GIG CYMRU NHS WALES Bwrdd Iechyd Prifysgol Cwm Taf University Health Board	**Reference Number: OP04** **Version Number: 1** **Next Review Date: Formal 01 June 2020** **(Informal annual)**

Closed Circuit Television (CCTV) Policy

Introduction

This policy has been developed to ensure compliance with existing legislation, helping ensure that good practice standards are applied to all CCTV systems in use within the organisation. Application of this policy will not only ensure the organisation complies with the law; it also fosters confidence amongst both public and staff that the organisation takes its responsibilities regarding data protection seriously.

Objectives

- Ensure an appropriate approach to the use of CCTV images within the UHB, ensuring that the legislation is followed appropriately;
- Assist staff with recognising their role and responsibility within the procedure;
- Ensure that managers are aware of their responsibilities.

Operational Date	**Expiry Date**
Immediate – approved by the Quality Safety and Risk Meeting	Formal Review – 01 June 2022 Informal Review – 01 June 2020

Scope

This procedure must be adhered to by all employees within the UHB, including locum staff and contractors.

Equality Impact Assessment	An Equality Impact Assessment has been completed, no adverse impact has been identified to date.
Distribution	Operational managers, Facilities staff and all staff via the intranet (SharePoint) and staff briefing.
To be read by	All managers and staff within Facilities, other managerial staff as needed.

Documents to read alongside this procedure	Identified within the document.
Approved by	Quality, Safety and Risk Committee, March 2019
Accountable Executive / Lead Director (responsible for formal review every three years)	Chief Operating Officer (John Palmer)
Author / Management Lead (responsible for informal review annually)	Acting Assistant Director (Facilities) (Russell Hoare)
Freedom of Information status	Open
If the review date of this procedure has passed, please ensure that the version you are using is the most up to date either by contacting the document author or the Corporate Services Department. **To avoid the use of out of date procedures, please do not print and then store hard copy of this document.** **Out of date policies cannot be relied upon.**	

Amendment Record

If a change has been made to the document, the changes must be noted and circulated to appropriate colleagues.

Detail of change	Why change made	Page number(s)	Date of change	Version	Name of Policy or procedure Author

CONTENTS

Policy Definition
A policy is a high level overall guide, which sets the boundaries within which action will take place, and should reflect the philosophy of the organisation or department.

It provides a prescribed plan for staff to follow, which should not be deviated from.

1. Purpose

Closed Circuit Television (CCTV) surveillance has become a common feature of today's society. Individuals are routinely caught on numerous CCTV cameras whilst visiting shops and offices, travelling on roads and other parts of the public transport network and also, in many cases, whilst in the workplace.

Whilst the use of CCTV continues to enjoy general support amongst the public and staff, it necessarily involves intrusion into their lives as they go about their daily business. There is an expectation that CCTV will be used responsibly and that effective safeguards to protect privacy are in place. Maintaining the trust and confidence of both the public and staff is essential if the benefits of CCTV are to be realised and if its use is not to become increasingly viewed with suspicion as part of a surveillance society.

This policy has been developed to ensure compliance with existing legislation, helping ensure that good practice standards are applied to all CCTV systems in use within the organisation. Application of this policy will not only ensure the organisation complies with the law; it also fosters confidence amongst both public and staff that the organisation takes its responsibilities regarding data protection seriously.

2. Policy Statement

The organisation recognises and accepts its responsibilities and legal obligations in accordance with current legislation and is committed to protecting the rights of its patients, visitors and staff in respect of the operation of CCTV systems.

The organisation fully supports the principles embodied in the CCTV Code of Practice (2017) produced by the Information Commissioner's Office (ICO), and these principles form the basis of the organisation's CCTV Policy.

3. Principles

CCTV systems within the organisation will be utilised:

- as a deterrent against criminal activity and anti-social behaviour;
- to detect criminal activity and anti-social behaviour;
- to assist in the apprehension and prosecution of perpetrators of criminal activity and anti-social behaviour;
- to monitor car parking as a means of maintaining traffic flow to avoid congestion;
- to identify vehicles entering health board sites using automatic number plate recognition (ANPR) to support the detection of criminal or terrorism activity, parking policy and parking enforcement. ANPR where installed will be routinely used to monitor all vehicles entering and exiting health board sites.

