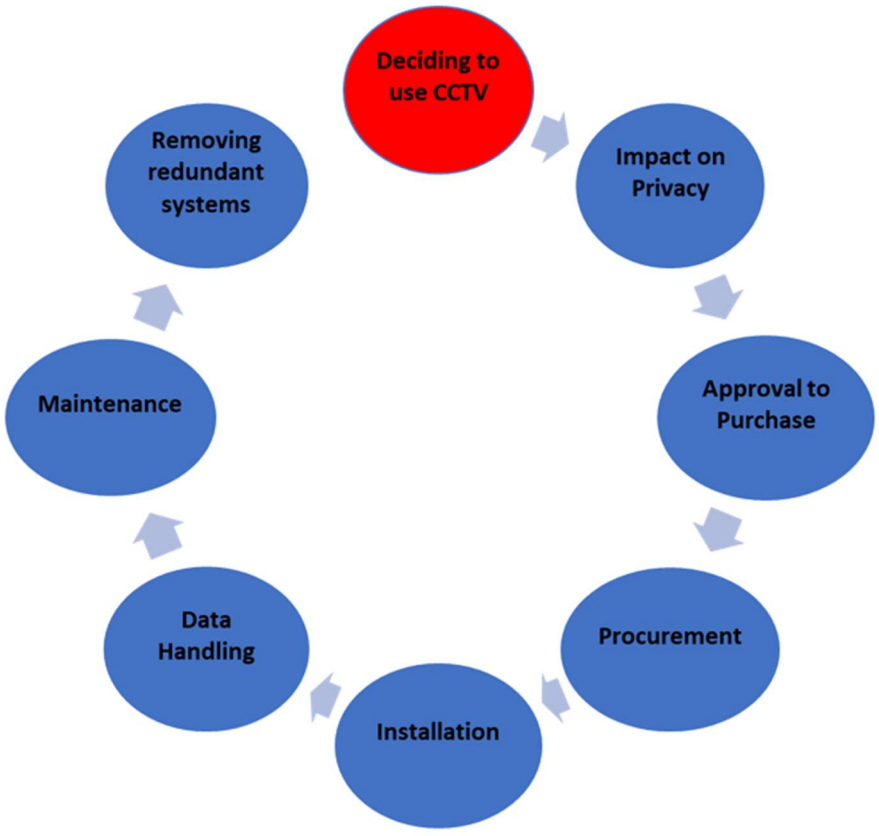
Fermanagh & Omagh
District Council
Comhairle Ceantair
Fhear Manach agus na hÓmaí

Surveillance Camera Systems Protocol

2023 – 2026



For Fermanagh and Omagh District Council and for organisations working on behalf of the Council or on Council premises

Surveillance Camera Systems Protocol

Document Control			
Protocol Owner	Head of Corporate and Strategic Services Head of Parks, Estates and Property		
Version	1.0		
Consultation	Senior Management Team ICT Manager Trade Unions		
Approved By	SMT	**Date**	19 April 2023
Review Date	April 2026		
Circulation	Councillors, Staff, Contractors (where relevant)		
Document Linkages	*Data Protection Policy* *Access to Information Policy*		

Contents

1. Introduction

1.1 Context

Our vision for Fermanagh and Omagh is of a welcoming, shared and inclusive district, where people and places are healthy, safe, connected and prosperous; and where our outstanding natural, built and cultural heritage is cherished and sustainably managed. One of the three key outcomes we aim to achieve is that 'Our communities are inclusive, safe, resilient and empowered'

Fermanagh and Omagh District Council (FODC) supports peoples' entitlement to go about their lawful business in safety, and the Council is committed to respecting people's rights to privacy.

To achieve this, FODC may choose to use technology, such as surveillance camera systems, to ensure that members of the public and FODC employees can conduct their business in safety. The public must have confidence that the use of surveillance systems is lawful, fair, proportionate, transparent and meets the other standards set in data protection law.

The balance between a legitimate purpose and privacy is at the heart of any consideration to install a surveillance camera system. Deciding on whether it is necessary, its purpose, why and how data is collected, accessed and, if necessary shared with other parties e.g. the Police Service of Northern Ireland (PSNI).

The operation of surveillance camera systems will necessarily evolve as the role of FODC, as a public body, evolves to fulfil its statutory purposes. This guidance reflects the technical capabilities of closed-circuit television (CCTV) systems that are available at this current time. FODC is cognisant of the developments in the technical capabilities, where more sensitive categories of personal data can be processed e.g. artificial intelligence-based surveillance systems, and other new technologies which emerge that may become available to public bodies to ensure public safety, rights and security, and so on.

Effective implementation of this protocol will ensure that FODC manages all surveillance camera systems in accordance with all relevant legislation and Council policies at all stages of the 'CCTV cycle' (see page 9) . FODC has identified this cycle as one which starts with the decision to install a surveillance camera system, consideration of privacy impacts, approval, procurement, installation, signage, storage, disposal and access to images, and finally, removal of systems where they are no longer needed to fulfil their original purpose.

This protocol, in the main, also applies to systems covering the town centre surveillance cameras in Enniskillen and Omagh. As surveillance camera systems installed in a town centre will capture images from a public place, they are deemed high risk, and so as well as a Data Protection Impact Assessment (DPIA), they require Information Commissioner's Office (ICO) approval. It would also have to be installed in discussion with the Police Service of Northern Ireland (PSNI) and other third parties. This will be captured in a standard operating procedure for town centre cameras, which will also cover the different processes for accessing images.

Over the next few years, FODC will need to transition all surveillance camera systems from analogue to digital.

1.2 What are 'surveillance camera systems'?

The Information Commissioner's Office (ICO) refers to the definition in Section 29 of the Protection of Freedoms Act 2012 (PoFA), which states that "surveillance camera systems" mean:

(a) closed-circuit television or automatic number plate recognition systems;

(b) any other systems for recording or viewing visual images for surveillance purposes;

(c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or

(d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).

