Culture and Communities Committee

10am Tuesday, 29 January 2019

Closed Circuit Television (CCTV) Code of Practice

Item number	8.4
Report number	
Executive/routine	
Wards	All
Council Commitments	51

Executive Summary

This report presents a Code of Practice for the Council's CCTV scheme; setting out the overarching principles, procedures, roles, and responsibilities governing all CCTV systems operated by the Council. The Council's CCTV scheme consists of a network of cameras owned and/or administered by the Council.

Report

CCTV Code of Practice

1. Recommendations

1.1 To agree the Council's CCTV Code of Practice attached at Appendix 1.

1.2 To refer this report and the accompanying Code of Practice to the Corporate Policy and Strategy Committee for its approval on 26 February 2019.

2. Background

2.1 The Council operates a CCTV camera estate across public spaces including housing blocks, the transport network, and Council buildings. Provision of CCTV services is non-statutory, and the service is provided to support public safety and security, including the prevention and detection of crime.

2.2 An internal audit review of CCTV infrastructure conducted in 2017/18, included a recommendation for the creation of a corporate plan for CCTV to ensure that all CCTV operations across the Council are managed efficiently, consistently, and are legislatively compliant.

3. Main report

3.1 A CCTV Working Group was created in January 2018 to take forward the internal audit's recommendations and a Policy and Procedures sub group was established to produce a citywide Council Code of Practice for CCTV. The document is attached at Appendix 1.

3.2 The Policy and Procedures sub group was chaired by an elected member and supported by representatives from different service areas including public space CCTV, housing, transport, building security, fleet services, and information governance. The group reviewed existing CCTV procedures, with each service area completing a Privacy Impact Assessment and liaising with the Information Governance Unit to identify gaps and areas for improvement. This exercise informed the development of a single, overarching CCTV Code of Practice for all service areas.

3.3 The Code of Practice applies across all Council operated, managed, and owned CCTV, and to support compliance, a suite of templates and staff operational guidelines are being developed which will be adapted to suit the specific needs of each service area. This additional documentation will embed legislative and

General Data Protection Regulation (GDPR) compliance and promote best practice across the Council's CCTV operations.

3.4 The Policy and Procedures sub group met every two months and reported its progress to the parent CCTV Working Group, which approved the Code of Practice on 11 January 2019. Once approved by this Committee and agreed at the Corporate Policy and Strategy Committee on 26 February 2019, the Code of Practice will be published on the Council's website.

3.5 In January 2019, the Policy and Procedures sub group will be replaced by an internal CCTV officers group which will oversee the development of the Code of Practice supporting documentation across the service areas. The officers group will report to the CCTV Working Group which will assume responsibility for governance; monitoring compliance under the Code of Practice and conducting an annual review of the document to ensure it remains fits for purpose and changes are made where required.

3.6 The CCTV Working Group aspires to meet the 'gold standard' for CCTV, and it is the intention that the CCTV officers group work towards obtaining Surveillance Camera Commissioner (SCC) certification from a relevant United Kingdom Accreditation Service (UKAS) accredited body.

4. Measures of success

4.1 All Council CCTV services adhere to the CCTV Code of Practice and promote best practice across CCTV operations.

4.2 To strive for continuous improvement across CCTV services and work towards obtaining SCC certification from a relevant UKAS accredited body as mentioned at 3.6 above.

5. Financial impact

5.1 The CCTV Code of Practice has been developed using existing resources from across service areas. Compliance with the Code of Practice will be supported within established governance structures and through existing budgets.

6. Risk, policy, compliance and governance impact

6.1 The internal audit highlighted that an overarching Code of Practice should be developed to support legislative compliance for the use of CCTV across the Council. To comply with the audit recommendations, the Code of Practice attached at Appendix 1 has been developed. There is a risk of both operational inconsistency across service areas and of non-compliance with legislation and GDPR if the Council does not adopt and adhere to the Code of Practice.

7. Equalities impact

7.1 The CCTV Code of Practice sets out the overarching principles which apply to the CCTV scheme owned and administered by the Council and ensures that its operation is fair and non-discriminatory, legal, and compliant with relevant legislation and GDPR.