CCTV systems will not be used to routinely monitor the workforce to ensure they comply with organisational policies or procedures. However, images of staff may be used if it is identified that staff are possibly involved in criminal activity, gross misconduct or behaviour which puts others at risk, or where the parking enforcement policy, which utilises ANPR systems, are in force to capture any non-compliance of the site parking terms and conditions. All such matters are to be investigated in accordance with Workforce and Organisational Development policies or in the case of parking enforcement in accordance with the parking enforcement policy.

Where an ANPR system is used, a privacy impact assessment will be undertaken to justify its use and show that its introduction is proportionate and necessary. When storing the information and cross referencing it with other databases to identify individuals, databases will be kept up-to-date and accurate. Appropriate safeguards will also be in place to keep the information secure.

4. Scope

This Policy applies to all CCTV systems owned by the organisation, it does not cover CCTV systems owned by external agencies even though they may be located on the organisations property, any such organisations are required to have their own compliant policies and procedures.

5. Legislative and NHS Requirements

It is the policy of the organisation to comply with NHS, UK and EU statutory and other legislative requirements in relation to the use and management of CCTV systems. The key legislation and national guidance documents that must be considered in the development and maintenance of this policy are:

- Data Protection Act (2018);
- General Data Protection Regulation (GDPR);
- CCTV Code of Practice (September 2017);
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Private Security Industry Act 2001;
- Security Industry Authority;
- Traffic Management Act 2004;
- Surveillance Camera Code of Practice 2013;

6. Procedure

This document is the overarching policy for the use of CCTV systems within the organisation. Each CCTV system within the organisation will have its own

administrative and management requirements dependant upon its intended use, environment, type of system, local conditions etc. Consequently, each CCTV system will have its own local CCTV procedure which will document the processes to be followed to ensure the contents of this policy are enforced.

6.1 Proposed CCTV Systems

Using CCTV can be privacy intrusive because it is capable of putting law-abiding people under surveillance and recording their movements within the organisation's premises. Use of CCTV needs to be carefully considered; the fact that it is possible, affordable or has general support from staff or the public should not be the primary motivating factor for the introduction of new systems.

Use of Covert CCTV (Directed) surveillance if required must be requested through the Police. If the request through the police is refused then authority can only be given by the Chief Executive NHS Wales or Department of Health and Social Services, regarding a requirement for directed surveillance activities within healthcare premises for security related matters. This is covered by WHC (2006) 060 following amendments to the Regulation of Investigatory Powers Act 2000 (RIPA), which removed NHS establishments from the schedules of the Act.

All directed surveillance (involving fraud and corruption) should be undertaken on behalf of the NHS bodies in England and Wales by the Counter Fraud and Security Management Service (CFSMS) previously known as the NHS Counter Fraud Service.

A Privacy Impact Assessment (PIA) must be conducted for all proposed CCTV systems. The PIA will be conducted in partnership with the Head of Facilities and the Information Governance Manager. No new CCTV system is to be commissioned without the prior agreement of both these individuals.

All PIAs will be conducted following the guidelines produced by the ICO.

6.2 Register of CCTV Systems

A register of all CCTV systems will be maintained by the organisation and held by the Corporate Services Information governance team. The register will contain details of the location, manager and intended use of each system.

6.3 Recording of Images in General and Treatment Areas

For the purposes of this policy, areas within the organisation will be classed as either general or treatment areas.

6.3.1 General Areas

General areas are those such as corridors or waiting areas where an individual would expect to be seen by other members of the public and by staff not immediately involved in the provision of their care. General Areas covered by CCTV will have "live" images of the area displayed on a CCTV monitor and could be continually monitored and recorded by members of the organisations security team.

6.3.2 Treatment Areas

Treatment areas are those where treatment is delivered and an individual might not expect to be openly viewed by other members of the public or by members of staff not immediately involved in their care.

Images from treatment areas will not be displayed or monitored "live" on a CCTV monitor, nor will they be continually recorded. Recording of images will be initiated as a direct response to any incident where there is a perceived threat to a member of staff, the public or LHB property. Once the incident has been satisfactorily dealt with the recording of images will cease.