Surveillance systems can be used to record the activities of individuals, often in high definition and with ease. As such, these systems can capture information about identifiable individuals and how they behave. This is personal data under data protection law.

Surveillance camera systems can include:

- Fixed exterior and interior CCTV cameras on Council owned buildings and facilities;
- Public space including town centre CCTV cameras;
- Temporary/re-deployable/mobile CCTV cameras in public spaces and vehicles which may be used to monitor littering, dog fouling or vandalism;
- In-vehicle all round vison cameras and dash cams;
- Body Worn Video (BWV) which may be used by Council enforcement staff;
- Unmanned aerial vehicle/drone;
- Facial Recognition Technology; and
- Smart doorbells.

For the purposes of this protocol, all of the above systems will now be referred to as 'CCTV' or 'CCTV systems.' This includes CCTV systems which are operated by:-

- FODC,
- Organisations operating on behalf of FODC, and
- Organisations operating on FODC premises.

1.3 Why does FODC use CCTV systems?

CCTV systems, including when and where they are located, are just one tool which can help FODC to achieve the following:-

- Enhancing the safety and well-being of staff and the public using Council premises, services, and town centres.
- Protecting Council property and assets and ensure Health and Safety obligations are met.
- Preventing, detecting, investigating, and reporting crime and to assist with the apprehension and prosecution of offenders, and to discourage anti-social behaviour.
- Assisting with investigation and processing of insurance claims, investigations and the overall management and supervision of Council buildings, premises, and events.
- Assisting with the preparation for, and conduct of, internal or external disciplinary investigations and hearings including those involving alleged or suspected criminal activity and/or breaches of Council policies in relation to the health, safety or wellbeing of employees, subcontractors, and the public generally.

1.4 Legal Context

In operating CCTV systems, the Council must comply with the following:-

- **The Data Protection Act 2018**: Fermanagh and Omagh District Council will treat CCTV systems, and images obtained and used as data, in accordance with the Data Protection Legislation. For any use of CCTV systems, a lawful basis must be identified under Article 6 of the UK GDPR[1]. As it is difficult to obtain genuine consent from individuals for processing their personal data in public spaces, it is likely the appropriate lawful basis will be either legitimate interests[2], or a task conducted in the public interest.
- **The Human Rights Act 1998**: Public authorities must comply with the rules laid down by the Human Rights Act. The main article relating to CCTV is Article 8: The Right to Respect for Private and Family Life. People have a degree of expectation to privacy, even in public places like High Streets. However, an organisation also has rights and is fully entitled to protect its property. A balance needs to be struck between the rights of the organisation and individuals.
- **The Freedom of Information Act 2000**: The FOI Act gives a general right of access to all types of recorded information held by the Council. It also sets out exemptions from that right.

[1] (a)the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b)processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c)processing is necessary for compliance with a legal obligation to which the controller is subject;
(d)processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e)processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f)processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

[2] A wide range of interests may be legitimate interests. They can be one's own interests or the interests of third parties, and commercial interests as well as wider societal benefits. The UK GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.

- **The Regulation of Investigatory Powers Act 2000** (when applicable). The Regulation of Investigatory Powers Act 2000, or 'RIPA' as it is commonly known, governs the use of covert surveillance by public bodies. The Council (see section 2.2) does currently not use covert surveillance systems.

The guidance is also in line with best practice, in particular:-

- The Information Commissioner's Code of Practice "In the Picture: A data protection code of practice for surveillance cameras and personal information"

1.5 Aim of this Protocol

The aim of this protocol is to regulate the installation, management, operation, use and data collection of CCTV systems.

1.6 Audience

This protocol and associated appendices are primarily aimed at FODC employees, to assist them in following the correct procedures when working with CCTV systems. In this way, the implementation of the protocol will ensure that FODC is following both legal requirements and best practice in the use of CCTV, which in turn protects the public's rights.

Those contracted to provide CCTV services should also be made aware of this protocol.

At each stage of this guidance, links are provided to the relevant forms which need to be completed at the different stages of the CCTV cycle. This will help staff to demonstrate an audit trail of decision making and subsequent actions taken.

2. Purposes

2.1 When can CCTV system be installed?

CCTV systems can be installed in Council premises for a number of purposes, including to:

- Increase, the safety of staff, customers and the public in and around Council premises;
- Safeguard employees during their employment;
- Safeguard members of the public;
- Protect Council buildings and assets;
- Assist in the prevention and detection of crime and anti-social behaviour;
- Assist with the identification, apprehension and prosecution of offenders;
- Gather evidence by a fair and accountable method;
- Assist in staff disciplinary, grievance, formal complaints and Health & Safety investigations following an incident or formal complaint;
- Comply with agreed Health and Safety obligations; and
- Assist with insurance claims.

Having the equipment is not important, the **purpose** is vital – equipment shouldn't be installed just because it can be, it should only be placed where there is a clear purpose for it.

2.2 When can CCTV systems not be installed?

Cameras will not be used to monitor the progress of staff or individuals in the ordinary course of lawful business. Managers are not permitted to use the cameras to observe staff working practices or time keeping or to assist them in the day-to-day management of their staff. Individuals will only be monitored if there is reasonable cause to suspect a criminal offence or breach of discipline or to investigate specific ongoing incidents.

Recorded material will not be sold or used for commercial purposes or the provision of entertainment.

3. Implementing and maintaining a CCTV System – Key Stages

Implementing a CCTV system requires careful consideration of a number of issues in a series of stages.

