CCTV Policy and Operating Procedure

Policy

Document Number	CORP 30/16
Responsible Officer	Chief Executive
Contact Officer	
Approval	Governance & Strategic Planning Committee
Effective Date	1 May 2017 - tbc
Modifications	n/a
Superseded Documents	N/a
Review Date	3 years or where there is a change in legislation or operational requirements.
File Number	
Associated Documents	Appendix 1 – Privacy Impact Assessment Screening Questions Appendix 2 – Privacy Impact Assessment Template Appendix 3 – Form 1 Central Register Appendix 4 – Form 2 Requests Received to View CCTV Images Appendix 5 – Form 3 Record of Maintenance Appendix 6 – Form 4 Declaration of Compliance Appendix 7 – Form 5 Record of Images Released Appendix 8 – Form 6 Individual Subject Access Request Appendix 9 – Form 7 PSNI Request Form

1 Preamble

1.1 Purpose

This policy sets out how Derry City and Strabane District Council uses closed-circuit television (CCTV) in the operation of its functions. It is designed to ensure that personal data consisting of the images of people captured by CCTV systems (data subjects) is processed fairly in terms of the Council's obligations as a data controller under the Data Protection Act 1998, the Local Government Act (Northern Ireland) 2014, the Regulation of Investigatory Powers Act 2000 and in terms of article 8 of the European Convention on Human Rights. The policy is also designed to comply with the CCTV Code of practice issued by the Information Commissioner's Office in 2014 and should be read alongside Derry City and Strabane District Council's Data Protection Policy.

1.2 Background

Derry City and Strabane District Council uses CCTV cameras in Council premises including offices, leisure and community centres, amenity sites and other outdoor venues (with the exception of Council outdoor events, which are controlled on behalf of Council by the City Centre Initiative). The cameras are used to record, store and process images of staff and service users. The CCTV system consists of:

- Fixed exterior and interior cameras situated on Council property, which continually record activities;
- Public space cameras, which are used only during special events;
- Temporary public space cameras, which are used from time to time to monitor indiscriminate littering and dog fouling occurrences;
- Body worn video cameras, which are activated from time to time by Council enforcement staff operating in public areas;
- Cameras which record Council meetings for broadcasting on the Council's website.
- Vehicle mounted cameras.

2 Scope

This policy applies to all Council departments and to the services they provide.

3 Definitions

3.1 CCTV or closed circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors.

3.2 Data controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data (including CCTV images) are, or are to be, processed.

3.3 CCTV manager is the person who is responsible to the Head of Service / Lead Officer for the day-to-day management and use of CCTV systems in their service.

4 Policy Statement

Derry City and Strabane District Council is committed to operating its CCTV systems in compliance with the relevant legislation and with the guidance issued by the Information Commissioner's Office.

4.1 Roles and Responsibilities

4.1.1 The overall responsibility for implementing Derry City and Strabane District Council's Data Protection Code of Practice as it relates to CCTV rests with the Chief Executive.

4.1.2 Each Director is responsible for managing the Council's CCTV network within their own particular facilities/areas. Heads of Service/Lead Officers act as the Data Controller for their service and are responsible for carrying out Privacy Impact Assessments on the use of CCTV in their services (see 5.2.10 below).

4.1.3 The Council's Data Controller is responsible for the management of centralised CCTV records, for providing advice and support as required and for liaising with the Information Commissioner's Office when required.

4.1.4 Responsibility for the day-to-day management and use of authorised CCTV systems is delegated to appropriately designated local CCTV managers in conjunction with the responsible Director, Head of Service or Lead Officer.

4.1.5 Staff who are authorised to have access to the CCTV system are required at all times to comply with the Council policy and procedures governing its use.

4.1.6 Staff who are not authorised to use the CCTV system must not attempt to access or view images or system records.

4.2 General Principals

Privacy Notice and System Usage

4.2.1 Through the use of its CCTV systems, the Council collects images of service users, members of the public, Elected Members and staff for the following purposes:-

- To enhance the safety and well-being of staff and the public (particularly children and adults at risk of harm) using Council premises and services;
- To prevent, investigate and detect crime and to assist with the apprehension and prosecution of offenders;
- To discourage anti-social behaviour including dog fouling and littering;
- To assist with insurance claims, investigations and the overall management and supervision of Council buildings, premises and events;
- To facilitate disciplinary investigations where criminal activity or breaches of health, safety and wellbeing of staff and facility users may have taken place;
- To enable citizens to view Council meetings in real time and historically via the internet.

