Western Health and Social Care Trust

Closed Circuit Television Surveillance System Policy (CCTV)

March 2017

Policy Title	Closed Circuit Television surveillance system policy
Policy Reference Number	Corp17/002
Implementation Date	March 2017
Review Date	March 2019
Responsible Officer	Maureen Kelly (Head of Support Services)

Contents

1.0 Introduction

This document sets out the appropriate actions and procedures which must be followed to comply with the Data Protection Act in respect of the use of CCTV (closed circuit television) surveillance systems operated and managed by the WHSCT.

In drawing up this policy, account has been taken of the following: -

- The Data Protection Act 1998;
- Freedom of Information Act 2000
- In the picture: A data protection code of practice for surveillance cameras and personal information produced by the Information Commissioners Office (Version 1: 15/10/2014);
- The Human Rights Act 1998;
- The Regulation of Investigatory Powers Act 2000;
- The Protection of Freedoms Act 2012
- Deprivation of Liberty Safeguards DOLS – Interim Guidance October 2010
- Code of Practice on Protecting the Confidentiality of Service User Information" (v2.0 2012)
- Trust Fraud Policy Statement 2015

The Data Protection Act 1998 came into force on 1st March 2000 and contains broader definitions than those of the previous Act (Data Protection Act 1984) and more readily covers the processing of images of individuals captured by CCTV cameras. This new 'Act' makes provision for, amongst other things, legally enforceable standards in relation to the collection and processing of images relating to identifiable individuals.

The Information Commissioners Office has reviewed and updated their CCTV Code of Practice which sets out the measures which must be adopted to comply with the Data Protection Act 1998. This goes on to set out guidance on following good data protection practice. The Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations as Data Controllers and also reassures the Public about the safeguards that operators should have in place. It also permits those whose image has been captured by a CCTV system, to request access to those images.

2.0 Scope

This policy will apply to all current, and past employees of the Western Health and Social Care Trust (WHSCT), persons acting as Agents of the WHSCT, individuals or Bodies acting as providers of services on behalf of the WHSCT, tenants occupying WHSCT managed facilities and all other persons and visitors whose image may be captured by the systems operated and managed by the WHSCT and who can be clearly identified from that image.
The policy will also apply to premises rented by the Western Health and Social Care Trust. In circumstances where the landlord operates a CCTV system, the landlord will act the data controller. Under these circumstances it is the landlord's responsibility to comply with the Data Protection Act in relation to storage and disclosure of images.

3.0 Policy Statement

The Chief Executive is legally responsible for all WHSCT CCTV systems and for the uses that they are employed. In operational terms, the Performance and Services Improvement Directorate (Support Services Department) will have day-to-day responsibility for ensuring compliance with the requirements of this policy, and all relevant legislation.

3.1 The 'purpose' of the WHSCT's use of CCTV equipment to record digital images is for the:

- Prevention and Detection of Crime and Disorder;
- Apprehension and Prosecution of Offenders (this may on occasion include the use of images as evidence in criminal/civil proceedings);
- Protection of Patient, Staff and Public Health and Safety;
- Protection of Public Health
- Protection of Patient, Staff and Public property
- Investigation of matters relating to Disciplinary Proceedings
- Protection of Assets
- Investigation of Incidents/Serious Adverse Incidents

The purposes above identify the main reasons that the WHSCT operates a passive CCTV system at its primary facilities. Any use of a CCTV system, or any proposed use of images captured by a CCTV system, for a purpose or purposes other than those set out above must be discussed and agreed through the Information Governance Steering Group (IGSG)

Prior to the installation of CCTV cameras on WHSCT premises checks must be undertaken to ensure the installation complies with this policy, the Data Protection Act 1998 and all relevant legislation. All proposals to install new CCTV systems, add to or upgrade existing systems or to reposition existing cameras should be completed in consultation with Support Services and Estates Services departments within Facilities Management.

4.0 Location of Cameras

It is critical that the location of cameras is carefully considered. The physical location that is captured by the cameras images, and the potential for capturing images of individuals, and the type of individuals that it is set to capture, will be a major driver in justifying the location and determining the extent of the cameras coverage. Each of these factors must comply with at least one of the purposes listed at 3.1 and importantly, comply with the Principles of the Data Protection Act 1998 and other relevant legislation. If a purpose (use) is proposed that is not clearly listed at 3.1, the proposed use must be authorised by the Director or Assistant Director of Performance Service Imporvement.