Stage 1: Deciding to use CCTV

- **Identification of Need**
- **Specification of Purpose**
- **Technical Compatibility**

Stage 2: Impact on Privacy
Stage 3: Approval to Purchase
Stage 4: Procurement
Stage 5: Installation

- **Location**
- **Signage**
- **Re-deployable CCTV cameras.**

Stage 6: Data Handling

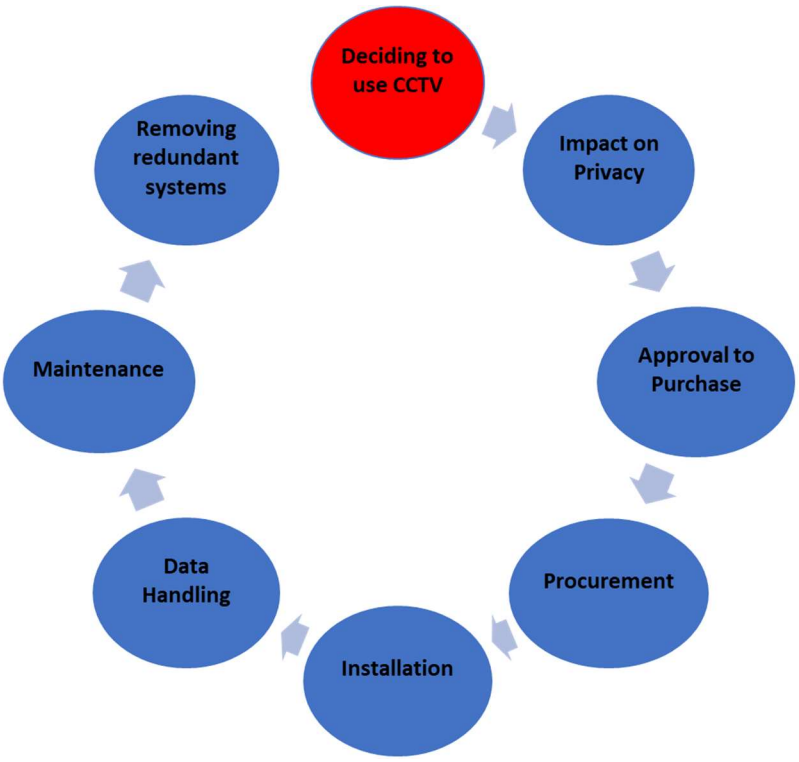
- **Storage**
- **Access**
- **Third Party Requests**
  - **PSNI**
  - **Regulatory and Investigatory Bodies**
  - **Solicitors/Insurance Companies**
  - **Subject Access Requests from individuals**
- **Internal Staff Matters**
- **Pixelation/redaction**
- **Covert/Dummy Cameras**
- **Confidentiality/Security**

- **Retention and Disposal**
- **Breach**

Stage 7: Maintenance

Stage 8: Removing redundant systems

Figure 1: Implementing CCTV System 'Cycle'



A checklist for staff involved at any or all of the stages above is at **Appendix 1**.

3.1 Stage 1 Deciding to Use CCTV

There are three elements of the first stage.

- **Identification of Need:** Council employees must give due consideration to the necessity for cameras, i.e., what is the problem that the CCTV system is trying to resolve? Is CCTV the only possible practical solution? Could a non-technical solution achieve the same outcome?
  Is it a helpful supporting tool which is lawful, necessary and proportionate in the circumstances?

- **Specification of Purpose:** If after looking at all the alternatives it is decided that CCTV is the only suitable solution, a clear purpose must be given for the system and each camera must be identified to justify the use (see section 2.1).

- **Technical Compatibility:** The Information and Communications Technology (ICT) Section and Estates should be involved in the process to ensure any new system can integrate within the existing ICT infrastructure and physical and environmental surroundings.

3.2 Stage 2: Impact on Privacy

At this point, it must be shown that the introduction of a CCTV system is proportionate and necessary. An assessment on the impact on privacy must be conducted if the system is likely to result in high risk to rights and freedoms of individuals, although it is good practice to carry out a Data Protection Impact Assessment (DPIA) anyway.

High risk includes, but is not limited to:-

- processing special category data[3];
- processing publicly accessible places on a large scale; or
- processing individuals at a workplace.

Officers can conduct a simple 'screening' process to determine if a new system requires a full DPIA using the FODC template but please contact the Data Protection Officer for advice if required. It is good practice to keep a record of the responses to this checklist for systems even if they are screened out.

If a full DPIA is required, employees must document this in the DPIA template. Guidance is available on the ICO's website. The Head of Corporate and Strategic Services/Data Protection Officer should be consulted in the process. Where risks cannot be mitigated down to an acceptable level, the ICO will be consulted.

Note: for CCTV systems which do not have a DPIA, retrospective DPIAs can be carried out, and should be done particularly where there is a high risk.

3.3 Stage 3: Approval for purchase and installation

If a new system is to be purchased e.g. for new purpose and location, or an amendment to an existing CCTV system (e.g. if it is to be moved or extended in any substantive way) is to be made, Director level approval will be required through a Business Case and subsequently via the appropriate procurement authorisations. The Business Case must include the detail on the decision making (stage 1) and the impact on privacy (stage 2).

The relevant Director from whom approval should be sought is the Director of the service area seeking to implement the CCTV system.

FODC will be changing out older analogue cameras and recording devices with digital systems over the next few years. Where the same number of cameras are

[3]The UK GDPR defines special category data as personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); health; sex life; and a person's sexual orientation.

fitted in the same locations when transitioning to digital, this will be considered maintenance. Other common maintenance work involves small works such as replacing a faulty camera or recording device. This will also be considered maintenance and not require Director level approval.

Approval for the purchase and installation of new CCTV systems must be obtained from a Director. Where appropriate, staff, Trade Union representatives and other stakeholders should be consulted. This will take place if the system is deemed 'high risk'. For example, this may be because the system is of a considerable size or involves installation of cameras in the workplace or in areas affecting a particular group of people.

As well as the DPIA (where required), the Business Case should include how the system will be paid for, annual costs and so on. A Risk Assessment should be conducted at the stage of the Business Case by the service area planning to install the CCTV system, to ensure the safety of staff and the public.

3.4 Stage 4: Procurement

Staff should refer to the most up to date FODC Procurement Policy and Procedures which are available on the staff hub.

Advice must be sought from the Council's Procurement Team to ensure that the correct procurement procedures are followed.

