

THE UNITED DIOCESES OF CORK, CLOYNE AND ROSS

RCN 20002954 CHY 2236

CCTV DATA PROTECTION POLICY

St. Nicholas' House, 14 Cove Street, Cork, T12 RP40

1. INTRODUCTION AND PURPOSE

This policy governs the operation of Closed Circuit Television (CCTV) systems installed at Bishop's Palace, Bishop Street, Cork, T12 WEY1, Ireland operated by The United Dioceses of Cork, Cloyne and Ross, which were installed in response to identified risks towards persons and property.

This policy regulates the use of CCTV and associated technology in monitoring the external environs of the premises under the remit of The United Dioceses of Cork, Cloyne and Ross (the "Diocesan Council") as occupier, ensuring compliance with:

- Regulation (EU) 2016/679 (General Data Protection Regulation - "GDPR")
- Data Protection Act 2018
- All applicable Irish data protection legislation

The CCTV system enhances security for occupiers and visitors, protects buildings and equipment, and creates awareness of surveillance during daylight and night hours for the purposes of: protecting occupiers and visitors; protecting buildings and assets; promoting health and safety; reducing crime and anti-social behaviour (including theft and vandalism); supporting An Garda Síochána in deterring and detecting crime; and assisting in identifying, apprehending and prosecuting offenders.

2. SCOPE

This policy relates to the location and use of CCTV and the monitoring, recording and subsequent use of recorded material.

This policy applies to all CCTV systems operated by The United Dioceses of Cork, Cloyne and Ross at Bishop's Palace, Bishop Street, Cork, T12 WEY1, Ireland.

3. LEGAL BASIS AND COMPLIANCE

3.1 Data Controller

The United Dioceses of Cork, Cloyne and Ross is the data controller for all personal data processed through the CCTV system.

Contact Details:

- Address: Diocesan Office, St. Nicholas' House, 14 Cove Street, Cork, T12 RP40
- Telephone: +353 21 500 5080
- Email: secretary@corkchurchofireland.com

3.2 Legal Basis for Processing

The Diocesan Council processes CCTV footage under the following lawful bases:

- Article 6(1)(f) GDPR - Legitimate interests: The protection of persons, property, and assets, prevention and detection of crime, and ensuring health and safety
- Article 6(1)(c) GDPR - Legal obligation: Where required to comply with legal obligations or court orders
- Article 6(1)(d) GDPR - Vital interests: Where necessary to protect someone's life

The Diocesan Council has conducted a Legitimate Interests Assessment (LIA) and Data Protection Impact Assessment (DPIA) which demonstrate that the use of CCTV is necessary and proportionate to achieve these legitimate aims and that individuals' rights and freedoms are appropriately protected.

3.3 Data Protection Principles

The Diocesan Council ensures that all CCTV operations comply with the GDPR principles that personal data shall be:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept for no longer than necessary
- Processed securely

4. GENERAL PRINCIPLES AND PROHIBITIONS

The CCTV system will be used in a professional, ethical and legal manner, and any diversion for other purposes is prohibited - for example, CCTV will not be used for monitoring staff or volunteer performance.

This policy prohibits monitoring based on protected characteristics including race, gender, sexual orientation, national origin, disability, or any other characteristics contained in equality legislation.

Video monitoring for security purposes is limited to uses that do not violate an individual's reasonable expectation of privacy.

CCTV systems will not be used to monitor normal activity on the premises.

The Diocesan Council will not engage in covert surveillance.

5. CAMERA LOCATIONS AND COVERAGE

Cameras are positioned to prevent or minimise recording of passers-by or other persons' private property.

CCTV monitoring may include: building perimeters, entrances and exits, gardens, curtilage and other premises on the property; monitoring of restricted access areas; verification of security alarms including intrusion alarms, exit door controls and external alarms; and video patrol of parking areas, main entrance/exit gates and traffic control.

Cameras are strategically located to: monitor external perimeters and access points; protect property and assets; verify security alarm activations; record evidence of criminal or anti-social behaviour; and ensure compliance with reasonable privacy expectations.

6. TRANSPARENCY AND SIGNAGE

6.1 Signage Requirements

In accordance with Article 13 GDPR and Data Protection Commission guidance, clear signage is displayed at the premises and prominently at entrances to inform individuals that CCTV is in operation.

All signage includes:

- Clear indication that CCTV recording is in operation
- The identity and contact details of the data controller (The United Dioceses of Cork, Cloyne and Ross)
- The purposes for which CCTV is deployed
- Reference to this policy and how to obtain a copy
- Information about data subject rights

6.2 Access to Policy

The Diocesan Secretary will provide a copy of this policy on request to visitors to the premises.

This policy is also available on request by contacting the Secretary at the address above.