6.4 Recording of Conversations

In general, CCTV systems must not be used to record conversations because this is highly intrusive and unlikely to be justified. Guidance provided in the ICO CCTV Code of Practice provides limited circumstances in which audio recording may be justified. One such circumstance would be where a recording is triggered due to a specific threat. Within the organisation, the only CCTV systems to which this will apply are:

- The Body Worn Video System employed by security personnel;
- The Prince Charles Hospital Emergency Care Centre (majors) Treatment Areas CCTV system.

Any other fixed CCTV system which has the ability to record conversations will have this facility turned off.

6.5 Date and Time Stamp

All CCTV systems installed are to be capable of date and time stamping recorded images.

6.6 Advisory Notices

Appropriate signage is important; people must be advised that they are in an area where CCTV surveillance is being carried out. Signs must be clearly visible, readable and of an appropriate size depending on location.

Within the organisation, signs are to be prominently displayed at entrances to CCTV coverage zones and be further reinforced with signs inside the coverage zone.

6.7 Security Industry Authority Licensing Requirements

Under the provision of the Private Security Industry Act 2001, any CCTV operators supplied under contract by external companies must hold a Public Space Surveillance (CCTV) licence. No external contractor will be allowed to operate any of the organisation's CCTV systems without an in-date license being held.

There is currently no requirement for the organisation's staff, who have CCTV operation as part of their routine duties, to be licensed, therefore all authorised University Health Board staff can monitor and review CCTV data. Contract security staff do not routinely man a Security Control Centre operating CCTV, or carry out CCTV surveillance duties.

6.8 Maintaining Integrity of Stored Images

Modern systems will make use of digital technology. The system used to store images must capable of maintaining the integrity of the image. This is to ensure that the rights of individuals recorded by the CCTV system are protected and that the recorded material can be used as evidence in court. If the integrity of recorded images cannot be maintained then this undermines the purpose of the system and it will be considered as unfit for purpose.

6.9 Image Viewing Areas

The viewing of both live and recorded images will be conducted in a restricted area with access to images limited to authorised personnel only. Unauthorised staff or members of the public will not be allowed access to the area where viewing is taking place. The systems manager is the Head of Facilities (Hotel Services) and delegated facilities security personnel.

The viewing of images must be conducted under the supervision of the system manager or nominated representative. Full details of images viewed along with details of the viewer and supervising officer must be recorded for future reference.

6.10 Retention Period for Images Stored on CCTV Systems

The Data Protection Act does not prescribe any specific retention periods for stored images. Rather, retention periods should reflect the organisation's purpose for capturing images.

Within the organisation, each system CCTV Procedure will specify the time for which images are to be retained on the system. This will be no longer than 31 days for any general system and 14 days for any treatment area footage.

Special provision must be made for CCTV systems covering ICT server rooms. In order to maintain accreditation images will be retained for one year.

Where an ANPR system is used, retention periods will be in place for the personal data which will be collected and stored and will be consistent with the purpose the data is being collected for. The information will be kept for the minimum period necessary and deleted once it is no longer required. Individuals will be informed that their personal data is being processed through signage explaining that ANPR recording is taking place and, if possible to do so, the name of the data controller collecting the information.

It will be the responsibility of the individual system manager to ensure that images are deleted after the appropriate time period. In the case of an investigation, whoever has taken possession of images will be responsible for their deletion/destruction upon completion. This responsibility will be emphasised when the images are signed for.

6.11 Retention Period for Internally Disclosed Images

A copy of images that have been disclosed to support an internal investigation will be retained, either digitally or on tape, until such time as the investigation is complete and the footage is no longer required and in accordance with Workforce and Organisational policies.

6.12 Disclosure of Stored Images

No individual will have routine access to stored images for any reason; access must be restricted and carefully controlled to ensure the rights of individuals are preserved.

The primary use of CCTV systems within the organisation is for crime prevention and law enforcement. It is important therefore that stored images can be used by appropriate law enforcement agencies when conducting an investigation, but only where appropriate and in line with the requirements of relevant legislation. Ultimately, stored images should only be disclosed where there is a specific reason for doing so.