Staff conducting procurement exercises for new CCTV systems must consult with the ICT department to ensure the technical specifications are correct and met by any contracted supplier.

3.5 Stage 5: Installation

Depending on the purpose of the CCTV system, the following must be considered to ensure the right balance between the overall purpose and people's privacy.

Location

- **What can be seen in the area in which the camera is pointed?** Do screens need to be blanked or camera angles adjusted for privacy concerns? e.g. if one is placed in a corridor outside a changing room, can inside the changing room be seen when the door is opened? What can be seen in the background e.g. private property or playgrounds? If cameras are in an area where staff are working, e.g. reception area, staff need to be informed and they have the right to have their desk/work area blanked out.

- **Are the cameras sufficiently visible?** All cameras should be located in prominent positions within clear view of the public and/or staff. This is so people know the area is covered by CCTV. (See also section on signage below).

CCTV sited in reception areas are intended to provide live feed of reception and other areas within a facility. If monitors can be seen by other employees, access to images should be noted, and staff should be advised of data protection issues. It is the responsibility of the Facility Manager to ensure the ability to view the monitors is restricted to those authorised to do so. All Digital Video Recording (DVR) equipment should be kept in a secure location with access granted to designated employees only.

We have a CCTV Register which includes all CCTV systems across all FODC premises and where they are installed.

When new cameras have been installed, all the relevant details of the system including its location should be added to the CCTV Register which is jointly managed by Corporate and Strategic Services, ICT and Estates.

A copy of a map or building plan showing the location of the CCTV cameras should be held by the relevant manager of the facility.

Signage

All areas where CCTV is in use should be clearly signed to comply with the Data Protection Act, including devices used on vehicles. This is to warn people that they are about to enter an area covered by CCTV cameras or to remind them that they are still in an area covered by CCTV. Signage can function as an additional deterrent if the CCTV has been installed to deter anti-social behaviour or criminal activity. CCTV signs should not be displayed in areas where there is no CCTV.

The sign should display:

- **Why the CCTV cameras are there (the purpose) (see section 2.1)**
- **Who the Data Controller is (Fermanagh and Omagh District Council); and**
- **Contact details for further information.**

The sign should be large enough to enable people to easily read the information. The position of the sign should also be considered to prevent it from being obscured.

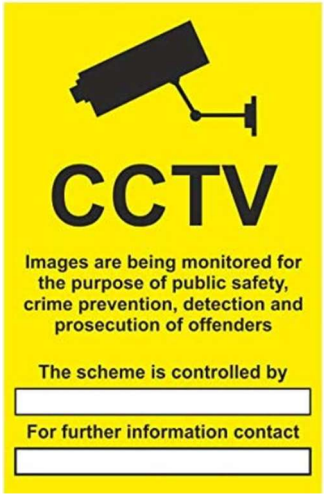
The ICO gives the following example of wording for CCTV signage:

> Where processing is not obvious to an individual, a sign could read "Images are being monitored and recorded for the purposes of crime prevention and public safety. This system is controlled by XXXXX. For more information, visit our website at (web address) or call 01234 567890."

Signage should be checked at least annually to ensure that contact details are up to date and that the signs have not been damaged or obscured. This should be done by the Facility Manager responsible for the system, as listed on the CCTV Register. The manager should make a note on the register that signage is up to date. Any

action required to physically update or replace signage should be initiated by the manager of the facility.

Data Protection Compliant Signage: Example:



For a template of FODC CCTV sign please see Appendix 2.

Re-deployable CCTV cameras

Re-deployable CCTV cameras are cameras which are temporary, and which may move around or between sites, depending on where they are needed.

This protocol applies to re-deployable cameras in the same way as fixed cameras, although additional information is required to cover the unique deployment tasks of this equipment:

- A Risk Assessment of the re-deployment;
- A Data Protection Impact Assessment for each deployment, *where it is considered high risk*;
- Secure anchorage and power supply for the cameras is available; and
- Suitable locations for 'CCTV in operation' signs.

3.6 Stage 6: Data Handling

- Storage
- Access
- Third Party Requests
    - PSNI
    - Regulatory and Investigatory Bodies
    - Solicitors/Insurance Companies
    - Subject Access Requests from individuals
- Internal Staff Matters
- Retrieval of data/images
- Pixelation for purposes of redaction
- Covert/Dummy Cameras

- Confidentiality/Security
- Retention and Disposal
- Breach

Storage

All recorded material should be treated as confidential and should be held in accordance with the FODC Records Retention and Disposal Schedule. **CCTV images should not be retained for longer than necessary.**

Data storage is automatically managed by the CCTV digital recorders which overwrite historical data in chronological order to enhance the storage capabilities. This process produces an approximate minimum of 4 weeks rotation in data retention.

All downloaded footage should be stored either on the R drive or a secure OneDrive account. If footage is stored on a USB, then it should be encrypted (password protected). If the USB is not protected and is lost, then that is a data breach.

Unused images or images awaiting issue will be held in a secure cabinet.

Provided that there is no legitimate reason for retaining the CCTV images (such as for use in legal or disciplinary proceedings), CCTV images will be stored in a secure place with controlled access and erased in line with the Records Retention and Disposal Schedule.

The CCTV Register will be stored in a secure place on the FODC OneDrive (and shared with those members of staff who are required to update it).

Access

CCTV systems should be seen as a system that holds personal information about employees, members of the public, visitors and tenants and will be protected accordingly. Accessing images needs to be controlled so that the rights of individuals are protected, but also to ensure there is an evidence trail should images be required for evidential purposes e.g. a PSNI enquiry or a health and safety investigation.

For data protection requirements, access to the CCTV systems, and images, will be restricted to authorised staff with responsibility for the facility (and listed on the CCTV Register) and for those with specific responsibilities e.g. Corporate and Strategic Service staff with responsibility for information management, ICT or investigating officers for a HR disciplinary.

Requests for access to images recorded on a CCTV system will be granted by Corporate and Strategic Services (via appendix 4).

