



CCTV Operations Policy Management and Operation of Non- Networked CCTV

Overview

Closed Circuit Television (CCTV) is one tool used by Cancer Fund for Children (CFFC) to prevent, detect, and reduce the fear of crime; it is also used for health and safety. CCTV system suitability across Cancer Fund for Children sites is assessed, and its implementation considered, in conjunction with other preventative methods in accordance with the guiding principles of the use of CCTV found on page 2.

CFFC uses CCTV in buildings, public spaces and car parks across its sites for public space surveillance. This policy sets out the terms governing the use and management of the CCTV equipment and images, which is managed by the IT & Facilities Team.

The use of CCTV cameras is regulated in Northern Ireland by the ICO (Information Commissioner's Office) and supplemented by guidance from the Surveillance Camera Commissioner Code of Practice, which can be found via the ICO website: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/video-surveillance/>

Scope

This Policy is to regulate the operation of Cancer fund for Children's public space Closed Circuit Television (CCTV) systems operating within various sites and details how CCTV will be used by the charity, employees, and contractors and accessed by law enforcement organisations.

All CCTV Equipment used by Cancer Fund for Children falls into the following category:

- Non-networked CCTV is a system which is locally recorded and non-monitored. Footage is retained on the local storage device and is downloadable for viewing.
- Remote access via app is provided to authorised members of staff only.

Our CCTV Operations Policy reflects the regulations laid down by the ICO and follows the 12 Guiding Principles in [The Surveillance Camera Code of Practice](#) published in 2013. The Code of Practice provides a framework for CCTV operators to act responsibly:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 1 of 11

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Objectives of Cancer Fund for Children CCTV

The CCTV systems operated by CFFC will not be used for any other purpose than those set out in this document, and the Law, without prior consultation with and the authorisation of:

IT & Facilities Manager: Corinna Decodts
Telephone: 074 2343 3308
Email: corinna@cancerfundforchildren.com

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 2 of 11



CCTV Operations Policy

Management and Operation of Non- Networked CCTV

The Charity will use CCTV for:

- Safeguarding the health and safety of employees, service users, building users, contractors and members of the public;
- Assist in the prevention and investigation of accidents, incidents and near misses;
- Identify and prevent dangerous or unsafe conditions and acts or omissions.
- Investigate the circumstances surrounding insurance claims;
- Ensure the security of Cancer Fund for Children's property and assets;
- Deterring crime, anti-social behaviour and assisting in the detection of criminal offences and suspected crime;
- Reducing the fear of crime and anti-social behaviour;
- Improving the safety and security of services users, visitors and the community who use the Charity's facilities;
- Assist in the identification, apprehension and prosecution of offenders.

The Charity will not use CCTV for:

- Monitoring the activities or targeting of anyone for reasons of age, gender, religion or race;
- Monitoring anyone lawfully going about their business, unless circumstances are such that give rise to particular concerns for that person's safety;
- Intruding into the privacy of any individual unless in pursuit of one of the above authorised uses;
- Purposes of entertainment;
- Covert surveillance.

If while carrying out CCTV equipment checks, poor health and safety practice, unsafe behaviour or acts of misconduct are observed, then under the statutory duty of care prescribed in The Health and Safety at Work (NI) Order 1978, the appropriate person(s) will be informed.

Employee Enquiries and Health and Safety Concerns

If an employee of CFFC or any authorised building user or contractor has any health and safety concerns that may be supported by a review of the CCTV images, a request should be made to the IT & Facilities Manager.

Ownership & Management of the CCTV system

The public space CCTV system is wholly owned by CFFC. The roles and responsibilities of Cancer Fund for Children personnel within the scope of this Policy are set out in Appendix 1. The day-to-day management of the CCTV is the responsibility of the IT & Facilities Manager, supported by the Facilities Management Officer and IT Officer for each location.

Senior Responsible Officer (SRO)

The IT & Facilities Manager has overall management responsibility for ensuring that all CCTV systems owned by CFFC are operated in accordance with all relevant guidance and legislation. The Senior Responsible Officer (SRO) is designated as defined in guidance issued by the Surveillance Camera Commissioner.

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 3 of 11



CCTV Operations Policy

Management and Operation of Non- Networked CCTV

Single Point of Contact (SPOC)

Cancer Fund for Children has designated the IT Officer responsible for CCTV enquiries as its Single Point of Contact (SPOC) for all CCTV systems operated by the Charity.