All cameras should be located in prominent positions within clear Public and Staff view, to both act as a visual deterrent and as a visual prompt for those entering the area that is covered by the camera.

Signs must, by law, be erected at all entrance points to WHSCT facilities and on the perimeter of each physical area being captured by CCTV systems informing individuals that they are about to enter an area covered by CCTV. Additionally, the internal cameras within WHSCT facilities should have signs erected within the premises advising Staff, Visitors and Tenants that they are in an area that is covered by a passive CCTV system. These signs must be clearly visible, the message must be clear, there must be a purpose/s provided for the recording (see 3.1) and the organisations name (the Data Controller) and a contact person must be listed.

Prior to the approved upgrading of existing CCTV systems or installation of a new CCTV system, ICT should be informed. Estates/ICT staff will approve and facilitate the installation of all necessary software and hardware onto the HSC network, in line with the WHSCT ICT Security Policy, to enable the recording, storage, retrieval and automatic deletion of images that are older than the limit set by the Retention and Disposal Schedule (See Section 4.5, page 8).

4.1 Quality of the Images

It is essential that the images produced by the equipment are as clear as possible, to ensure that they are effective for the purpose(s) for which they are intended. For example, if the purpose is ‘apprehension and detection of offenders’, then the quality should be such that allows individuals to be identified from the captured image.

All camera installations and service contracts should be undertaken by approved security companies. Upon installation all equipment is to be tested to ensure that only the approved predetermined areas are monitored and that the images are of sufficient quality, and available for viewing in live and play back mode. All CCTV cameras and equipment should be serviced and maintained on a regular basis.

Regular checks must be undertaken to ensure time and date captured by the WHSCT CCTV systems is correct. This is critical in the event that an incident is either time sensitive or date specific, and will add weight to the image in the event that the image is used as evidence by either the WHSCT or others.

4.2 Processing of Images

Images, which are not required for the purpose(s) for which the equipment is being used, should not be retained for longer than is necessary in order to comply with Principle 5 of the Data Protection Act, which states that ‘Personal data processed for any purpose or purposes shall not

be kept for longer than is necessary for that purpose or those purposes' (see 3.1 above). While images are being retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of individuals whose image may have been recorded to ensure compliance with Principle 7 of the Act which requires that 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'. It is critical that access to and security of the images is controlled in accordance with the requirements of the Data Protection Act 1998. This requirement will be monitored on a regular basis by the Support Services Manager.

Access to images recorded on a WHSCT CCTV system will be granted by the Support Services Manager or designated deputy. No viewing of live feed images captured by a CCTV system is permitted other than for those staff tasked with monitoring live feed monitors. Any access to WHSCT systems which contains personal information is restricted. 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.

All images will be recorded on a digital format, (where existing equipment permits) and stored on secure WHSCT servers or dedicated server space, taking advantage of existing HSC ICT security mechanisms (see ICT Security Policy). All live feed monitors located within the WHSCT's facilities should be positioned so as to prevent unauthorised viewing by any person other than those tasked with that particular role.

4.3 Access to and Disclosure of Images to third parties

Access and disclosure of images is permitted only if it supports the purpose of this policy and is in line with the provisions of the Data Protection Act 1998 or another piece of relevant legislation, some of which are listed at section 1.0.

Where the images are required for evidential purposes in legal or WHSCT disciplinary proceeding, a digital recording of these will be made by nominated Support Services Staff acting at the direction of the Support Services Manager or deputy. These recordings will be viewed to ensure that the correct images are captured. Only persons trained in the use of the CCTV equipment and who have appropriate authorisation should access any captured data.
All requests for access to images must be made using request form (appendix 1)

It is critical that access to and disclosure of the images recorded, by CCTV and similar monitoring equipment is restricted and carefully controlled. This will ensure that the rights of individuals are protected and preserved, but also ensure that the continuity of the evidence trail remains intact should images be required for evidential purposes e.g. A Police enquiry or an investigation being undertaken as part of the WHSCT's disciplinary procedure.

Access to the medium on which the images are displayed and recorded is restricted to WHSCT staff and third parties as detailed in the scope of the policy at section 2.0. Accessing images for any other purpose not listed at 3.1 is not permitted unless prior approval has been sought and granted from the Director or Assistant Director of Performance Service Improvement.