CSS will keep a record of each time images are viewed and/or downloaded. Under normal circumstances, 2 copies will be downloaded, one on a USB to be released, and one, known as the master copy, to a secure R drive folder.

Any staff member found to be misusing Council CCTV footage/images (e.g. viewing, downloading or distributing footage) without permission will be subject to disciplinary procedures.

Third Party Requests

Images can be shared with other organisations for the purpose of law enforcement, investigation of incidents/claims or to comply with subject access requests. All disclosures must comply with the Data Protection Act 2018.

However, no person or authority has the automatic right to unfettered access to images stored on a CCTV system. Third Parties, as with staff, are not permitted to trawl the Council's CCTV system on the off chance of detecting something.

Images provided to the PSNI, other enforcement agencies or for internal investigations, should at no time be used for anything other than the purposes for which they were originally released.

PSNI

In instances when the PSNI request information held by FODC, the PSNI will usually complete a Form 81 (which outlines the legal basis for the request). However, FODC appreciates under certain exceptional circumstances, e.g. locating missing child/vulnerable adult, it may be necessary to access the CCTV footage immediately.

Regulatory and Investigatory Bodies

Other regulatory bodies may request footage to review or investigate an incident. When requesting footage, a regulatory/investigatory body is required to provide justification to FODC before access to CCTV images will be provided. All regulatory/investigatory bodies should detail the relevant legislation and the relevant section/article which permits disclosure or provides them with an exemption from data protection legislation. If satisfied with the request, CSS will ask ICT to facilitate a viewing of the images and/or a release a copy of the footage.

Solicitor/insurance company

Where FODC receives any request for information connected to legal proceedings or prospective proceedings, we must be assured that the release of this information will be used for this purpose. Therefore, all requests connected to legal action or proceedings must be made via a solicitor's letter or by an Order of Court.

CCTV involvement in insurance claims fall into two categories:

- **Incidents which may result in claims against FODC** When a report is received which may result in a claim, the officer responsible for dealing with the incident should consider whether CCTV covers the area. If it does, they

should put a request through to Corporate and Strategic Services who will work with ICT to download images for that period. This must be done as soon as possible to ensure images are not recorded over. If evidence is issued to the officer dealing with the incident, they become responsible for the security, safety and integrity of the images. All recorded images must be stored in a secure place with access limited only to those people involved in the subsequent claim. Images should be retained and disposed of as per the Records Retention and Disposal Schedule. When images are destroyed a disposal form should be completed. Advice can be provided by Corporate and Strategic Services as required.

- **Claims involving third parties** Members of the public involved in an accident need to contact their insurance company to ask them to write to FODC, giving as much detail as possible.

    - If the incident was not caught or the request arrives after the images have been recorded over, there will be no relevant images and the requester should be informed.
    - If relevant images are found on the recorder, the insurance company solicitor should be informed and asked if they want a copy. The images may then be copied, redacted as necessary through pixelation (see pixelation/redaction), and sent to the relevant person accompanied by a letter reminding them that FODC retains 'copyright' over the images. They must also be reminded that they are then responsible for the security and destruction of the images and that the images may not be used for any other purpose other than the one they were released for. Details of the footage released should be included in the letter and they should be asked to sign one copy of the letter confirming they have received the images, and that they accept the conditions of release. A detailed record of all actions must be maintained. Failure to comply with FODC's conditions of release may result in legal action being taken against the person who signed the acceptance letter.

Subject Access Requests (SAR) from individuals

Anyone can make a request for their own images via a Subject Access Request (see Appendix 3: Subject Access Request Form).

All requests for access to personal information held on a CCTV system will be processed through Corporate and Strategic Services. Once requests have been validated, ICT staff will be tasked with retrieving the images, copying them on to removable media such as a USB, and if necessary, conducting pixelation (see pixelation/redaction).

When approved for release, in most cases FODC will provide the requestor with the information within one month of receipt of the request.

If a request for access is refused (for example due to an ongoing criminal investigation), then a written response detailing the reasons why the request has

been refused will be sent to the requestor no later than one month from receipt of the request.

Once a request has been approved by FODC and images have been released to an individual, FODC is no longer responsible if they are used for a purpose other than that for which it was originally requested.

Internal Staff Matters

CCTV footage may constitute evidence relating to an internal investigation into the conduct of a member of staff.

As part of an internal investigation, Human Resources (HR) will appoint an Investigating Officer. This officer may decide to access and view CCTV footage as part of the investigation.

Images will only be released after the Investigating Officer has submitted a formal request to Corporate and Strategic Services (via Appendix 4: CCTV Image Release / Viewing Request Form). The Investigating Officer will then hold the relevant footage on the R drive in a secure folder relevant to the investigation.

To ensure the images are not lost due to the overwrite period, HR/the Investigating Officer can ask CSS to retain the images until they are required.

Once authorised, arrangements will be made to enable the Investigating Officer to view the images, and if necessary, be issued with two copies of recorded material on suitable media. Note that only the Investigating Officer is permitted to view the images at this stage.

The reason for the second copy is, if it is decided to use CCTV images in an employment related hearing, the person being investigated must be given a copy of the images to permit them and their representatives to mount a defence.

At the end of the hearing all copies of the images are to be collected by HR, held on file and destroyed once the appeals process and any Employment Tribunal processes have been completed.

Staff who are the subject of a Council disciplinary, complaint or grievance procedure have the right to request that footage be retained if they believe it will support their defence. The process will be the same as that shown above for the investigating officer.

The Council will not permit viewings or release images to individuals being investigated internally or externally, which may be handed over to an external agency such as the PSNI or an enforcement agency. The responsibility for investigating and disclosing images to those involved in the investigation are covered by the Police and Criminal Evidence Act (PACE) and the Evidence and Disclosure Act and the prosecuting authorities are required to follow the procedures set out in these Acts. It should be noted that other enforcement agencies will operate under other legislation, but the use of the evidence still rests with them.