The SPOC's role is operational for all matters relating to surveillance cameras. The SPOC will support the IT & Facilities Manager (the SRO) regarding compliance with Protection of Freedoms Act 2012 (PoFA).

The SPOC will act as the main contact point for anything related to surveillance camera systems and will introduce consistent surveillance camera policies and procedures that can be applied to all Charity CCTV systems at an operational level. The SPOC will ensure that all staff across the Charity operating surveillance cameras receive appropriate evidence-based training and awareness, including current and future regulatory and legislative obligations.

Policy Contributors

This Policy has been prepared in consultation between the Charity and our specialist CCTV Contractor (see details in Appendix 4).

The Policy complies with the Home Office Surveillance Camera Code of Practice, issued by the Home Office and overseen by the Surveillance Camera Commissioner. In particular, the '12 Guiding Principles' set out within that code (as above on page 2) and 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information' issued by the Information Commissioner's Office.

Revision and Consultation

This Policy will be subject to regular review annually, see version control for further information.

CCTV Equipment: Cameras

The CCTV consists of permanent (fixed in situ) static cameras with no audio recording capabilities. The images from these cameras are securely stored locally (physical access control and data encrypted at rest and in transit) on the hard drives of Network Video Recorders (NVRs). CFFC operate no "dummy" or "covert" cameras. The location and number of cameras is provided in Appendix 2.

Signage

The Charity has a consistent and compliant approach to CCTV signage. CCTV signage is an extension of the CFFC Privacy Policy. All areas where CCTV is in use will have clear signage displayed to comply with the "right to be informed" under UK GDPR. Signage will advise individuals that they are about to enter an area or remain in an area covered by CCTV.

Additionally, signage will act as a deterrent against crime. CCTV signs will not be displayed in areas which do not have CCTV cameras. The information on the sign will explain why the CCTV camera(s) are there,

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 4 of 11



CCTV Operations Policy

Management and Operation of Non- Networked CCTV

who operates them (Cancer Fund for Children), and contact details including a telephone contact for further information. The signs, position and the message will be large enough to enable people to easily read the information. An example of the current CCTV design can be found in Appendix 3.

Maintenance

Checks and maintenance will be carried out on a scheduled basis to ensure compliance with legal obligations, the ICO and the Surveillance Camera Commissioner's (SCC) Code of Practice, with particular reference to principle 8, and to ensure that images recorded continue to be of appropriate evidential quality and the systems are fit for the purpose intended. CCTV equipment will be checked and maintained to ensure that it is operating correctly and to ensure the integrity of the images.

Access

The control of the CCTV system will remain with CFFC at all times. Only authorised members of staff will have least-privilege access to the operating controls. Secondary control capabilities are accessible and will only be used by authorised, trained personnel when specifically required and are protected by secure login procedures.

Confidentiality

All staff with access to the operation of the CCTV system will observe strict confidentiality in respect of all information gained and observed during the course of undertaking the management and operation of the CCTV. This shall prohibit the disclosure of any such information to any third party (except as may be required by law) without the written consent of the IT & Facilities Manager.

Use of CCTV Systems

The purpose of all CCTV cameras operated by CFFC is to provide surveillance of public areas only. All camera locations have clearly visible, legible signage that will give clear notice that CCTV is in operation. Cameras will be sited and configured to view public areas only and not surveil private dwellings or other areas where privacy is expected.

Cancer Fund for Children will take all reasonable steps to ensure that the non-networked CCTV equipment cameras will be positioned to:

- Provide the most appropriate coverage in and/or around the relevant operational area; and
- Record images relevant to the Purposes.

CCTV Cameras are fixed in position during the installation by the installation engineers and shall remain in these positions. In the event that the cameras have moved out of alignment, this must be reported as soon as possible to the IT & Facilities Manager.

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 5 of 11



CCTV Operations Policy

Management and Operation of Non- Networked CCTV

Data Recording

Ownership of Copyright

All data captured by the CCTV cameras and related equipment and stored on any form of recording media held internally or externally will remain the property of Cancer Fund for Children.

Recording Retention Period

All images from the CCTV system will be recorded onto hard drives which employ full-disc encryption. Hard drives are located locally at each site. Recorded data will be stored for a maximum period of 25 days. The Video Management System (VMS) or embedded software automatically overwrite footage every 25 days by continuously overwriting the oldest data. Each location is assessed for specific retention periods to ensure that data is not retained for longer than necessary.