Applications (Form 81) which contains information on persons specified, location, date, time, type of information required and nature of inquiry made by the Police Service of Northern Ireland (PSNI) or other body charged with investigating any infringement of law, for access to CCTV images, must be submitted to Support Services Department, and approved by a Support Services Manager (Band 5 or above), prior to disclosure to the requesting body. As with any agency, the Police or other regulatory body are required to provide justification to the WHSCT before access to

CCTV images will be provided, and then, only relevant images will be furnished once a request has been approved. No person or authority has the automatic right to unfettered access to images stored on the Trusts CCTV system.

4.4 Access to Images by Individuals (Subject Access Requests DPA 1998)

Applicants requesting access to their recorded image from a WHSCT CCTV system, have the right to do so under section 7 of the Data Protection Act 1998. All requests for access to personal information held on a CCTV system will be processed by the Information Governance Department. Once applications (Appendix 2) have been processed and permission granted, Support Services Staff will be tasked with retrieving the electronic data and copying this on to removable media such as a CD for transfer by the WHSCT to the requestor.

Requests will be considered and processed in line with Subject Access requirements under the Data Protection Act. The WHSCT will provide the requestor with the information within 40 days of receipt of the request. If a request for access is refused, then a written response detailing the reasons why the request has been refused will be sent to the requestor, again, no later than 40 days from receipt of the request.

Note: Once an application has been approved by the WHSCT and images have been released to an applicant, the WHSCT is no longer responsible for any further purpose that those images may be used for. All third party data, in this case, images of other persons captured by the CCTV equipment, will be irreversibly removed from the copy released to the subject where it is technically feasible. Not to do so may be in breach of the third parties rights as afforded by one or more of those pieces of legislation and codes of practice listed at section 1.0.

4.5 Retention and Disposal of Images

Good Management Good Records guidance states that Close Circuit TV images must be kept for 28 days and then permanently erased unless required for evidential purposes e.g. potential legal claims from slips/falls, assaults on staff/visitors etc.

4.6 Tenants within Western Health and Social Care Trusts Property

The WHSCT operates CCTV systems within locations as outlined in (Appendix 3) for one or more of the purposes listed at section 3.1 to the benefit of both WHSCT staff and tenants located within these facilities. Where a legitimate need arises for a tenant/occupier to access images captured by one or more of these CCTV systems, the WHSCT Support Services Department will, facilitate access to any relevant images to the requesting bodies provided they meet the proposals of one or more of the purpose listed at section 3.1. It should be noted that as Data Controller, the WHSCT needs to be assured by the requesting organisation or agency, that the request is legitimate and complies with all relevant legislation, policies and procedures operating within the WHSCT.

5.0 Interaction with other Trust Policies

This policy should be read in conjunction with the WHSCT Data Protection / Confidentiality Policy and Freedom of Information procedures and ICT Security Policy and at each of the local offices.

It should be noted that images captured on CCTV systems that do not identify individuals, may not be subject to the provisions of the Data Protection Act 1998. However, these images may still be requested and released by virtue of the provisions of the Freedom of Information Act 2000.

All images captured by WHSCT operated CCTV systems will be retained for 28 days as identified in the WHSCT Retention and Disposal Schedule. Only in the event that images are required for evidential purposes or if they are the subject of a Freedom of Information request or Subject Access request under Data Protection Legislation, should images be retained for longer than the agreed retention period.

6.0 Roles and Responsibilities

As stated in Section 3 Policy Statement. The Directorate of Performance and Services Improvement has operational responsibility to ensure compliance with the requirements of this policy and all relevant legislation

- The Support Services Department has day to day responsibility for ensuring the WHSCT is compliant in respect of all applicable legislation and relevant Codes of Practice Support Service Managers report directly to the Head of Patient and Client Support Services in relation to compliance with the policy.

- Support Service Managers or designated deputy has the following responsibilities.

    - Conduct an annual review of CCTV systems and usage
    - Ensure that CCTV images are being stored securely and handled in accordance with this policy and relevant legislation and the ICO 'CCTV' Code of Practice
    - Ensure that images are retained in line with the WHSCT Retention and Disposal Schedule, and that this electronic record is managed as any sensitive personal record would be within the WHSCT organisations.
    - Ensure that images are disposed of in a secure and irreversible manner
    - Ensure access protocols are in place and are being followed at each WHSCT site
    - Ensure that viewing and disclosure of images is in line with WHSCT policy and legal obligations
    - Ensure that staff using or maintaining the CCTV systems are sufficiently trained and aware of their obligations under the Data Protection Act and their Contract of Employment
    - Ensure that each system is regularly maintained and identify if system upgrades are necessary
    - Ensure that each passive CCTV system has adequate signage advising members of the public and staff that they are being monitored.

