Western Health and Social Care Trust

Closed Circuit Television Surveillance System Policy (CCTV)

September 2021

Title:	Closed Circuit Television Surveillance System Policy			
Author(s):	Sonia Gormley Head of Support Services			
Ownership:	Support Services			
Approval By:			**Approval Date:**	
Original Operational Date:	March 2017		**Next Review:**	November 2022
Revised Dates	November 2020 September 2021			
Version No.:	3	**Supersedes:**	Closed Circuit Television Surveillance System Policy November 2020	
Reference No.:	**Corp17/002**			
Links to Other Policies, Procedures, Guidelines or Protocols:	-Data Protection Act 2018 /GDPR -WHSCT Data Protection/Confidentiality and Freedom of Information Procedures -ICT Security Policy			

Contents

1.0 Introduction

This document sets out the appropriate actions and procedures which must be followed to comply with Data Protection legislation 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 2018 / General Data Protection Regulation (GDPR);
- 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 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 2018

The EU General Data Protection Regulation (GDPR) came into force on 25th May 2018. The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of the new Act apply, like the GDPR, from 25 May 2018.
The new legislation replaces but also builds upon the previous UK Data Protection legislation (Data Protection Act 1998). It contains broadly similar definitions and principles as in the previous Act. There are 6 main principles in the new Data Protection legislation, as follows:

A. lawfulness, fairness and transparency
B. Purpose limitation
C. data minimisation
D. accuracy
E. storage limitation
F. integrity and confidentiality

A 7th overarching principle of 'accountability' introduces a requirement to demonstrate how we are complying with the legislation. In accordance with Article 5(2) of the GDPR the Trust shall be responsible for, and through its policies, procedures and protocols will demonstrate compliance with the Data Protection Principles listed above (Accountability).

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 Defining the Purpose for the use of CCTV

The purposes are decided and agreed by the Trust who, as the data controller for the personal information, uses the cameras to ensure the safety of its staff, the patients/service users who access its services and the general public who access the buildings (for which it has occupier liability for) and grounds. Therefore the purposes of the CCTV system are:

- 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). The purposes are decided and agreed by the Trust who, as the data controller for the personal information, uses the cameras to ensure the safety of its staff, the patients/service users who access its services and the general public who access the buildings and grounds.

Prior to the installation of CCTV cameras on WHSCT premises checks must be undertaken to ensure the installation complies with this policy, the requirements of data protection legislation 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 data protection principles 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 Information Governance Steering Group (IGSG)

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 appendix 1 needs to be completed and authorised. Support Services, estates and IT need to be involved. Support Services/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 4.0, page 10).

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 metadata 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

Data Protection legislation requires that personal identifiable information, held in all formats (including images), is processed in accordance with the rights of individuals, including the right of access; and is processed in accordance with GDPR principles to ensure that data is:

- The purpose of the processing is clearly defined by the Trust
- Collected only for a specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Purpose limitation)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed - (data minimisation)
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay – (Accuracy)
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures - (Integrity and Confidentiality)

The 'purpose' of the WHSCT's use of CCTV equipment to record digital images is set out in section 3.1 of this policy.

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. . It is therefore critical that access to and the security of CCTV images is strictly controlled

to ensure compliance with data protection requirements. This 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

Requests for Third Party Information

Access and disclosure of images is permitted only if it supports the purpose of this policy and is in line with the provisions of data protection legislation or other relevant legislation, some of which are listed at section 1.1. The Trust's CCTV system only holds data for 28 days before it is automatically deleted. Therefore must be made within the 28 days to ensure the relevant footage is secured. Due to the limitations of the systems, a maximum of 24 hours of footage can be saved for each request and where possible requestor should specify a time period.

The Trust does not have the technical ability within its CCTV systems to redact third party information so, as data controller, the Trust must balance all releases of third party information with the data protection rights of the third parties, as described in legislation.

All internal requests for access to images must be made using request form at Appendix 2.

All staff, patients, service users and the public can make a separate request for CCTV footage (when it involves recording of their person) via a Subject Access Request (see section 4.4).

Only persons trained in the use of the CCTV equipment and who have appropriate authorisation may access or view any captured data.

Third Party Images Required for Legal Proceedings

Where information is connected with a possible offence, the PSNI should be contacted in the first instance, who will advise and/or may request the relevant footage. Where the Trust receives any request for information connected to legal proceedings or prospective proceedings, it must assure itself 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.

Internal Disciplinary Proceedings

In line with the Trust's conditions of employment, images may be used for WHSCT disciplinary proceedings and a digital recording of these will be made by nominated Support Services Staff acting at the direction of the Support Services Manager or deputy.

Statutory Disclosures or Disclosures Required by Legislation (other than data protection)

Where images are requested though a legislative requirement (other than data protection and the circumstances above), this must be put in writing to Support Services, detailing the relevant legislation and the relevant section/article which permits disclosure or provides an exemption from data protection legislation.

