Closed Circuit Television (CCTV) Policy

Ref: 1301

The Pioneer Group

1. Policy Aim

This policy sets out how we will operate and manage the CCTV system designed to promote public confidence by ensuring that all public area CCTV systems which are linked to the CCTV Control Room are operated in a manner that will ensure their effectiveness and preserve the civil liberty of law abiding citizens at all times. This Policy and associated CCTV Code of Practice will assist the Pioneer Group to comply with our legal obligations under the Data Protection Act 2018.
The operation of CCTV service aims to:

- Assist in the prevention and detection of offences
- Reduce both the real and perceived level of crime
- Improve confidence in the rule of law
- Assist in the apprehension and prosecution of offenders
- Gather evidence by a fair and accountable method
- Create a safer community, improving the quality of life for all by:
- Creating a safe environment
- Deterring public disorder, harassment and anti-social behaviour
- Assisting with environmental management
- Monitoring the movement of people in emergency situations, e.g. evacuation

2. Scope

The CCTV scheme comprises of cameras which have been sited in specific locations across Castle Vale and are controlled, monitored and recorded at a dedicated CCTV Control Room. As the Pioneer Group expands into new areas, CCTV may be deployed in these area. The cameras have been sited to capture images which are relevant to the purposes for which the scheme has been established.

This policy does not apply to stand-alone CCTV systems which may be in use in other parts of the Pioneer Group, which will have their own separate monitoring and management arrangements.

3. Related Documentation

Data Protection Act 2018

The CCTV scheme is registered with the Information Commissioner's Office (ICO). The scheme will be managed in accordance with the Data Protection Act 2018 and specifically the General Data Protection Regulation (GDPR).

Human Rights Act 1998

The scheme and those connected with it acknowledges the provisions within the Human Rights Act 1998 and its impact on issues relating to the use of CCTV. The scheme is considered necessary for the purposes already outlined and to fulfil the requirements of legislation. The system will be used proportionally, legally and remain accountable.

Criminal Procedures and Investigations Act 1996

The Criminal Procedures and Investigations Act 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the prosecution of its own case (known as unused material) but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by Section 7 of the Data Protection Act 1998 (known as subject access).

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 came into force on 2nd October 2000. It places a requirement on public authorities listed in Schedule 1; Part 1 of the act to authorise certain types of covert surveillance during planned investigations.

Private Security Industry Act 2001

The Private Security Industry Act 2001 outlines a system for the statutory regulation of the private security industry. It creates the offence of engaging in conduct for which a licence is required when not in possession of the appropriate licence, which includes public space surveillance (CCTV) under contract. While those employees of The Pioneer Group that operate and manage the CCTV system are 'in house' and therefore not subject to a licensing requirement, we have voluntarily elected to train and licence them to the same level as if they were contracted staff.

4. Compliance

Regulatory background: Information Commissioners CCTV Code of Practice

In order to support the requirements of the CCTV policy and associated Code of Practice, the CCTV system has been registered with the Information Commissioners Office (ICO). This CCTV policy outlines the overarching CCTV principles applied in the management and delivery of the CCTV service. This policy must be read in conjunction with CCTV Codes of Practice and the CCTV Procedure manual. Both the CCTV Code of practice and CCTV procedure manual have been put in place by the Information Commissioners Office as guidance to ensure compliance with relevant legislation during its operation. More specific and detailed information about how the CCTV service is managed can be found in the CCTV Code of Practice and CCTV Procedure Manual.

5. Background/Context

The basic legal requirement for this policy is to ensure that we comply with the Data Protection Act. However there are other legal obligations that must be met in operating public space CCTV. There are four main areas of law that relate to the CCTV policy. They are, the Data Protection Act 2018 (DPA), the Human Right Act 1998 (HRA), the Criminal Procedures and Investigations Act (CPI), and the Regulation of Investigatory Power Act 2000 (RIPA).

6. Policy Detail

6.1 Changes to the CCTV Code of Practice

The policy will be reviewed every three years to ensure that it is effective and promotes best practice. However, a review will be carried out sooner should there be any changes to statutory and regulatory requirements or if any significant risks are identified as part of any audit.

6.2 CCTV Signage

We will ensure that there are CCTV signs that comply with the CCTV Code of Practice prominently placed at the entrances to the Castle Vale Estate. In addition to this, we may place signs within the estate where areas are covered by CCTV. All signs will display the organisation operating the system along with a contact number.