Retrieval of data / images:

If you receive a request to view/download CCTV footage, you should forward the request to Corporate and Strategic Services to deal with.

Who retrieves the footage?

- Buildings/facilities – CSS asks ICT to retrieve
- Redeployable/Mobile camera – CSS asks Officer responsible for hardware to remove sd card and forward to ICT
- Dash cams – Enforcement Officers download (CSS does not keep copies but should be informed of all viewings/downloads)
- Refuse vehicle footage – Refuse Managers contact service provider (CSS does not keep copies but should be informed of all viewings/downloads)

Corporate and Strategic Services must be informed each time any camera is accessed to view and/or download footage.

Pixelation/redaction

Images are personal data. As data controller, FODC must redact personal information as needed. Pixelation may be required, depending on who has requested the images. Even if a face is not clear, a person could be identified by mannerisms, clothes, context, this also includes information such as car registration plates.

Where extensive pixelation is required and this requires the use of additional software, this may incur a charge. The requester will be informed of this prior to the process of redaction. More information can be found on the Council website.

Covert Cameras

In the extremely unlikely event that covert cameras are necessary, this requires the written authorisation of the Chief Executive or his/her nominee, following the procedures outlined in The Regulation of Investigatory Powers Act 2000. A Data Protection Impact Assessment should be conducted and the Information Commissioner's Office should be consulted.

For these circumstances to occur, there must be reasonable cause to suspect that unauthorised or illegal activity is taking place, or is about to take place, or that a breach of Council rules is occurring or is about to take place (e.g. breach of health and safety legislation).

Covert monitoring will be undertaken only for a limited and reasonable period consistent with the documented objectives and council must take legal advice before initiating covert surveillance.

All decisions relating to the use of covert surveillance will be fully recorded.

FODC will consult on any approach with the PSNI. Legal opinion will also be sought.

Dummy cameras/signage

The Council does not deploy 'dummy' cameras nor install misleading signage. Displaying signs where dummy cameras, or no cameras, are installed creates a literal false sense of security. Staff, customers and pedestrians may feel safer in areas displaying this signage, incorrectly believing that any criminal activity will be monitored or recorded. Using these signs may cause legal problems, whilst drawing attention to the fact that the CCTV cameras are not real. However, signage may be in place at a location where there is no camera if the camera has been recently vandalised or removed for servicing, in this instance, signage should be removed if the camera will not be replaced.

Neither are officers to purchase cameras that can monitor conversation or be used to talk to individuals as this is seen as an unnecessary invasion of privacy.

Confidentiality/Security

Cameras are to be installed in such a way that they cann**ot** view private spaces, such as houses, gardens, schools, unless they can be fitted with privacy zones which block out private areas so that they cannot be viewed or recorded.

Unless suspicious behaviour is apparent or an immediate response to events is required, staff will not direct cameras at individuals or their property.

Staff who have access to images, and CCTV equipment, will be required to sign a 'Confidentiality Statement,' which prohibits them from downloading images unless requested or letting undesignated staff/the public view images. Once signed, the Confidentiality Statement should be placed in the person's personnel file and CSS will also retain a list of staff who can access footage.

Only designated members of staff should be viewing and/or downloading images. Staff must report instances where they suspect others are viewing or downloading images without the authority to do so.

Retention/Disposal and Copyright

The Council's CCTV systems hold data for varying periods of time before being recorded over, on average 4 weeks.

Downloaded images will be retained for 3 years unless it is known that they are, or could be, subject to a claim/court case.

All images will be disposed of securely when no longer required.

Images that are saved and subsequently destroyed should be listed on a Disposal Form (Appendix 5).

FODC's Retention and Disposal Schedule specifies the time periods and methods of disposal of CCTV images alongside all other Council records.

All images remain the property and copyright of Fermanagh and Omagh District Council. Images should not be reproduced by any individual or organisation without the permission of the appropriate Director.

Breach

Data breaches occur when:

- Footage is viewed without a specific, legitimate purpose and without the required authorisation.
- Cameras, recording equipment or recorded data is tampered with or misused.
- Downloaded data is not held securely and is either accessed and viewed or lost.

A breach could lead to disciplinary action, which may result in dismissal and/or criminal prosecution. It is considered a gross misconduct to unnecessarily invade a person's privacy – to monitor or zoom in on a person, vehicle and place of work/school or residence. Also, casual viewing/trawling of images by anyone is strictly forbidden; viewings must only be undertaken for a specific, legitimate purpose.

The responsibility for guaranteeing the security and proper use of the CCTV system will rest with the Head of Service of the facility of the system concerned, with the help of the manager of the facility.

The Data Protection Officer will investigate all breaches or allegations of breaches of security or misuse. The Council has 72hrs (this includes weekends/evenings) to report a breach of personal information to the ICO which presents a high risk to the rights and freedoms of individuals. If staff become aware of a data breach, they must report it to Council's Data Protection Officer immediately who will decide whether to report it to the ICO and advise the CEO of the Council accordingly.

3.7 Stage 7: Maintenance

The relevant manager of the facility or designated officer must check and confirm the site's CCTV system is functioning correctly, i.e. cameras and recording system are working, times and dates are correct (this particularly needs to be checked in March and October after the time changes), and camera views should be checked regularly to ensure they are not obscured by vandalism, foliage or anything else. If there is an issue, they must contact the relevant service provider so that the system can be serviced and repaired as required. Individual services and building managers will be responsible for the purchase, deployment, and maintenance and management of their own systems. Estates will only be responsible for any systems that are identified as being of their responsibility.

Some systems may need substantial work or replacing, for example if it beyond repair or the technology is obsolete. Other systems may need only minor repairs. It is the responsibility of the manager of the facility, with support from ICT and Estates, to establish if a system needs fully replacing.

3.8 Stage 8: Removing redundant systems

CCTV systems, either temporary or permanent, which no longer fulfil their purpose should be removed, together with any CCTV signage. This may be because the problem the system was installed to help address has been resolved e.g. a temporary camera installed to monitor vandalism has resulted in no more incidents occurring.