The following paragraphs cover the more common requests for disclosure of images:

6.12.1 Data Protection Subject Access Requests

Data Protection legislation provides individuals the right to request access to images of themselves and this is known as a Data Protection Subject Access Request. The University Health Board will have a process to ensure that individuals can exercise this right and in accordance with the organisations Data Protection Policy.

6.12.2 Freedom of Information Requests

It is possible that requests to access recorded images may be made under the Freedom of Information Act. Section 40 of the FOIA contains a two part exemption relating to information from which an individual could be identified. Where requests such as these are concerned, the following should be considered:

- Are the images those of the requester? If the requester can be identified from the CTTV images, the images constitute their personal information. The request should be treated as a Data Protection Subject Access Request and dealt with as explained at paragraph 6.12.1.
- Are the images of other people? If they are, the images can only be disclosed if disclosing the information does not breach the Principles contained within the Data Protection Act.

6.12.3 Requests for Disclosure to the Police

Ad Hoc requests for disclosure of CCTV images by the Police are covered in the organisations protocol – Disclosure of Personal Information to The Police; this is to be adhered to for all ad hoc requests.

6.12.4 Emergency Requests for Disclosure to the Police

The Protocol: Disclosure of Personal Information to the Police is necessarily complex to ensure the principles of the Data Protection Act are adhered to and individuals' rights to privacy are protected.

In emergency situations the time taken to complete paperwork, and obtain official approval, may delay the process of an investigation and may be required in the interest of public protection, which in turn may cause risk or harm to staff and patients, and / or may hinder the timely apprehension of perpetrators of crime. Examples are when incidents occur out of normal 9 – 5 working hours,

when those with authority for facilitating access to stored images are unavailable.

Some examples of this may be:

- when a serious crime is believed to have occurred and Police require immediate access to stored images to assist with the rapid apprehension of the perpetrator;
- when a vulnerable adult absconds and needs to be located quickly in order to prevent them coming to harm.

During such situations it would be justified to:

- authorise access to view stored images in response to an oral request;
- allow completion of formal paperwork to be delayed until as soon as practicably possible after the emergency situation has been dealt with.

Those accepting oral requests in emergency situations will need to make a judgement as to whether access is justified or not, and be prepared to justify their actions once the emergency situation has been dealt with. Full details of the reasons for access, actual images accessed and by whom must be recorded for subsequent completion of formal paperwork.

Those individuals within the University Health Board empowered to accept oral requests are in the first instance the on-call Facilities Manager contactable through the switchboards, senior members of staff and site managers, and will be documented (by post / site title) in the site CCTV system's procedure document.

The individual accepting an oral request will inform the Head of Facilities (Hotel Services) and the Senior Manager On Call of any emergency disclosure of stored images at the earliest opportunity.

6.13 Disclosure of Still Prints and Other information

Still prints and other information, such as car registration numbers, that could be used to identify an individual shall be offered the same protection as any other stored image.

6.14 Further Disclosure of Images

Once recorded images have been disclosed to another body, such as the Police, the receiving body then become the data controller for their copy of the images. It is their responsibility to ensure no further disclosures are made that are incompatible with the original reasons for disclosure, and to comply with the DPA in relation to safeguarding the images.

6.15 Authority to Disclose Information

The individuals with authority to disclose personal information in the form of CCTV images will vary from system to system dependant on its use and location. Consequently, those individuals with the authority to disclose are the on-call Facilities Manager contactable through the switchboards or alternatively are to be named (by post/site title) in the site systems CCTV procedure document.

7. Training Implications

Although there is currently no requirement for the organisation's staff, who have CCTV operation as part of their routine duties, to be licensed and authorised University Health Board staff can monitor and review CCTV data, however it is considered best practice. It would be desirable that University Health Board staff who are required as part of their role and who routinely man a Security Control Centre operating CCTV, or carry out CCTV monitoring and surveillance duties are licensed.

All CCTV operators will be provided with access to the ICO CCTV Code of Practice, the organisation's CCTV Policy and the CCTV procedure for the system they operate. Each operator will sign a register to indicate they have read and understood these documents. Training will be provided to operators in the functionality of any systems they operate.