Forensic Admissibility of Images

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 3.0 is not permitted unless prior approval has been sought and granted from the Director or Assistant Director of Performance Service Improvement.

Requests from PSNI and Regulatory/Investigatory Bodies

The Police Service of Northern Ireland (PSNI) may request CCTV footage from the Trust to investigate crime, whilst regulatory bodies may request footage to review or investigate an incident.

PSNI Requests

When requesting information held by the Trust, the PSNI will usually complete a Form 81 (which outlines the legal basis for the request). However, the Trust appreciates this may hinder a police investigation and it may be necessary to retrieve the CCTV footage immediately. For that reason, the PSNI can request CCTV footage by directly contacting the Support Services Department and the release will reviewed and approved by a Support Services Manager. In the first instance the PSNI will be offered to view the footage and receive a copy, if required. To protect against a fraudulent request, the requesting PSNI officer, should provide and a Crime Reference number (at the time of the request) and photographic identification (when collecting or prior to viewing the footage).

Investigatory Bodies/Regulators

When requesting footage, a regulatory/investigatory body is required to provide justification to the WHSCT 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 an exemption from data protection legislation. When satisfied of the legal basis the Support Services Manager will approve and will decide to facilitate a viewing of the records or a release a copy of the footage.

4.4 Access to Images by Individuals (Subject Access Requests under GDPR)

Applicants requesting access to their recorded image from a WHSCT CCTV system, have the right to do as a right of Subject Access under data protection legislation. All requests for access to personal information held on a CCTV system will be processed through the Information Governance Department. Once applications (Appendix 3) have been validated, Support Services Staff will be tasked with retrieving the electronic data and copying this on to removable media such as a CD. Consideration will need to be given to only providing images relating to the incident in question and the rights of third party not connected to the incident. 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. The Trust recognises that 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 1.1.

Requests will be considered and processed in line with Subject Access requirements under Data Protection legislation. This will require approval to release provided by the relevant service manager or senior officer authorised to approve release of the images.

When approved for release, in most cases the Trust will provide the requestor with the information within one month 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 1 month 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. The requestor must ensure the information is held securely and in line with data protection requirements and securely destroyed when no longer required.

4.5 Covert Surveillance

On occasions, the Trust will need to deploy the use of covert surveillance equipment to detect cases of fraud, abuse and theft from Trust premises. This will only occur in exceptional circumstances, when all other detection options have been explored. A Data Protection Impact Assessment (DPIA) is required and signed off by the Service Lead and forwarded to the Data Protection Officer, Information Governance Department. Any decision will have the method and timeframe agreed by a senior manager and with the authorisation of the Chief Executive.

Where appropriate, the PSNI, Human Resources and Information Governance Department may be involved in the decision-making process in relation to the deployment of covert surveillance. The use of covert surveillance will be the exception rather than the rule.

The Trust has powers to use covert surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA). However this policy does not deal with the use of RIPA in the context of CCTV within the Trust and any proposed use of RIPA should be formally made to the Chief Executive.

Covert surveillance is monitoring conducted in a way which ensures the individuals concerned (data subjects) are unaware that it is taking place. As this raises issues around privacy, there should be clear grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals about the monitoring would prejudice or impact on the validity its use. All decisions around the use of covert surveillance must be formally recorded.

Any covert surveillance will be strictly targeted at obtaining evidence within a set timeframe to ensure the monitoring does not continue after the investigation is complete.

Access to images recorded on the Covert surveillance system will be agreed with the Chief Executive or designated deputy.

Privacy considerations

Consideration should be given to the use of covert surveillance in areas which data subjects would genuinely and reasonably expect to be private (toilets, changing rooms etc). It is acknowledged that this type of surveillance will capture images of individuals not involved in the suspected activity and these recordings will be treated confidentially and securely disposed of, on completion of the exercise This ensures information obtained through covert surveillance is used only for the purpose of detecting crime or where is there a likelihood of substantial and detrimental impact upon patient safety.

Information collected in the course of monitoring will only be used further if it reveals information that the Trust could not reasonably be expected to ignore, such as criminality or a patient safety concern.

The retention period of any recording will be subject to the regional disposal schedule, Good Management, Good Records.

Any decision on the use of covert surveillance may also require consultation with Corporate Support Services, the Governance Department and the Information Governance Department.

Proportionality and Necessity

Within data protection legislation, any decision on the processing of personal data must be proportionate to the rights and expectation of the data subject and be necessary for a specific purpose. It is important to consider and record both in any deliberations on when to use covert

surveillance. As such, a Data Protection Impact Assessment must be completed and a Template DPIA is available on the IG Hub, StaffWest.