Managers of facilities should ensure that CCTV is checked annually in terms of whether it is fit for purpose and request that it is removed if no longer needed.

Anyone who is disposing of equipment, especially the Digital Video Recorder (DVR), needs to ensure this is disposed of properly and that all data bearing images is removed and sent for secure destruction.

All CCTV systems must be listed on the CCTV Register. The register should be reviewed at least annually at the start of the financial year, although we recommend more regular reviews.

4. Roles and Responsibilities

Roles and Responsibilities of relevant staff are set out in the table below

Role	Staff Responsible
Overall responsibility for implementing this protocol	Chief Executive
Responsibility for managing the CCTV systems within their own facilities/areas. Approval of businesses cases for new CCTV systems	Directors
Act as the Data Controller for specific services areas and carrying out Privacy Impact Assessments on the use of CCTV in their services where required. Ensure that CCTV systems within a specific service areas/facilities are secure and working correctly	Heads of Service
Adherence to the implementation of this protocol and procedures; development of training for staff re accessing of footage Approval of request for viewing and downloading CCTV footage	Head of Corporate and Strategic Services Head of Parks, Estates and Property Head of Corporate and Strategic Services
Downloading of CCTV footage	IT Section

Technical advice/issues	
General maintenance issues/purchasing new cameras –	Service provider and Building / asset manager.
Health and Safety advice Risk Assessments for new CCTV systems	Corporate Health and Safety
Authorising access to images, general enquiries, and complaints	Corporate and Strategic Services
Data Protection Impact Assessments	Relevant manager implementing CCTV system Advice from Corporate and Strategic Services
Reporting of data breaches to Council's Data Protection Officer (DPO) Reporting of data breaches as required to the ICO	All staff DPO
Day to day management including checking date/time settings of CCTV systems is accurate, times are correct (particularly after electrical failures. Checking that camera views are not obscured or damaged. Attending training as required	Manager of Facility/Area
Protecting images	All staff
Awareness of data protection issues Awareness that unauthorised staff are not allowed to access, view or download images.	All staff

It is important to note that CCTV systems are subject to inspections by the Information Commissioner's Office or Regulation of Investigatory Powers Commissioner. In addition, systems are subject to inspections by Elected Members, the Chief Executive, the Internal Auditor, the Head of Parks Estates and Property, or the Head of Corporate and Strategic Services, as required. These inspections are purely to ensure the system is running in accordance with legislation and this protocol.

Any employee who is involved with CCTV equipment, in particular accessing and downloading of images, should be aware that they could be asked to attend court by the Public Prosecution Service if a case using Council CCTV images is brought to court.

Appendices

Appendix 1

Checklist for new CCTV systems

Stage 1: Deciding to use CCTV

- The problem you are trying to address has been clearly defined and installing cameras is the best solution.
- You have considered the need for using CCTV and have decided it is required for a specific purpose. It will not be used for other purposes.
- The system is compatible with FODC ICT systems.
- A Risk Assessment has been conducted.
- All of the above is documented in the Business Case required for installing new CCTV systems.

Stage 2: Impact on Privacy

- A Data Privacy Impact Assessment has been conducted for the system, in the case of it being high risk e.g. processing special category data; processing publicly accessible places on a large scale; or processing individuals at a workplace. Where a DPIA has been conducted, and residual risks cannot be mitigated down further, this must be submitted to the Information Commissioner's Office for approval. For further guidance please see the ICO's website on DPIAs.
- The DPIA should be included with the Business Case if it is required.

Stage 3: Approval to Purchase

- Approval for the system has been sought from, and given by, a Director (via the Business Case process and procurement authorisations).

Stage 4: Procurement

- The system has been purchased in line with FODC procurement policy and procedures.
- FODC ICT section has been consulted on the technical specifications required to ensure systems are compatible with existing IT infrastructure.
- A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.

Stage 5: Installation

- There is a named individual who is responsible for the operation of the system.
- Cameras have been positioned to avoid capturing the images of persons not visiting the premises.
- There are visible signs showing that CCTV is in operation, the purpose, who is responsible for the sign and contact details.

- Images from this CCTV system are securely stored, where only a limited number of authorised persons have access to them.

Stage 6: Data Handling

- Recorded images will only be retained for approx. 4 weeks until recorded over.
- Requests for downloading/viewing footage are made using the correct form and submitted to Corporate and Strategic Services who will process the request.

Stage 7: Maintenance

- Regular checks are conducted to ensure that the system is working properly and produces high quality images.
- Management of Service level agreements with providers if applicable.
- Regular, at least annual, review of our use of CCTV, the systems and the register.

Stage 8: Removing redundant systems

- Systems which are technically out of date or no longer needed are removed along with signage.
- All recording devises and material is disposed of securely.

Appendix 2

The sign should be large enough to enable people to easily read the information. Signs should advise:

- Why the CCTV cameras are there (the purpose – see section 2.1). For example:-
    - Ensure the health and safety of members of the public and employees
    - Protect Council property
    - Prevent and detect crime and anti-social behaviour

- Who the Data Controller is (Fermanagh and Omagh District Council); and
- Contact details.

You can use the wording 'Images **may be** recorded for …' but please check with CSS for when this can be used.

Fermanagh & Omagh District Council
Comhairle Ceantair Fhear Manach agus na hÓmaí

Fermanagh and Omagh District Council

Subject Access Request Form

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal information is held about you, the reason(s) why it is being held and who uses that information. You also have a right to a copy of that information. This includes images captured by CCTV.

The Council's Rights

The Council is only required to give you the information you are seeking if it is satisfied as to your identity. We are not required to provide information if someone else can be identified from it, unless that person consents to the disclosure, and we may deny access to personal information where this is allowed by the Act. However, in any event, we will respond to your application within one month of receipt if you have provided us with sufficient information relating to your identity, and to assist us in locating the required information, if any.

