to comply with UK Data Protection Legislation and the nine Data Protection Principles, thereby ensuring that:

- Those capturing images of individuals comply with the UK Data Protection Legislation;
- The images captured are usable; AND
- Reassurance is available to those whose images are being captured.
- The current CCTV Code of Practice can be obtained from ICO at www.ico.gov.uk.
- As The Board's CCTV systems are operated on, or behalf of, a public authority, The Boards also needs 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 one's "private and family life, his home and his correspondence"). This will include assurance that:
- The system is established on a proper legal basis and operated in accordance with the law.
- The system is necessary to address a pressing need, such as public safety, crime prevention or national security.
- It is justified in the circumstances.
- It is 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.

Covert activities of the law enforcement community are covered by *The Regulation of Investigatory Powers Act, 2000* (RIPA). Covert surveillance can only be authorised by the policy, security services, or other agencies empowered by the act. Advice on covert surveillance should be sought from the Local Counter Fraud Specialist (LCFS) or Local Security Management Specialist (LSMS).

*The Freedom of Information Act, 2000* allows the disclosure of information held by public authorities under certain circumstances; however, data obtained from CCTV systems should only be disclosed, if the disclosure does not breach the Data Protection Principles (DPP).

**4. Definitions**

The following definitions are used throughout this policy:

**Approved** – Formal confirmation that this document meets the required standards

**CCTV** – Closed-Circuit Television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. CCTV systems may use digital or analogue technology, or a mixture of both, and include digital video recorders (DVR), or other media to provide permanent storage.

**Stakeholder** – An individual or Board with an interest in the subject of the document

**Surveillance** – The monitoring of the behaviour, activities, or other changing information, usually of people, for the purposes of influencing, managing, directing, or protecting.

**4.1. Intended Users**

Within this policy, where it states "all employees", the definition of which applies to all the employees and Board Members.

**5. Responsibilities**

- Ensuring that all individual CCTV Systems are registered with the ICO;
- Ensuring that each individual system is managed by a named member of staff with the appropriate level of authority;
- Act as the data controller for all of the Board's CCTV systems;
- Delegate the duties of data controller to the named manager for each discrete CCTV system;
- Advise appropriate staff on all Data protection Act issues relating to CCTV systems;
- Provide advice to authorising senior managers to enable them to make informed decisions on authorisation;
- Take part in the planning and authorisation process for all new CCTV systems;
- Commission periodic audits of CCTV systems to ensure that they remain compliant;
- Investigate any breach of information security in relation to the Boards' CCTV systems.
- Ensuring the physical security of the system to ensure that only authorised persons have access to data;
- Ensuring that data requests from law enforcement agencies are referred to the Chief Executive at the earliest opportunity;
- Reporting all faults in the system;
- Ensuring that each system is serviced at least annually.

- Routinely inspecting CCTV systems to ensure that they remain DPA compliant;

- Providing an operational requirement for a new CCTV systems in-line with guidance produced by the Home Office, *HOSDB CCTV Operational Requirements Manual, 2009*;

- Providing an operational requirement for all existing CCTV systems where all upgrades or modifications are carried out;

- Measuring progress against the operational requirement on all new works and upgrades;

- Provide assistance and advice on the use of CCTV images following incidents;

- Ensuring the CCTV systems have a maintenance and management contract in place.

The **Line Managers** have a responsibility to ensure that the policy is implemented within their area and that their teams are aware of the policy and have received appropriate training where necessary. Risk assessments should be raised and managed by senior management, and it is their responsibility to seek advice where appropriate.

All **Members of Staff** are accountable for their professional practice and hold individual responsibility to be aware of and read policies appropriate to their roles, and others where necessary. They should be aware and comply with their responsibilities within the individual policies of the Boards.

**6. Planning new CCTV Schemes**

CCTV systems are intrusive and the decision to install CCTV must be informed by a thorough assessment of the requirements and issues the system is intended to address. All schemes should be assessed on the impact of people's privacy.

collectively consider the following issues:

- Who will take responsibility for the system and images under the Data Protection Act?

- What is the purpose of the system, and what problems it is meant to address?

- What are the benefits to be gained from its use?

- Can CCTV technology realistically deliver these benefits?

- Can less privacy-intrusive solutions, such as improved lighting, achieve the same objective?

- Is there a need for images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?

- Will the system deliver the desired benefits now, and remain suitable in the future?

- What future demands may arise for wider use of images, and how will these be

addressed?

- What are the views of those who will be under surveillance?

- What can be done to minimise intrusion for those who may be monitored?

If justification is found for the new system, a statement of overall security need is required. Once a system is agreed, it must be authorised by the Chief Executive.

Key stakeholders should ensure that the system is procured and installed in accordance with the operational requirement.

**7. Management of CCTV Schemes**

It is good practice to appoint a existing staff member to act as a local building manager to ensure that CCTV systems they control operate efficiently, effectively and are maintained to ensure that they continue to meet the operational requirements for the system. Managers of CCTV systems should ensure the following:

- Appropriate signs are prominently displayed on the site to ensure that visitors are aware that they are subject to CCTV surveillance. Signs should be clearly visible and readable, contain details of the organisation, the purpose of the system, and who to contact about the scheme (a telephone number should be sufficient);

- All faults should be reported immediately;

- A deputy should be appointed to ensure that the system continues to be managed in the absence of the manager. The deputy will require appropriate training.

- All staff required to monitor or operate the system are given appropriate training, including periodic training on the Data Protection Act.

- Written local procedures are available for each system. These should include details of those authorised to export data from the system, a plan of all camera locations with camera numbers, manufactures user guides for digital recording devices, and fault reporting procedures;

- An incident report is submitted for any incident involving CCTV system.