8. Sustainability impact

8.1 All CCTV services will be operating under one overarching Code of Practice which supports both consistency across the service areas, and clarity in compliance.

9. Consultation and engagement

9.1 The Policy and Procedures sub group was supported by representatives across the service areas who contributed to the development of the Code of Practice. Additionally, members of the CCTV Working Group were invited to submit feedback on the Code of Practice prior to the Group's meeting on 11 January 2019, at which the document was discussed and subsequently approved.

10. Background reading/external references

10.1 None.

Alistair Gaw

Executive Director for Communities and Families

Contact: Rona Fraser, Senior Manager, Community Justice

E-mail: rona.fraser@edinburgh.gov.uk | Tel: 0131 529 3517

11. Appendices

11.1 CCTV Code of Practice.

Appendix 1

City of Edinburgh Council CCTV Code of Practice

1. Introduction

This Code of Practice (COP) applies to the City of Edinburgh Council's (Council's) closed circuit television surveillance scheme. The Scheme consists of a network of cameras which are owned and administered by the Council.

The COP sets out how CCTV cameras operated under the Council's CCTV Scheme will be operated. It defines roles and responsibilities in relation to the Scheme's ongoing and fair operation, and also how requests for information from CCTV should be handled.

All CCTV systems operated by the Council must comply with the principles and procedures set out within this document.

2. Legal Framework

The following legislation is relevant to the Council's operation of CCTV.

2.1 General Data Protection Regulation

CCTV will capture personal data and is therefore required to operate in compliance with the General Data Protection Regulation (GDPR). GDPR places certain obligations upon organisations to ensure that personal data is captured fairly, lawfully, and handled in accordance with data subject rights. All CCTV systems operated by the Council must comply with data protection principles.

The Council is registered with the UK Information Commissioner, and the use and management of CCTV is recorded within the Council's Record of Processing. General advice on data protection, including access to information, can be provided by the Information Governance Unit (IGU).

2.2 Data Protection Act 2018

The Data Protection Act 2018 (DPA) provides certain restrictions to GDPR and also governs how personal data must be handled for law enforcement purposes.

General advice on data protection, including access to information, can be provided by the Information Governance Unit (IGU).

2.3 Human Rights Act 1998

The European Convention on Human Rights, Article 8 (the right to respect for private and family life) provides that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The purpose of a CCTV system, and any impact that might have on a person's human rights, must be considered prior to the system being operated. In particular, if a CCTV system is likely to interfere with someone's private and family life, the Council must be clear that the purpose falls within one of the factors noted as necessary for a democratic society.

2.4 Criminal Procedure (Scotland) Act 1995

The Criminal Procedure (Scotland) Act 1995 introduced a statutory framework for the disclosure of material to defendants of material which the prosecution would not intend to use in the prosecution of its own case (known as unused material).

Where CCTV material is required for this purpose, it will normally be requested via Police Scotland as part of their initial criminal investigation and may then be disclosed by them through the court process.

2.5 Freedom of Information (Scotland) Act 2002

The Freedom of Information (Scotland) Act 2002 (FOISA) provides a right of access to information held by a public authority. The right of access will apply to information captured via CCTV although it is likely that exemptions relating to personal data will apply in some cases.

All FOI requests should be referred to and managed by the Information Governance Unit.

2.6 Regulation of Investigatory Powers (Scotland) Act 2000

The Regulation of Investigatory Powers (Scotland) Act 2000 requires public authorities listed in Schedule 1: Part 1 of the act to authorise certain types of directed surveillance during planned investigations.

Only certain nominated Council officers are allowed to authorise directed surveillance.

3. Definitions

3.1 CCTV Scheme shall mean the totality of the arrangements for closed circuit television in the CCTV areas covered by the Council's CCTV and listed at 5.2, and is not limited to the technological system, staff and operational procedures.

3.2 CCTV system means the surveillance items including cameras and associated equipment for monitoring, transmission and controlling purposes, for use in a defined area. The term will also encompass the capability for effectively capturing data, in any medium, so it can be viewed or processed.

3.3 Central Monitoring Facility (CMF) or CCTV Monitoring Suite refers to the secure area where public space CCTV is monitored and where data from public space CCTV can be retrieved, reviewed and processed. This area is staffed 24/7, 365 days a year and will also be the first point of contact for telephone enquiries from the public and for the collection and analysis of public space CCTV by designated Council and police officers.