If you wish to find out what information, if any, may be held about you then please complete **all relevant sections** on the following application form.

Sections

Sections 1, 2 and 3 require you to give sufficient information about yourself as the Applicant (and the Data Subject if this is a separate person) to help the Council to confirm your identity. We have a duty to ensure that the personal information which we hold is secure, and we must be satisfied that you are who you say you are.
Section 4 requires you to enclose evidence of your identity, by enclosing documents with your application.
Sections 5 and 6 will help us locate the information you have requested.
(Complete Section 5 for non-CCTV requests or Section 6 for CCTV requests.)

Data Protection
In accordance with the Data Protection Act 2018, Fermanagh and Omagh District Council has a duty to protect any information we hold on you. The personal information you provide on this form will only be used for the purpose of dealing with your request and will not be shared with any third party unless law or regulation compels such a disclosure. For further guidance on how we hold your information please visit the Privacy section at www.fermanaghomagh.com/your-council/privacy-statement/

Section 1: Your Details	
Applicant's Full Name (inc. Title)	
Postal Address (inc. Postcode)	
Email Address	
Phone Number (A phone number would be helpful if we need to contact you about your request)	
Preferred method of contact, if required, e.g. phone, email, letter	
Preferred format for receipt of information e.g. view onsite, paper copy, computer disc, email	

Section 2: Verification	
Are you, the Applicant, also the Data Subject? Yes/No If Yes, please proceed to Section 3. If No, please fill in the rest of Section 2.	
Please attach a copy of the authority you have to act on the data subject's behalf. N.B. This request will not be processed unless accompanied by this authority.	
Data Subject's Full Name (inc. Title)	
Postal Address (inc. Postcode)	
Phone No	

Section 3: Data Subject - Additional Personal Details	
Date of birth	
If any data which may be held about the data subject is likely to include a name or address which is different to that given in Section 1 or 2, please give details below:	
Different First Name/Surname/Maiden Name	
Different Postal Address (inc. Postcode)	
For CCTV requests only:	
Gender	
Height	

Section 4: Data Subject - Proof of Identity
To help the Council to establish your identity, please enclose **two** of the following documents which between them, confirm your name, address and date of birth: Medical Card, Birth/Adoption Certificate, Utility Bill, Passport, Driving Licence or any other document bearing the above details. Clear photocopies of documents will be accepted. If requesting CCTV at least one of the two documents must have a recent, full-face photograph.

Section 5: Notification Details (for non-CCTV requests)
The Council holds information in relation to the following areas: Corporate functions, Leisure and Cultural services, Environmental Health, Community Services, Staff Administration (internal purposes only), Financial, Property Services, Customer Services, Public Relations, Registration, Licensing, Animal Welfare, Planning, Other Commercial/Non-commercial purposes. Please identify from the above list from which area(s) you wish to request any personal information which may be held about you:

Section 6: CCTV requests only (please note we will not check or trawl footage)	
Please provide further information which will help to locate the images you are requesting:	
Date	
Time (1 hour period maximum)	
Location	
Description of clothing or any other person with the data subject	
If the request involves a vehicle, property or any other useful information please provide detail	

Section 7: Declaration

I declare that the information given in this application is correct.

Signed:

Dated:

When you have completed this form, please send it to:

Head of Corporate and Strategic Services
Fermanagh and Omagh District Council
Townhall
2 Townhall Street
Enniskillen
Co Fermanagh
BT74 7BA

OFFICE USE ONLY

Date form received	
Date form checked	
Date identification documents checked	
Detail of identification documents received	
Date identification documents given back (if originals received)	
Member of staff completing	
Name	
Position	
Location	
Date request completed	
Signature	

Appendix 4

Fermanagh & Omagh District Council
Comhairle Ceantair Fhear Manach agus na hÓmaí

Fermanagh and Omagh District Council
CCTV Image Release / Viewing Request Form

Data Protection
In accordance with the Data Protection Act 2018, Fermanagh and Omagh District Council has a duty to protect any information we hold on you. The personal information you provide on this form will only be used for the purpose of CCTV records management and will not be shared with any third party unless law or regulation compels such a disclosure. For further guidance on how we hold your information please visit the Privacy section at www.fermanaghomagh.com/your-council/privacy-statement/

Ref no (provided by CSS)	
Type of request	Image Release / Image Viewing (please delete as applicable, and if request changes from a viewing to a release, please let CSS know)
Date of request	
Details of requester (name, and organisation if app.)	
Reason for request (ensure this fits within the purpose/s of the cameras)	
Detail of image(s) requested – location and date/times	
Staff members dealing with request: - Request approved by (Head of Corporate and Strategic Services) - Downloaded by (if applicable) - Released footage / Assisted with viewing (delete as applicable)	
Proof of ID checked (if necessary)	
Date and time of release / viewing	
Name of person receiving / viewing image(s) Signature	
Declaration	I understand that I am viewing/receiving these images only for the purposes detailed above and agree they will not be shared with anyone else without prior approval from FODC. I will be responsible for the security of the image(s) in accordance with data protection legislation (as amended from time to time). If applicable, I understand that the FODC staff member releasing this footage may not have seen the images contained within.

Requests to view and/or download footage should be sent to Corporate and Strategic Services before images are accessed. If requests are time sensitive, footage can be retrieved before informing CSS but this form should still be submitted.

Fermanagh & Omagh District Council
Comhairle Ceantair Fhear Manach agus na hÓmaí

Record of Destruction

Please consult the Records Retention and Disposal Schedule (RRDS) prior to disposal.

Destruction method: Confidential Shred/Deletion from electronic folder (please delete as appropriate)

Department			
Section			
RRDS Document Ref (if applicable)	**Title of Records** (as per the RRDS)	**Date span** (earliest and latest dates)	**Number of files** destroyed/deleted

I hereby certify that the records described above have been prepared for shredding/shredded/deleted (please delete as appropriate).

Bag tag reference (if applicable):	
Print name:	
Signature:	
	(Head of Service)
Date:	