Use of Recorded Data for Law Enforcement Purposes

Reason to View Recorded Data

When the police or other enforcement agency believes that footage of a criminal offence has been recorded, they may request relevant CCTV footage under the Law Enforcement Regime, Part 3 of the DPA 2018. At no time shall the images supplied to the police or other law enforcement agency be used for anything other than the purpose specified and identified when the images are released from the Charity. The responsibility for the images safekeeping and integrity will transfer to the police or other law enforcement agency once the media has left the possession of the CFFC. The Charity will not be liable for any mishandling, compromise in security or other misuse of the recording media whilst in the custody of the police or other law enforcement agency.

Request to View Recorded Data by Non-Enforcement Agencies

If, in exceptional circumstances, the release of recorded data is requested by agencies other than the police or other enforcement agency, such a release will only be granted under the authority of the IT & Facilities Manager. The procedures for handling and logging the recorded data are as described for the police or other enforcement agency, however commercial agents such as insurance companies may be charged a fee to cover administration costs.

Any requests from members of the general public or a third party will be dealt with under the provisions of the Data Protection Act 2018, UK GDPR or the Freedom of Information Act 2000.

Release of Images for Entertainment Purposes

The Charity will not release any images, either directly or indirectly, to any organisation for inclusion in any television or other media production designed purely for entertainment purposes or educational/factual programs. Likewise, material can only be released to the media as part of an ongoing criminal investigation by Police with the permission of Charity guided by the IT & Facilities Manager.

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 6 of 11



CCTV Operations Policy

Management and Operation of Non- Networked CCTV

Data Protection

Cancer Fund for Children takes the security and privacy of data seriously and is committed to being transparent about how we collect and use personal data and meet our data protection obligations. We are registered on the ICO's Data Protection Register (Registration number: Z1792224) and comply with our legal obligations under UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

CFFC will take all appropriate steps to ensure that CCTV will not be intentionally or deliberately intrusive of individuals or private premises.

Data Protection Definitions

There are two types of data under the 2018 General Data Protection Regulations:

“Personal data” which means any information relating to a living individual who can be identified from that information (a “data subject”) on its own or when taken together with other information. This may include both facts and expressions of opinion about the person and indication of the intentions of the Charity or others in respect of that person. It does not include anonymised data.

“Special category data” which means information about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

Images collected by Cancer Fund for Children public space CCTV will normally fall under the “Personal data” category.

Lawfulness of Processing

The Charity uses CCTV cameras as a proportionate response to support safety around it’s premises and work with its partners to reduce both the level and fear of crime. It achieves this in a number of areas including:

- Providing a visible deterrent to crime, thereby providing reassurance to staff and visitors alike;
- Improving the safety and security of staff, visitors and contractors who use the facilities in the areas covered.

Subject Access Requests

Individuals have the right to request a copy of their personal data being processed by the Charity. In the case of CCTV footage this will always be in electronic form.

Cancer Fund for Children should respond without delay and within one month of receipt of the request. The time limit may be extended by a further two months if the request is complex or if a number of

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 7 of 11



CCTV Operations Policy Management and Operation of Non- Networked CCTV

requests from the individual are received. CFFC will write to the individual within one month of receiving the original request to explain why an extension may be necessary.

If a subject access request is manifestly unfounded or excessive CFFC is not obliged to comply with it. The Charity will explain to an individual if they refuse to respond to a request and of their right to complain to the Information Commissioner's Office.

In most cases a fee will not be charged to comply with a SAR. However, in some cases a 'reasonable fee' may be chargeable for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.

Dependent on the circumstances surrounding particular SARs, Cancer Fund for Children may not permit the release of images to individuals being investigated by enforcement agencies (including the police) where images have been handed over as part of the investigation or other exemptions under UK GDPR. The responsibility for investigating and disclosing images to those involved in the investigation are covered by the Police and Criminal Evidence Act 1984 (PACE) and the Crown Prosecution Service (CPS) Evidence and Disclosure Policy which prosecuting authorities are required to follow. It should be noted that other enforcement agencies will operate under other legislation but the use of and disclosure of evidence rests with them.

Requests for CCTV footage can be made by emailing supportercare@cancerfundforchildren.com

The Charity will verify identification before the request can be processed.

Data Security

As per Article 5(1)(f) of the UK GDPR which concerns the 'integrity and confidentiality' of personal data, Cancer Fund for Children takes the security of personal data seriously. Alongside Article 32(1) of the UK GDPR, CFFC has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure and to ensure that data is not accessed, except by those who have lawful authority in connection with the proper performance of their duties.