7. RETENTION AND STORAGE

7.1 Retention Period

CCTV footage will be retained for a maximum of 28 days, except where images identify an issue (such as a break-in or theft) and are retained specifically in the context of an investigation or prosecution.

After 28 days, footage is automatically deleted unless:

- It has been identified as evidencing a crime or incident requiring investigation
- It is subject to a subject access request
- It is required for ongoing legal proceedings
- There is another lawful basis for extended retention

7.2 Storage Security

Images will be stored in a secure environment with access restricted to authorised personnel and an access log maintained.

Security measures include:

- Physical security: locked storage in restricted areas
- Technical security: encryption, password protection, secure networks
- Organisational security: access controls, audit logs, authorised personnel only
- Regular security reviews and updates
-

Access to the CCTV system and stored images is restricted to authorised personnel only, namely the Diocesan Secretary and other persons specifically authorised by the Diocesan Council.

8. ACCESS TO CCTV FOOTAGE

8.1 Authorised Personnel

Routine access to live monitoring and stored footage is limited to:

- Diocesan Secretary
- Other individuals specifically authorised by the Diocesan Council for legitimate purposes

8.2 Disclosure to Third Parties

CCTV footage may be accessed by An Garda Síochána where required by law regarding suspected crime or following a request when a crime or suspected crime/illegal/anti-social behaviour has taken place; the HSE or other statutory bodies charged with child safeguarding; data subjects or their legal representatives pursuant to an access request; individuals or their legal representatives subject to a court order; or the Diocesan Councils' insurance company where required to pursue a claim for damage to insured property.

8.3 Requests from An Garda Síochána

Information obtained through CCTV may only be released when authorised by the Diocesan Secretary following consultation with An Garda Síochána. All requests will be fully recorded. If An Garda Síochána is seeking footage for a specific investigation, they may require a warrant, and any such request should be made in writing with the Secretary immediately seeking legal advice.

All disclosures to An Garda Síochána must be: documented in writing; recorded in the access log; authorised by the Diocesan Secretary; and compliant with data protection legislation.

Where An Garda Síochána requests covert surveillance on the premises requiring judicial consent, any such request will be made in writing and the Diocesan Council will seek legal advice.

9. DATA SUBJECT RIGHTS

9.1 Right of Access (Subject Access Request)

Any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided the image/recording exists (has not been deleted) and no exemption or prohibition applies to the release.

Individuals may exercise their right of access by submitting a written request to:

The Diocesan Secretary The United Dioceses of Cork, Cloyne and Ross St. Nicholas' House
14 Cove Street Cork, T12 RP40

Under the GDPR and Data Protection Act 2018: no fee is charged for access requests (unless the request is manifestly unfounded or excessive); the Diocesan Council must respond within one month of receipt (extendable by two further months for complex requests); and requesters should provide all necessary information to assist in locating the footage, such as date, time and location of the recording.

9.2 Third-Party Protection

Where footage identifies other individuals, images may only be released where they can be redacted or anonymised so that other persons are not identified or identifiable. Other images will be obscured before data is released.

9.3 Other Rights

Under GDPR, data subjects also have:

- Right to rectification - to correct inaccurate personal data
- Right to erasure - in certain circumstances, to request deletion
- Right to restrict processing - to limit how data is used
- Right to object - to object to processing based on legitimate interests
- Right to lodge a complaint - with the Data Protection Commission

To exercise these rights, contact the Diocesan Secretary using the details above.

10. ACCOUNTABILITY AND RESPONSIBILITIES

The Diocesan Council is responsible for:

Ensuring CCTV systems are implemented in accordance with this policy; overseeing and coordinating CCTV monitoring for safety and security purposes; evaluating all existing

systems for policy compliance; and ensuring monitoring is consistent with the highest standards and protections.

Reviewing camera locations and being responsible for release of information or recorded materials; maintaining a record of access (access log) to material; and ensuring monitoring tapes are not duplicated for release.

Ensuring the field of view from cameras conforms to this policy; ensuring all monitored areas do not breach enhanced privacy expectations; and ensuring external cameras are non-intrusive and comply with the principle of reasonable expectation of privacy.

Ensuring monitoring recordings are stored securely with access by authorised personnel only; ensuring images are stored for no longer than 28 days unless required for investigation or proceedings; ensuring camera control is solely to monitor suspicious behaviour and criminal damage, not individual characteristics; and ensuring camera control does not infringe reasonable privacy expectations.

10.1 Supervision and Administration

Supervising the access and maintenance of the CCTV system is the responsibility of the Diocesan Secretary, who may delegate administration to another staff member.

10.2 Data Protection Impact Assessment

The Diocesan Council maintains a Data Protection Impact Assessment (DPIA) which: identifies and minimises data protection risks; assesses necessity and proportionality; documents security measures; and is reviewed regularly and updated when systems change.