If appropriate, Digital cameras by cable or wireless. This recording device must be secure and only accessible to those authorised to access the data stored on the device and analogue CCTV systems will have a recording device which is connected to all.

A retention time of 31 days is accepted to be a reasonable period to retain data. Digital systems will overwrite data based upon the settings programmed into the recorder; however, retention times may be

influenced by other restrictions imposed upon the system such as picture quality and image compression. This should be considered when planning and maintaining a system.

Recording devices should have an appropriate media drive to enable the exporting of images to portable media such as DVD. A supply of write-only DVDs should be available with every recording device.

System monitoring screens must be secured and only visible to those authorised to view images. Where the images relate to public areas which are generally accessible and the images merely mirror what can be seen by individuals present in that area there is unlikely to be a problem if a monitor showing these images can be seen by those using the premises, however, images from restricted areas should not be visible to the public.

New and established CCTV schemes should only be modified following a thorough review and planning process. This will ensure that the scheme remains DPA compliant. The following are examples of actions that may affect the legal status of a system:

- Changing the field and direction of view of cameras;
- Placing cameras in inappropriate areas, such as toilets, bathroom areas, changing rooms, and any other area where higher levels of privacy expected.
- Using systems for covert surveillance without authority.

**8. Image Security and Processing**

CCTV systems produce images which must be secured at all times. Recording devices, media, and monitors should be secured appropriate. CCTV systems are installed to provide better security and should therefore be used both proactively and reactively to achieve the aims that were intended when the system was installed. This means that images should be available to appropriate, authorised staff and to the law enforcement authorities.

Some members of the Board's staff who have access to passive monitoring using approved, installed monitors should be able to view images from appropriate cameras. This may include networked CCTV systems using Internet Protocol (IP).

CCTV systems may be used proactively following incidents and can assist with the investigation process; however, any request to view recorded data must be made through the local data controller for the system concerned and where necessary advice should be sought from (insert). Images can only be used for a purpose for which the system was intended. This would cover potential criminal or disciplinary investigations but would not necessarily cover issues of civil liability between individuals such as damage only traffic accidents on the Boards property.

Law enforcement agencies routinely request access to appropriate CCTV images when dealing with potential criminal offences. These investigations can be initiated by the Boards, members of staff, or people unconnected with Boards business.

The Police have a right to request access to such information under the Data Protection Act, provided they can show that the information will be used for the prevention and detection of crime, or the apprehension or prosecution of offenders. Data provided must pertain to the investigation.

Where requests are made by the Police, they should be referred to the Chief executive who should consider the reasonableness of the requests and arrange a time with the Police to export the data requested from the recording device on the production of a formal *Section 29, Data Protection Act* form. If the Chief Executive has any doubts about the request, professional advice should be sought before images are provided.

Most requests from the Police can be dealt with during normal working hours, although there may be occasions where urgent access is sought, particularly when dealing with serious crimes. The Boards' premises should have an emergency procedure to consider such requests incorporated in the local CCTV procedure.

On every occasion that the Police request to view or copy images, an incident report must be raised, and the Police must sign the *Access to View or Copy CCTV Images* (Appendix C). The form must also be signed by the staff member facilitating the copying of the data. The Chief Executive should be informed of the incident and review each individual request. The completed access form should be stored securely.

The Police and others legitimately requesting access to images should only be given copies of the original data. Copies should be made onto portable media, such as write-only DVDs and handed over against a signature. Images should not be sent by email or other networked systems. The Police will usually provide their own portable media storage devices.

There may be very rare occasions when the Police require the original recording device, or the hard disk drives from the device. This may be necessary to safeguard forensic data following a serious incident. Chief Executive should not release recording devices or hard disk drives unless the Police produce a warrant.

Images should only be viewed in a room or area which is secure and allows access only to those authorised to view the data. This requirement should be considered when planning and installing CCTV systems. Special care must be taken at location where there are multiple monitors as it is possible that images replayed on one monitor in a secure room, may also be visible on other monitors on the site which may not be secure.

All media containing CCTV images must be treated as confidential waste if disposal is required. It should be noted that images should only be retained for as long as is necessary to achieve their purpose. Digital media stored on recording devices will be overwritten and VHS tapes, where used, will be recorded over as required by the Data Protection Principles. Data exported from recording devices must be strictly controlled and destroyed when no longer required.

**9. Breaches of Policy**

Misuse of CCTV equipment and unauthorised processing of data may be criminal offences under the Data Protection Act.

**10. Complaints**

Any complaints received concerning CCTV systems should be handled in accordance to the *Complaints Policy*

**11. Training**

Appropriate members of staff are given adequate training to enable them to operate installed CCTV equipment.

Details of all trained personnel and their responsibilities shall be recorded in local procedures.

Suitable training shall be provided by contractors for all new CCTV systems. Where an existing system is subject to a maintenance agreement, this shall include appropriate training for designated staff.

**12. Monitoring Compliance**

Appointed managers are responsible for monitoring compliance with this policy and shall monitor overall compliance for all of the Board's CCTV systems.

**13. References**

This policy was created with reference to the following:

- *CCTV Code of Practice* - published by the Information Commissioner's Office
- *CCTV Operational Requirements Manual, 2009*
- *Data Protection Act, 1998*
- *Freedom of Information Act, 2000*
- *Maintenance of CCTV surveillance systems – code of practice, 2008* - published by the British Security Industry Association
- The Boards' *Policy* (at time of initial Policy creation)
- *Equality Act 2010*