Examples of CFFC activities to secure CCTV footage include:

- Encryption at rest and in transit - meaning that information is "masked" so that it cannot be read without special knowledge (Decryption - such as a password). The masked information is said to then be "encrypted".
- Physically controlling access to systems and networks allows us to prevent intrusion by individuals who are not authorised to access or view personal information.
- Implementing "least privilege" access control ensures that authorised individuals have access to data required to fulfil their job function.

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 8 of 11



CCTV Operations Policy

Management and Operation of Non- Networked CCTV

Training and Guidance

Induction training for all new members of staff includes compulsory training on cybersecurity and data protection. Regular data protection updates are also provided to all staff and managers. All staff are required to complete mandatory evidence-based training on UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Legal Requirements and Applicable Legislation

At all times, and without exception, CFFC staff will comply with all legislation, policies, codes of practice and guidelines relating to the operation of the CCTV System. In addition to CFFC Policies, procedures, guidelines and codes of practice and operational procedural manuals, CCTV and its operation are subject to legislation under:

- UK GDPR
- Data Protection Act 2018
- Data Protection Code of Practice for Surveillance cameras and Personal Information.
- The Human Rights Act 1998 – Article 8 gives individuals the right to privacy, Article 6 gives individuals a right to a fair trial and Article 5 gives the right to Liberty and Security.
- The Freedom of Information Act 2000 – all recorded information and information relating to individuals are subject to the provisions of the Data Protection Act 2018.
- The Private Security Industry Act 2001 – where required by the Act, operators of CCTV will be licensed under the Act.
- The Protection of Freedoms Act 2012.

Complaints Procedures and Comments

The Procedure for Complaints against the CCTV System

Any complaint received regarding CCTV operations will be dealt with following the complaints procedure set out by Cancer Fund for Children. Further information can be found here:

<https://cancerfundforchildren.com/wp-content/uploads/2024/10/CFFC-Feedback-and-Complaints-Policy-October-2024.pdf>

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 9 of 11



CCTV Operations Policy

Management and Operation of Non- Networked CCTV

Appendix 1: Management of the CCTV system (Roles and Responsibilities)

Responsible Officer	Title	Responsibilities
Corinna Decodts	IT & Facilities Manager Senior Responsible Officer (SRO)	<ul style="list-style-type: none"> Complaints, Compliance, Subject Access Requests Overall responsibility for CCTV Management of external contractors
Drew Crothers	IT Officer Single Point of Contact (SPOC)	<ul style="list-style-type: none"> System physical security Key holder for secure compartments System checks, downloading and copying of images Reporting of faulty non-networked CCTV equipment
Advanced Overwatch	Specialist CCTV contractor	<ul style="list-style-type: none"> CCTV Installation and maintenance Corrective works and callouts Staff training Production of compliant reporting on all works

Appendix 2: CCTV Location Information

Location	Address	Telephone	Fixed Cameras
Curlew Pavilion	Portside Business Park, Airport Road West, Belfast BT3 9ED	028 9080 5599	2

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 10 of 11

Appendix 3: Example of Charity CCTV Signage

Compliant CCTV signage is deployed across the entrances and around CFFC sites to advise of the presence of CCTV recording in progress. Such CCTV signage is an extension of the Charity's Data Protection Policy.



Appendix 4: CCTV Contractor Information

Company Name	Advanced Overwatch
Address	1 st Floor, Beresford House, 2 Beresford Road. Coleraine BT52 1GE
Telephone Number	028 7087 8077
Appointed Contact	Mr Patrick Logue (Managing Director)
Office Email Address	info@advancedoverwatch.com
Website Address	https://advancedoverwatch.com
SSAIB Registration Number	NIRE127
ConstructionLine Registration Number	00321414
SIPP Acclaim Registration Number	00321414
Specialist Insurance Held	Yes
Staff Vetted	BS7858:2019
ISO Accreditations	ISO 27001:2013, ISO 9001:2015
Cyber Essentials Verified	IASME-CE-032431
ICO Registered	ZA481203
Data Protection Specialism	IAPP: CIPP/E, CIPM
Professional Membership	MSyI, CTSP, IPSA

Approved By: Corinna Decodts IT & Facilities Manager	Date Issued: 31/03/26	Revision No: 01
Authorised By: Phil Alexander CEO	Review Date: 31/03/27	Page 11 of 11