3.4 Controller determines the purposes and means of processing personal data. A controller can act either alone or jointly with others.

3.5 Data shall mean all information generated by the system.

3.6 Incident is an activity that raises concern which requires the CCTV system to be reviewed/checked in a targeted way. Incidents will normally be a concern for the safety or security of an individual or property, a suspected criminal offence which is about to take place, is taking place or has taken place, or any occurrence that requires the attention of, or warrants specific action by, the operator.

3.7 Owner is the City of Edinburgh Council (the Council), the organisation with overall responsibility for the formulation and implementation of policies, purposes and control over the scheme.

3.8 Personal data is any information relating to an identified or identifiable natural person ("data subject"). Images of people captured on CCTV is personal data because individuals can be identified from their appearance.

3.9 Recorded material means any medium that has the capacity to store data and from which data can later be recovered irrespective of time elapsed since its generation. It can also include a hard copy print which records an image or images that already exist on recorded electronic material**.**

3.10 Special Category data is personal data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. It is recognised that CCTV images may include special category data in respect that that information which can be seen through images of the data subject. The most obvious of these is racial or ethnic origin in circumstances where this can be observed, or, dependent on the nature of the event being recorded, may include political opinions, religious belief or sexual orientation. However, guidance from the ICO suggests that an image on its own should not normally be considered to include special category personal data. Special category data will only be involved where any other information collected confirms the special category information depicted in the picture, or the special category data is specifically processed in a targeted way e.g. CCTV operators asked to identify the location of male suspect in the Meadows using a wheelchair.

4. Roles and Responsibilities

4.1 Senior Information Risk Owner (SIRO) has delegated authority through the Corporate Leadership Team with specific responsibility for information risk and mitigation, ensuring that any information threats and breaches are identified, assessed and effectively managed. The Head of Strategy is the Council's SIRO.

4.2 Information Asset Owners are Heads of Service. They are responsible for ensuring that data and information processed by their service is done in accordance with the law, Council policy, and procedure. This will include CCTV systems operated in their service area.

4.3 CCTV Working Group is formed of CCTV System Managers. It provides a forum through which the strategic approach to the CCTV Scheme can be monitored and revised as necessary.

4.4 System Manager has responsibility for the implementation of the policies, purposes and control of a specific CCTV system operated within the Council's CCTV Scheme. They are responsible for ensuring that the CCTV system is operated in accordance with the law, Council policy, and procedure; and that documentation to support the use of CCTV is routinely reviewed and kept up to date.

4.5 Operators are employees of the City of Edinburgh Council that operate the CCTV network. They will have access to CCTV in order to fulfil their role and may be required to access the system and produce evidence where it is required for the management of incidents. Operators will normally undergo a Criminal Records check and achieve Security Industry Accreditation where required.

5. The Scheme

5.1 Data Controller

The Council is the Controller of all CCTV systems included within the scope of the CCTV Scheme.

5.2 Scope

The Council's CCTV Scheme includes the following CCTV systems:

- Public space CCTV cameras (cameras located at static external locations)
- Mobile CCTV (re-deployable cameras which can be moved to new locations as required)
- Mobile CCTV van
- CCTV (security of schools, hostel accommodation, and other Council owned buildings)
- CCTV (designated housing e.g. high-rise blocks)
- Fleet services CCTV (bin lorries)
- Transport (traffic management)
- Cameras operated by the Council out with Edinburgh e.g. Park & Rides

5.3 Purpose

The Council operates the CCTV Scheme in order to support the performance of public tasks carried out in the public interest. This processing falls within Article 6 (e) of GDPR.

CCTV cameras operated under the Scheme will only be installed where a primary purpose, listed below is met.

Primary purpose(s)
Maintaining public order and reducing anti-social behaviour
Deterring and preventing crime, particularly violent crime
Reducing the fear of crime
Protecting property
Assisting crowd control for live events such as demonstrations, protests, major public events
Facilitate monitoring and management of the transport networks.

As a result of the Council operative CCTV systems, it is recognised that recorded material can also be used for certain secondary purposes because it is available.