6.3 Control Room Access

Access to the monitoring area will be strictly controlled and the security of the Control Room shall be maintained at all times. Only those persons with a legitimate purpose will be permitted access to the Control Room. The duty controller in the absence of the Control Room Manager (The CCTV and Estates Manager or Senior Caretaker) is authorised to determine who has access to the monitoring area. This will normally be:

- Operating staff
- Our management and authorised personnel
- Police officers requiring to view images of a particular incident in an official capacity, or collecting/returning media being considered for intelligence or evidential purposes. Liaison visits are encouraged and will take place by prior appointment.
- Engineers and cleaning staff (who will receive supervision throughout their visit)
- Independent Inspectors appointed under this Code of Practice may visit the control room without prior appointment
- Organised visits by authorised persons in controlled circumstances

All visitors to the monitoring area, including Police Officers, will be required to sign a visitors log and a declaration of confidentiality.

6.4 Observation and Recording of Incidents

Recording will be throughout the 24 hour period in 'real time. The system will be proactively monitored between the hours of 08:00 – 19:00 by the duty controller. In the event of an incident the operators will concentrate on the scene and gather evidence to assist in further investigations. This will then be passed on to the relevant authorities adhering to the requirement of the Data Protection Act 2018.

6.5 Management of Recorded Material

CCTV recorded images will be retained for a period of 28 days, following which they shall be automatically deleted. On occasions images may need to be retained for longer periods, as a requirement of an investigation into crime. While images are retained, access to and security of the images will be controlled in accordance with the requirements of the Data Protection Act 2018.

6.6 Records and Documentation

To ensure compliance with the Data Protection Act 2018, comprehensive and accurate records and documentation will be maintained. Access to the control room, or reviewing of CCTV footage and including the completion of administrative documents, and internal audits will be recorded. To ensure the effective management of access to data obtained within the control room, each operator will maintain a log of any event or occurrence including change of operator, the state of the recording equipment and incidents including details of time, date, location, name of operator dealing and action taken.

6.7 Viewing recorded Images

Viewing of recorded images will take place in a restricted area. Other employees will not be allowed to have access to that area when viewing is taking place.

6.8 Removal of Medium for Viewing

The removal of medium on which images are recorded, for viewing purposes, will be documented in accordance with Data Protection principles and the procedural manual.

6.9 Access to data: Privacy and disclosure

Cameras must not be used to infringe an individual's right of privacy. The cameras are generally sited where they will not be capable of viewing inside any residential property. If it is found that there is a possibility of intrusion into private areas, CCTV Operators are trained to recognise privacy issues relating to such areas and agree to adhere to this principle. In addition, the use of privacy filters will be considered for any CCTV camera where a risk of privacy intrusion cannot be mitigated. All CCTV Operators must be able to recognise a request for access to recorded images by a data subject and be aware of individual's rights under the relevant section of the CCTV Code of Practice.

6.10 Access to data by Third Parties

Access to images by third parties will only be allowed in limited and prescribed circumstances. In the case of the CCTV scheme, disclosure will be limited to the following:-

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- Prosecution agencies
- Legal representatives or insurers acting on behalf of a Data Subject
- The media, where it is assessed by the Police 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 assessment the wishes of the victim of an incident should be taken into account.
- The people whose images have been recorded and retained (Data Subject), unless disclosure to an individual would prejudice the criminal enquiries or criminal proceedings.
- Those other authorised bodies registered with the Information Commissioner

6.11 Accountability

The CCTV and Estates Manager or designated supervisor will provide periodic progress reports on the scheme. The manager/supervisor will resolve technical and operational matters. Failure of the operators to comply with the procedures and code of practice should be addressed by the manager/supervisor. Person(s) misusing the system could be subject to disciplinary or legal proceedings.

The manager/supervisor will accept prime responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He/she has day-to-day responsibility for the management of the Control Room and for enforcing the disciplinary policy. Any breach of the Code of Practice, or of any aspect of confidentiality, will be dealt with in accordance with our policy and procedures. Staff must recognise that any such breach may amount to gross misconduct, which could lead to dismissal.

7. Data Protection Statement

7.1 Data Protection

CCTV surveillance has become a common feature of daily life. Members of the public are recorded on numerous CCTV cameras as they move around the estate, visiting shops and offices, and travelling on the road and other parts of the public transport network. Whilst the use of CCTV service continues to enjoy general public support, it necessarily involves recording imagery on the lives of ordinary individuals as they go about their day to day business. This means we have a number of important legal obligations as all public and private organisations are legally obliged to protect any personal information they hold. Members of the public expect it to be used responsibly with effective safeguards in place. Maintaining public trust and confidence in the use of CCTV is essential to ensure it is not viewed with suspicion as part of a surveillance society.

We manage the data referred to in this policy in accordance with the Data Protection Act 2018. Further information can be found in our privacy statement at https://www.pioneergroup.org.uk/privacy-policy/