- All Trust Staff are legally bound by the Data Protection Act 1998, Common Law Duty of Confidence and their Contract of Employment to protect personal information in their care or charge. This policy sets out to protect personal information in electronic format, gathered by the legitimate monitoring of CCTV systems at WHSCT locations.

7.0 Documentation

The Support Services Department will hold copies of all documentation and records relating to the CCTV systems securely.

8.0 Covert CCTV

The Trust may consider the use of CCTV covert cameras in circumstances where there are reasonable grounds to suspect that a crime/serious misconduct is taking place. In such circumstances the Trust will adhere to the requirement under the Regulation of Investigatory Powers Act 2000.

9.0 Screening Statement

This policy supports the right to have personal information protected and only used in specified circumstance, which are supported in law. Information captured by these systems will only be shared where that sharing is both lawful and reasonable. This policy also affords a right of access to those individuals whose image is captured in line with the individual's rights under the subject access provisions of the Data Protection Act 1998. This policy also complements Article 8 of the Human Right Act through its restrictions on the use of images captured. The policy also applies equally to all individuals whose images are captured irrespective of what their relationship might be with the Data Controller, whether employee, visitor, tenant or agent.

Appendix 1

CCTV IMAGES: REQUEST FORM

Name: ……..

Department: ……..

Tel/Email address: ……

Purpose of Request:(3.1 CCTV Policy)

- ☐ Prevention and Detection of Crime and Disorder;
- ☐ Apprehension and Prosecution of Offenders (this may on occasion include the use of images as evidence in criminal/civil proceedings);
- ☐ Protection of Patient, Staff and Public Health and Safety;
- ☐ Protection of Public Health
- ☐ Protection of Patient, Staff and Public property
- ☐ Investigation of matters relating to Disciplinary Proceedings
- ☐ Protection of Assets
- ☐ Investigation of Incidents/Serious Adverse Incidents

Details of Request

……

……

……

Exact location of Camera :……..

……

Relevant dates:……...

Relevant times:……...

Signed: ----------

Date: ----------

Please return to: Site Management Support Services Department (within relevant sectors i.e. Altnagelvin, SWAH, Omagh, Gransha including community facilities)

Appendix 2

DATA PROTECTION ACT 1998
CCTV Images Subject Access Application Form

This form is to be completed when you request information pertaining to you that has been recorded on Close Circuit TV by the Western HSC Trust. This application should be completed by the person whose image is recorded.

Please enclose photographic ID with a recent photograph of yourself. Please also include the fee of £10 (cheques payable to 'Western HSC Trust') for processing this request. This fee will be refunded if the images are not available or cannot be provided for any reason.

Name …… Mr / Mrs / Miss / Ms

Address……

Postcode……. Contact Telephone No……..…..

Exact Location of camera…….

Relevant dates…….

Relevant Times……..…..

(please provide further information overleaf to help identify the relevant information)

Data Subject Declaration

I wish to access personal data in the form of images that the Western HSC Trust has recorded on its CCTV system. I understand that the Trust may need to contact me to confirm my identity or to request more information from me to find the personal data that I have requested. I enclose the Trust fee and understand that the 40 day reply period will begin once I provide all the information the Trust needs to find my personal data.

I confirm that **I am the Data Subject** and not someone acting on his or her behalf.

I confirm that the enclosed photograph is a true likeness of me.

I understand that CCTV images are only retained by the Trust for 28 days after which they are permanently erased unless required for evidential purposes (in line with the Information Commissioner's Code of Practice)

Signed……..…... Date…….

Please return this form to: WHSCT Information Governance Office, Main Building Tyrone & Fermanagh Hospital, 1 Donaghanie Road, Omagh, Co-Tyrone, BT79 0NS

Please contact the above address if you would like help completing this form

Additional Information

(for example: further details or description of the data subject and / or the incident that occurred; the reason for making this access request; etc..)

Internal Trust Use only

Date application received: _____

Date additional information received (if applicable): _____

Request processed by: _____

Access provided (copy or view only) and date: _____

_____

Reason for refusing access and date: _____

_____

Signature: _____

Appendix 3

Location of CCTV Camera Trust wide

Location	Internal	External
Altnagelvin	256	133
Tyrone County Hospital Omagh	9	13
Tyrone and Fermanagh Omagh	0	17
South West Acute Hospital	314	14
Gransha Hospital,	47	19
Great James St	2	5
William St	0	5
Strabane HC	11	4
Waterside HC	2	2
Limavady HC	2	1
Dungiven HC	3	10