When considering a covert recording device, a decision must be made on whether it is proportionate and necessary to use both audio and video recording. A default position would be to use only one or the other and any decision to use both must be justifiable and explained clearly within an email or corporate record, detailing the decision. Again this decision must be agreed by the key senior staff involved in the process.

Data Sharing

In situations where data has been approved and recorded by the Trust, it can be shared with the following bodies/organisations, without consent from the data subjects:

- Police Service for Northern Ireland (for the purpose prevention/detection of crime)
- Any UK police service/authority (for the purpose of prevention/detection of crime)
- Departmental Legal Services (for the purpose of seeking Legal Advice
- Professional Medical or Social care bodies eg NISCC, GMC, NMC (for the purpose of ensure patient and public safety)
- Governmental Anti-Fraud bodies (for the purpose prevention/detection of crime or fraud)
- NI Ombudsman's Office (for the purpose of maladministration or misconduct in public office)
- The Department of Health (for the purpose of ensure patient and public safety; or where there is a theft or misuse of a controlled drug or substance)

This list is not exhaustive and may include other relevant organisations, connected to the investigation. For clarity any additional organisation not on the above list will require approval from the Information Governance Department.

Evidence and Next steps

Inappropriate conduct is considered to be gross misconduct and as such will breach the employment contract provisions and professional guidelines/registration (if the staff member is a registered health/social care professional). The findings from the CCTV will be brought to the relevant Director to decide (in conjunction with senior colleagues as required) whether to instigate the formal disciplinary procedure and commence an investigation. In line with the Trust's Disciplinary Procedure, other Directors may be consulted and consideration will be given to whether it is appropriate to notify and engage the police, the Department of Health NI and regulatory bodies.
The Director will then make a recommendation to the Trust's Chief Executive on the necessary action for the Trust to take. The Chief Executive will choose to formally approve the recommendation and this will be recorded, accordingly.

4.6 Retention and Disposal of Images

Data Protection legislation requires that information held in a form which permits identification of data subjects is kept for no longer than is necessary for the purposes for which the personal data are processed; (Storage Limitation)

In its CCTV Code of Practice, the ICO further states that organisations should ensure that data is retained for the minimum time necessary for its purpose and disposed of appropriately when no longer required.

The Trust complies with Department of Health (DoH) guidelines on the retention and disposal of records. DoH 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.

All images captured by WHSCT operated CCTV systems will be disposed of after 28 days unless there is a statutory or legal requirement to retain for longer than the normal retention period. 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 a copy of the image will be taken and held securely. This will be accessed only by authorised officers until approved for release.

4.7 Tenants within Western Health and Social Care Trusts Property

The WHSCT operates CCTV systems within locations as outlined in Appendix 5 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 and Confidentiality Policy, Freedom of Information procedures, ICT Security Policies and relevant operational procedures

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 2018 / GDPR. However, these images may still be requested and released by virtue of the provisions of the Freedom of Information Act 2000.

6.0 Roles and Responsibilities

As stated in Section 3 Policy Statement the Directorate of Performance and Service 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 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 DoH Retention and Disposal guidelines (GMGR), and that this electronic record is managed as any sensitive personal record would be within the WHSCT.
  - 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 data protection and associated legislation, a common law duty of confidentiality 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 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 General Data Protection Regulation. 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 Trust as Data Controller, whether employee, visitor, tenant or agent.

Western Health and Social Care Trust

Appendix 1

Request to install CCTV within a Trust Properties

PRELIMINARY INFORMATION

Scheme Description:

Facility:

Scheme Objective:

What is 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	☐
Other	☐

Details of request

_____

_____

_____

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)**

Approval by AD Facilities Management- _____ Date _____

Approval by IGSG- _____ Date _____

Originator of Scheme: _____ Date: _____

Name and telephone number of Unit representative to be contacted by Support services and estates teams

_____

I CONFIRM THAT THE ABOVE SCHEME IS BEING ACTIVELY CONSIDERATED WITHIN ___DIRECTORATE AND REQUIRES APPROVAL FROM PSI ASSISTANT DIRECTOR, COSTED AND PRIORITIED BY ESTATES.

SCHEME DIRECTOR _____ Date: _____

Support Services use only

Is there CCTV already installed? Yes or No

If Yes, what is the make and model _____

Who will be responsible for viewing and downloading footage?

Does it comply with CCTV Policy?

Appendix 2

CCTV IMAGES: WESTERN TRUST INTERNAL 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: louise.connor@westerntrust.hscni.net

Appendix 3

DATA PROTECTION ACT 2018 / GDPR
CCTV Images Subject Access Application Form

This form is to be completed when you request information pertaining to you (or a personal individual that you have the legal authority to represent) 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 or by their appointed personal representative.

Please enclose photographic ID with a recent photograph of yourself / the data subject.
Please provide below the details of the person the information / image relates to (the data subject):

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 identity or to request more information to find and identify the personal data / image(s) that I have requested.