Secondary purpose(s)
Supporting legal proceedings

Providing assistance with issues relating to public safety and health
Contributing to the location of vulnerable / missing individuals
Providing assistance and reassurance to the public in emergency situations

5.4 Principles of CCTV Operation

The Council's CCTV Scheme will be operated in accordance with the following principles.

5.4.1 We will only use CCTV for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

5.4.2 We will always take into account its effect on individuals and their privacy.

5.4.3 We will be as transparent as possible regarding our use of CCTV, including publishing information about how to make a complaint.

5.4.4 All CCTV systems will be operated in accordance with documented procedures in which responsibilities will be clear, and these are effectively communicated to all relevant employees.

5.4.5 CCTV images will not be stored for longer than is necessary.

5.4.6 All CCTV will be appropriately secured to safeguard against unauthorised access or use.

5.4.7 All CCTV systems will have effective and routine review and audit mechanisms to ensure legal requirements, policies and standards are complied with.

5.4.8 CCTV will be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in pursuit of a legitimate aim.

5.4.9 CCTV systems will be accurate and kept up to date to ensure that they meet their legitimate aim, and appropriate evidential value can be achieved as necessary.

6. Documentation and Signage

The following documentation will be in place to support use of CCTV systems within the Council.

6.1 Code of Practice

The Council's CCTV Scheme will be operated in accordance with an agreed Code of Practice. This sets out the framework, principles and required documentation for the operation of CCTV systems within the Scheme. The Code of Practice is owned by the CCTV Working Group and is reviewed on an annual basis to ensure it remains relevant and fit for purpose.

6.2 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment will be completed for all CCTV systems within the Council to ensure that systems comply with data protection principles.

6.3 Operating Guidelines

All CCTV systems must have documented operating guidelines which provide practical information on how CCTV is to be used in each area. These should include, as necessary, roles and responsibilities for each system, assessments and processes to be carried out for new siting of cameras, training for operators, procedures for use and review of cameras, partnership arrangements (as required), and processes for retention and access to CCTV.

Operating guidelines should be routinely reviewed to ensure they remain relevant and fit for purpose.

6.4 System Inventory

All CCTV systems must be supported by documentation recording specific camera specification, siting, purpose, and justification. This inventory must be routinely reviewed to ensure it remains accurate, and that the purpose and justification of the use of each camera remains valid and fair.

6.5 Signage

The presence of CCTV cameras will be indicated by clear signage which indicate the organisation responsible for the CCTV system, the purposes of the CCTV, and contact details for questions and complaints.

7. Retention

Information captured by CCTV systems will be retained in accordance with the Council's Record Retention Schedule.

8. Access Requests and Management

Requests for access to CCTV should be handled in accordance with Council policy and procedure indicated below. Specific procedures to support access requests to specific systems should be documented within relevant operating guidelines.

All requests to access CCTV should be documented.

8.1 Requests from organisations

Information from CCTV systems may be requested by external organisations for a variety of reasons. Most commonly, the Council will receive requests for CCTV footage from the police when they are investigating crime, or from partner organisations for the purpose of investigating an incident.

Operating guidelines must include detail on how such requests should be handled. Unless alternative arrangements have been approved, all requests for personal data, including those made by the police for crime investigation purposes, should be referred through the Information Governance Unit to ensure compliance with data protection principles.

8.2 Requests from, or on behalf of, individuals

Individuals have statutory rights to access information held by the Council, this includes footage captured by CCTV systems. Individuals can access personal data about themselves under data protection legislation, and more general information, including environmental information, held by the Council under freedom of information legislation.

Individuals can exercise these rights on their own, or ask others to act for them e.g. solicitors, insurers etc.

In accordance with Council policy, these requests must be forwarded to the Information Governance Unit for processing.

8.3 Internal requests (from within the Council)

CCTV systems should only be used in accordance with the purposes set out in this document and the system's relevant operating guidelines. Where requests are received for access to CCTV from within the Council, the purpose for the access should be assessed in accordance with the systems purposes and normal access procedures.

If the request falls out with the system's standard business process, and the primary purpose(s) of the CCTV system, advice should be sought from the relevant System Manager and the Information Governance Unit if necessary.