11. DATA PROCESSORS AND THIRD-PARTY CONTRACTORS

11.1 Security Company Arrangements

The CCTV system is controlled by a security company contracted by the Diocesan Council. A written contract is in place detailing areas to be monitored, data storage duration, permitted data uses, security standards and verification procedures. The contract requires the security company to provide all reasonable assistance with subject access requests within statutory timeframes.

Security companies operating cameras on behalf of clients are data processors operating under the instruction of data controllers. They must have appropriate security measures to prevent unauthorised access, alteration, disclosure or destruction of data, including robust encryption for remote access and appropriate access controls. Staff have been made aware of their data security obligations.

All data processor contracts comply with Article 28 GDPR and include:

- Processing only on documented instructions
- Confidentiality obligations for personnel
- Appropriate technical and organisational security measures
- Sub-processing restrictions
- Assistance with data subject rights requests
- Deletion or return of data upon contract termination

- Audit rights and compliance verification

12. RECORD KEEPING AND ACCOUNTABILITY

The Diocesan Council maintains the following documentation:

- Records of processing activities (Article 30 GDPR)
- Data Protection Impact Assessment for CCTV operations
- Legitimate Interests Assessment justifying the use of CCTV
- Access logs recording all viewing and disclosure of footage
- Data processor contracts with security companies
- Training records for authorised personnel
- Subject access request records
- Incident and breach logs

13. DATA BREACHES

In the event of a personal data breach involving CCTV footage:

- The breach will be assessed for risk to individuals' rights and freedoms
- If the breach poses a risk, it will be reported to the Data Protection Commission within 72 hours of becoming aware
- If the breach poses a high risk to individuals, affected data subjects will be notified without undue delay
- All breaches will be documented including facts, effects and remedial action

14. TRAINING AND AWARENESS

All personnel with access to CCTV systems receive training on:

- Data protection principles and GDPR compliance
- This policy and operational procedures
- Security and confidentiality obligations
- Handling subject access requests
- Incident reporting procedures

Training is refreshed regularly and recorded.

15. POLICY REVIEW AND UPDATES

This policy will be reviewed and evaluated from time to time, taking cognisance of changing information or guidelines from the Data Protection Commission and An Garda Síochána.

The policy will be reviewed:

- At least annually
- Following any significant incident or data breach
- When legislation or guidance changes
- When CCTV systems are modified or expanded

Effective Date: 7 February 2026

Next Review Date: February 2027

Policy Owner: The United Dioceses of Cork, Cloyne and Ross

Approved by: [The Diocesan Council / The Bishop]

16. CONTACT AND COMPLAINTS

For questions about this policy, CCTV operations, or to exercise data protection rights:

The Diocesan Secretary

The United Dioceses of Cork, Cloyne and Ross

St. Nicholas' House

14 Cove Street

Cork,

T12 RP40

Telephone: +353 21 500 5080

Email: secretary@corkchurchofireland.com

Complaints to the Data Protection Commission

If you are dissatisfied with how the Diocesan Council handles your personal data, you have the right to lodge a complaint with:

Data Protection Commission

21 Fitzwilliam Square South

Dublin 2

D02 RD28

Ireland

Telephone: +353 (0)761 104 800 / Lo Call 1890 252 231

Email: info@dataprotection.ie

Website: www.dataprotection.ie

APPENDIX 1 - KEY DEFINITIONS

CCTV (Closed-Circuit Television) - The use of video cameras to transmit a signal to a specific place on a limited set of monitors, with images recorded on videotape, DVD or other digital recording mechanism.

Data Controller - The United Dioceses of Cork, Cloyne and Ross, which determines the purposes and means of processing personal data collected through CCTV.

Data Processor - A person who processes personal information on behalf of a data controller, such as a security company contracted to operate CCTV systems.

Data Subject - An individual who is the subject of personal data - any identifiable person whose image is captured on CCTV.

GDPR - Regulation (EU) 2016/679, the General Data Protection Regulation, which governs the processing of personal data in the European Union.

Personal Data - Any information relating to an identified or identifiable living individual, including images captured on CCTV that allow identification.

Processing - Any operation performed on data, including obtaining, recording, keeping, collecting, organising, storing, altering, adapting, retrieving, consulting, using, disclosing by transmitting, disseminating or making available, aligning, combining, blocking, erasing or destroying data.

Premises - Bishop's Palace, Bishop Street, Cork, T12 WEY1, Ireland, its gardens, environs and outhouses, and any other premises operated by The United Dioceses of Cork, Cloyne and Ross where CCTV is installed.

Diocesan Secretary - The Diocesan Secretary of the United Dioceses of Cork, Cloyne and Ross, St. Nicholas' House, 14 Cove Street, Cork, T12 RP40.

Subject Access Request - A request by an individual to access their personal data held by the Diocesan Council, including CCTV footage.

The Diocesan Council - The United Dioceses of Cork, Cloyne and Ross