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)

I understand, in most cases recent photographic ID will be required to allow the Trust to identify relevant images.

I understand that applications received without the necessary documents (e.g. ID / consent / legal documentation) will not be processed and will be returned

I understand that access to personal information is provided free of charge; however, the Trust reserves the right to charge a fee or to refuse to respond to a request that is manifestly unreasonable or excessive.

I understand that Data Protection legislation allows the Trust up to 1 month to respond to most requests and this may be extended for a further 2 months for complex requests. This time period will begin once I provide all the information the Trust needs to find my personal data / the relevant images.

I confirm that I am the Data Subject and wish to access information relating to me personally; or
I am acting as an advocate on the data subject's behalf and enclose separate written proof of my authority to access this personal information. I also enclose a copy of ID both for myself and ID for the data subject.

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

I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the records / information referred to under the terms of Data Protection legislation / Access to Health Records (NI) Order 1993

I understand that the Western Health & Social Care Trust is no longer responsible for the security and confidentiality of any Health& Social Care records which have been photocopied and supplied to me

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 4

Form 81

Keeping People Safe

OFFICIAL [PARTNERS]

PERSONAL DATA REQUEST FORM

This form contains sensitive information. Do not disclose or disseminate it or the information contained within it without firstly seeking permission from the originator. This form must be handled securely in accordance with the Data Protection Principles as set out in the Data Protection Act 2018.

To (name and position if known): _____

Organisation and Address: _____

The request for information is made by me as an employee for PSNI for the purposes of a police investigation. Section 32 of the Police (Northern Ireland) Act 2000 states that it shall be the general duty of police officers to protect life and property, preserve order, prevent the commission of crimes and where an offence has been committed to take measures to bring the offender to justice.

The personal data I require relates to the following individual(s):
(Include identifying details of the person where known, such as name, address and date of birth)

_____

_____

_____

I have the following information to assist you in locating the personal data and other information:
(Include further details, where available, to assist locating the information sought)

_____

_____

_____

I require the following personal data and other information:
(Describe the information sought)

_____

_____

_____

_____

_____

I require the personal data and other information to assist with my enquiries into:
(Describe the subject of those enquiries as far as is possible without prejudicing them)

_____

_____

_____

_____

_____

Form 81
PB 5/18

OFFICIAL [PARTNERS]

Signed: _____ Rank/Number: _____ Date: _____

Print Name: _____ Post: _____

District/Area/Dept address: _____

Phone: _____ Fax: _____ Email: _____

If the nature of the enquiries is specified above this form must be countersigned by a Sergeant or Supervisor; if the investigation is such that no explanation can be given, this form will be countersigned by a Superintendent.

Signed: _____ Rank/Number: _____ Date: _____

Print Name: _____ Post: _____

This section to be completed by the recipient of request for personal data and information

Response

Please reply to all requests so that we know they have all been considered and to help prevent duplication.

As part of your decision making process, please take into account the requirements upon you/your organisation in relation to the request, for example the Crime and Disorder Act 1998, (any person or organisation has a power to provide information to a relevant authority in order to achieve a crime and disorder objective), the Local Government Act, Children Acts 1889 and 2004,. and other legislation relevant to your organisation.

Signature: _____ Date: _____

Name: _____ Position: _____

Organisation & Dept: _____

_____

_____

The information requested above has been approved for disclosure and is attached*

The information requested above has not been approval for disclosure*

**Delete as applicable*

Please explain why you have decided not to disclose the information so that we know whether you need additional information or for us consider presenting to the Court to obtain a Disclosure Order:

_____

_____

_____

_____

_____

_____

_____

If there is insufficient room please continue on an additional sheet(s).

The subject of the request should not be given any indication that this request has been made prior to consultation with the requesting officer. If your organisation subsequently received a request for a copy of this document (eg under the Data Protection Act or Freedom of Information Act) for this information, please contact the PSNI DP or FOI Officer.

Western Health and Social Care Trust

Appendix 5

CCTV Request

Hospital/Trust_____

Date of Request_____

REASON FOR REQUEST (e.g. evidence gathering, identification. Other) _____

This request for CCTV is made for the purposes of a police investigation/evidential purposes. Only information which is deemed relevant and necessary for the purposes of this information will be requested. The requisite police powers are contained in the following legislation:

Section 32 of the Police (Northern Ireland) Act 2000.

Police and Criminal Evidence (Northern Ireland) order 1989.

Crime Reference Number _____

Investigating Officer_____

NATURE OF ACCESS

☐ View Only ☐ View and Copy ☐ Copy Only

CCTV Operator showing/providing a copy of recorded media

Name (print)_____ Signature_____ Date_____

Location of CCTV Camera Trust wide **Appendix 6**

Location	Internal	External
Altnagelvin	491	147
OHPCC	180	64
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