4.2.2 The CCTV system will only be used for the purposes indicated above.

4.2.3 Images obtained from CCTV systems are normally automatically overwritten at intervals ranging from 14 to 31 days, dependent on the type of equipment in use at each location (with the exception of Council meeting webcasts which are available for two years), unless they are needed for investigation purposes. It is necessary to hold images for this duration due to the time lapse between an incident/accident taking place and notification of this being received by the Council. Where recorded images are needed for investigation purposes they will be held for the minimum period necessary to carry out the investigation and will be destroyed following this (see Retention of Images below).

4.2.4 Viewing of live images on monitors should be restricted to those authorised to view them, for example to monitor congestion for health and safety purposes. Control units for the display of CCTV images should therefore be situated in restricted areas where they are not visible to members of the public, unless the monitors display scenes which are in plain sight of the public.

4.2.5 Images collected by CCTV systems may be shared with other organisations or individuals for the purposes of law enforcement, investigation of incidents/civil claims, or to comply with subject access requests. All disclosure of personal information will be in compliance with the Data Protection Act 1998 and the Data Sharing Code of Practice issued by the Information Commissioner's Office. Where images are obtained of persons committing acts of an illegal nature and/or acts which breach any byelaws, rules or regulations, these images may be used as evidence.

4.2.6 Images may also be disclosed for the purposes of internal investigations, subject to the purposes set out in paragraph 4.2.1.

4.2.7 Individuals have the right of access to personal data that the Council holds about them, including CCTV images, and this right can be exercised by making a subject access request (see section on Access and Disclosure below) to the Data Controller for the service.

4.2.8 Signs must be displayed to identify all areas subject to CCTV surveillance and the signs should be clearly visible and legible to members of the public, Elected Members and staff. The signs must indicate the purpose for which cameras are installed and the contact details for Derry City and Strabane District Council as the organisation responsible for the CCTV system.

4.2.9 Cameras must be sited in such a way that they only monitor locations intended to be covered. They will not be used to look into private property.

4.2.10 Concealed cameras will only be used in very exceptional circumstances and in strict accordance with the Regulation of Investigatory Powers Act 2000, where there is reasonable cause to suspect that illegal activities are taking place or about to take place, or in instances of potentially serious breaches of Council policy.

Approval and Documentation

4.2.11 All CCTV installations require mandatory screening to ensure that the processing of personal data in this way is justified. The Information Commissioner's Office Guidance on screening is contained in Appendix 1.

4.2.12 Screening will be signed off by Heads of Service/Lead Officers. Where screening identifies the need for a Privacy Impact Assessment to be undertaken, it will be the responsibility of the appropriate Head of Service/Lead Officer to ensure that this is completed using the template issued by the Information Commissioner's Office contained in Appendix 2.

4.2.13 Notwithstanding 4.2.11 above, Privacy Impact Screening / Assessments are required to be in place and documented for all CCTV installations throughout the Council. Where no existing Privacy Impact Screening/ Assessments are in place, these must be carried out using the questions / template issued by the Information Commissioners Office contained in Appendices 1 & 2. Following this, existing Privacy Impact Assessments will be reviewed annually to establish whether the continued use of CCTV is justified.

4.2.14 Privacy Impact Screenings and where necessary Assessments must be carried out for all proposed new installations of CCTV.

4.2.15 When a Privacy Impact Assessment has been signed off by the Head of Service/Lead Officer, reviewed by the Director and approved by the relevant Council Committee, the Head of Service/Lead Officer should forward it to the Council's Data Controller, along with details of the CCTV scheme.

4.2.16 A central register will be maintained listing the locations where CCTV cameras are sited and the purposes for which the systems have been installed (CCTV Form 1). Any new installations of CCTV or revised locations, including body worn or temporary cameras, should be notified to the Council's Data Controller so that the appropriate records can be updated. Each part of the system must fully comply with the provisions of this Code of Practice.

4.2.17 Requests from individuals and statutory bodies such as law enforcement agencies to view CCTV images and the outcomes of such requests should be recorded on CCTV Form 2. System repairs or re-siting of cameras should be recorded on CCTV Form 3. Those authorised to view images must provide a signature agreeing to abide by this Code of Practice (CCTV Form 4).

4.2.18 Records must be kept of CCTV images released (see Processing Images below).

Maintenance of Cameras and Equipment

4.2.19 Heads of Service/Lead Officers are responsible for ensuring that adequate maintenance arrangements are in place for the CCTV equipment used in their service area and they should ensure that the equipment is protected against vandalism, remains in good working order and is repaired promptly when damaged. This is essential to ensure that images required for evidential purposes are of good quality.

4.2.20 Maintenance logs should be kept and completed when maintenance work is carried out on any Council CCTV equipment (CCTV Form 3). All maintenance contractors' visits will be by arrangement.

Processing Images

4.2.21 It is important that access to and disclosure of images is restricted and carefully controlled, not only to safeguard the rights of individuals but also to ensure that evidence remains intact should the images be required for evidential purposes.

4.2.22 Directors, Heads of Service and Lead Officers must ensure that:

- access is restricted to those staff who need to have access to recorded images for the purpose(s) for which the system was installed and where appropriate, external statutory agencies;
- images are viewed by authorised staff in a secure and confidential location;
- downloaded and saved images from body worn video or temporary cameras are only viewed in the event of an incident having taken place which needs to be investigated - if no such incidents have taken place the images should be deleted after 31 days;

- those authorised to view images are issued with a copy of the Code of Practice and sign a declaration that they fully understand their obligations to adhere to its conditions;
- in emergency/out of office hours situations the Duty Officer in charge of Council premises may authorise requests by PSNI officers to view CCTV images at monitoring stations;
- if recorded images are released, a CCTV log (CCTV Form 5) is maintained at each location to record this. The logs should include a description of the images, the purpose for which they were released and the secure location where they are stored. Two copies of each incident should be made, one for retention by the Council and one for the requesting person/organisation.

Access and Disclosure

4.2.23 Derry City and Strabane District Council's Data Protection Policy covers arrangements for access to CCTV images. As the operator of the CCTV system, Derry City and Strabane District Council has discretion to refuse any request for information unless there is an overriding legal obligation such as a court order, or information access rights exist such as subject access requests and freedom of information requests.

Requests from Individuals for Disclosure of CCTV Images

4.2.24 Under the Data Protection Act 1998 an individual has the right of access to personal data held in relation to them which includes CCTV images. In this case they can make a subject access request to view the data and to be provided with a copy of the images. This must be provided within 40 calendar days of the Council receiving a request. In these circumstances a judgment must be made as to whether disclosure of the images will impede crime prevention and detection. If this is the case, the information held about the requester is exempt from disclosure.

4.2.25 If information requested also contains images of a third party, a judgment should be made as to whether providing these images would involve an unfair intrusion into the third party's privacy or cause unwarranted harm or distress. If this is not the case, the images can be released, however it may be necessary to disguise or blur images of the third party to protect their privacy. If it is considered necessary to anonymise footage of third parties, this will be carried out on behalf of the Council by a sub-contracted processor that guarantees security of images and privacy. Subject access requests from individuals should be made using CCTV Form 6. There is a fee of £10 payable in this case.

4.2.26 Where an individual requests CCTV images of themselves under the Freedom of Information Act (FOI), this information is exempt from the Act and the request should be treated as a data protection subject access request. If the images requested under the FOI are those of other people, they can only be disclosed if this does not breach the data protection principles. If individuals can be identified from the CCTV images, this is personal information about them and it is unlikely that this information can be disclosed, as it may be unfair processing in contravention of the Data Protection Act.

Requests from Outside Bodies for Disclosure of CCTV Images

4.2.27 Requests for the disclosure of images may come from the Police Service of Northern Ireland (or other law enforcement agencies such as the Department for Work and Pensions - Benefit Fraud Section). If not disclosing the information requested would be likely to prejudice any attempt by the police to prevent crime or catch a suspect, the information may be released. Requests for disclosure of images from the PSNI should be made using CCTV Form 7 or using the PSNI's Personal Data Request form.

4.2.28 Where the Council decides to disclose personal data to external agencies, this will be done in compliance with the Data Protection Act 1998 and the Data Sharing Code of Practice issued by the Information Commissioner's Office. Where a request for recorded images is received from solicitors, they must sign an undertaking that they will adhere to this Code of Practice and return the images to the Council for erasing once no longer required in any legal proceedings.

Disclosure Records

4.2.29 Records of each decision made about the disclosure or non-disclosure of personal information and the reasons for the decision should be maintained using CCTV Form 2. Copies of these forms should be forwarded on a monthly basis to the Information Management Section.

4.2.30 All staff queries or issues concerning CCTV should be directed to the Data Controller for their service. Staff who receive subject access requests from the public should provide the person making the request with the relevant form and direct them to the relevant Data Controller for the service.

4.2.31 All subject access requests will be dealt with by the Data Controller for the relevant service in consultation with the appropriate Director and local CCTV manager.

Duties of Staff Who Have Access to CCTV Systems

4.2.32 All staff with access to the Council's CCTV systems must keep personal data secure and not disclose it to anyone without the approval of the Council. Under Section 55 of the Data Protection Act 1998 there is an offence, which is defined as:

'A person must not knowingly or recklessly, without the consent of the data controller, obtain or disclose personal data or the information contained in personal data, or procure the disclosure to another person of the information contained in the personal data.'

4.2.33 Staff operating the Council's CCTV systems are required to sign CCTV Form 3 to document their agreement to conform with this Code of Practice.

Retention Of Images

4.2.34 The CCTV system operates in such a way that information recorded is automatically overwritten after intervals ranging from 14 to 31 days (dependent on the type of equipment in use at each location). Recordings of Council meetings however are available on the Council website for 2 years and will be held for historical purposes for 6 years before being erased.

4.2.35 If images need to be retained for any of the other reasons set out in 5.2.1 (above) they will be retained on a suitable media device and this will be recorded on a CCTV log (see Processing Images above).

4.2.36 Recorded images for use by Derry City and Strabane District Council will be kept for the minimum period necessary, i.e. until closure in the event of an investigation, in accordance with the Council's Retention and Disposal Schedule and then destroyed or erased. This should be recorded on the relevant CCTV log (see Processing Images above).

4.2.37 Where a law enforcement body is investigating a crime, images may need to be retained for longer. At the conclusion of a prosecution the images will be retained by the relevant agency until the end of a custodial sentence or for six months following a non-custodial sentence. The images will then be returned to the Council and destroyed/erased.

5. Legal & Policy Framework

This policy sets out to ensure that the Council complies with the legislation outlined in **Section 1.1 Purpose** (above) and with the CCTV Code of Practice issued by the Information Commissioner's Office in 2014.

5.1 Linkage to Corporate Plan

5.1.1 This policy contributes to the achievement of two of the Council's strategic objectives:

 Provide effective and facilitative cross functional support services; Protect our environment and deliver physical regeneration.

6. Impact Assessment

6.1 Screening and Equality Impact Assessment

This policy has been screened out for equality impact assessment.

6.2 Impact on Staff and Financial Resources

There will be no impact on staff and financial resources as a result of this policy.

6.3 Sustainable Development

There will be no sustainable development impact as a result of this policy.

7. Implementation

The Democratic Services and Improvement Unit is responsible for the implementation of this policy.

7.1 Support and Advice

Support and advice will be provided through the Policy and Information Management Section.

7.2 Guidelines and Forms

All required guidance and forms are provided in the appendices to this policy:

Appendix 1 – Privacy Impact Assessment Screening Questions
Appendix 2 – Privacy Impact Assessment Template
Appendix 3 – Form 1 Central Register
Appendix 4 – Form 2 Requests Received to View CCTV Images
Appendix 5 – Form 3 Record of Maintenance
Appendix 6 – Form 4 Declaration of Compliance
Appendix 7 – Form 5 Record of Images Released
Appendix 8 – Form 6 Individual Subject Access Request
Appendix 9 – Form 7 PSNI Request Form

7.3 Communication Strategy

All staff and Elected Members will be provided with a copy of this policy and any necessary training will be provided for those with responsibility to implement it.

7.4 Risk Management

Failure to comply with this policy could increase the risk of the Council failing to comply with legislation and with the Information Commissioner's Office

procedures for data protection. This could result in financial penalties and reputational damage for the Council.

8. Monitoring, Review and Evaluation

8.1 This CCTV Code of Practice will be reviewed every three years, or earlier in the event of changes to legislation.

8.2 Privacy Impact Assessments will be reviewed annually, to establish whether the continued use of CCTV is still justified and proportionate, or whether a less privacy intrusive method could be used.

Appendix 1 – Privacy Impact Assessment Screening Questions

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Will the project require you to contact individuals in ways that they may find intrusive?

Appendix 2 – Privacy Impact Assessment Template

Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of	Responsibility for action

	actions	

Contact point for future privacy concerns