8. Review, Monitoring and Audit Arrangements

This Policy will be reviewed at least once every three years. An earlier review may be warranted if one or more of the following occurs:

- as a result of regulatory / statutory changes or developments;
- due to the results / effects of critical incidents;
- for any other relevant or compelling reason.

8.1 Annual Review of CCTV Systems

The effectiveness of each existing CCTV system will be reviewed annually to ensure it continues to achieve its intended purpose. If it is not achieving its intended purpose the system will be stopped or modified. A register of reviews will be developed and maintained and audits will be carried out using a CCTV/security audit tool.

8.2 Date and Time Checks

The systems date and time will be checked at least monthly to ensure accuracy.

9. Managerial Responsibilities

9.1 The Organisation

Under the Data Protection Act, the organisation is the Data Controller for all CCTV systems it operates, and is therefore legally responsible for all information processed within those systems. Within the organisation, CCTV is considered a security function, responsibility for which lies with the Director of Primary Care and Mental Health and this responsibility has been delegated to the Head of Facilities .

9.2 Head of Facilities

The Head of Facilities is responsible to the Chief Operating Officer and Assistant Director of Facilities for:

- advising the organisation of any requirements; statutory, legislative or other relating to CCTV;
- developing and reviewing the CCTV Policy and procedures;
- appointing appropriately trained staff to conduct day to day CCTV duties;
- ensuring complaints and disclosure requests are dealt with in an efficient and effective manner;
- maintaining a register of CCTV systems and their annual reviews;
- together with the Information governance team, authorisation of new CCTV systems;
- ensuring the organisation's CCTV operators are provided with adequate training in the use of the systems they operate.

9.3 Site / Department Nominated CCTV System Manager

Each site / department CCTV system run by the organisation will have a nominated system manager responsible to the Head of Facilities for the day to day operation of the system and in accordance with the site system procedure. It will be the responsibility of the department manager to produce a local procedure. Whole site system managers will be nominated by the Head of Facilities. Where there is a departmental system, the system manager will be the department manager unless the Head of Facilities is informed of a named replacement.

Specific responsibilities are to:

- ensure compliance with the documented purpose of the CCTV System;
- conduct an annual review of the CCTV system using the CCTV / security audit tool;

- ensure maintenance of the integrity and security of the CCTV System and the protection of the rights and interests of the public and individuals;
- ensure that disclosure requests are dealt with in an efficient and effective manner;
- maintain a register of authorised users of the CCTV system;
- organise training for CCTV operators in the use of systems they operate;
- check the CCTV systems date and time for accuracy on a monthly basis.

9.4 Information governance team

The Information governance team is responsible for:

- providing annual notification to the ICO of the CCTV systems, and their intended use within the organisation;
- advising the organisation of any requirements; statutory, legislative or other relating to CCTV;
- providing advice and decisions regarding non-routine requests for disclosure;
- together with the Head of Facilities, policy review and authorisation of new CCTV systems.

10. Retention or Archiving

Copies of this policy will be archived and stored in line with the Organisation's Records Management Policy.

11. Non Conformance

Failure to correctly adhere to this policy may result in the dismissal of CCTV stored images presented as evidence in the pursuit of a prosecution or may result in litigation against the organisation for breaches of the Data Protection Act 2018 or the Human Rights Act 1998.

There is a requirement for all staff to comply with this policy and, where requested, to demonstrate such compliance. Failure to comply will be regarded as a disciplinary incident, and will be dealt with under the appropriate University Health Board Human Resources Policy.

12. Equality Impact Assessment Statement

Once the Policy has been assessed each document should have one of the following statements:

Either

This Policy has been subject to a full equality assessment and no impact has been identified.

Or

This Policy has been subject to a full equality assessment and some issues have been identified and highlighted to ensure that due regard and weight is given to them in carrying out this policy (see Equality Impact Assessment Action Plan).

13. References

- Data Protection Act 2018;
- General Data Protection Regulation (GDPR);
- CCTV Code of Practice (September 2017);
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Private Security Industry Act 2001;
- Security Industry Authority;
- Traffic Management Act 2004;
- Surveillance Camera Code of Practice 2013;

Appendix A - Equality Impact Assessment

Approved 12th January 2011 as part of the Policy for the Management, Identification and Authorisation of Policies and Procedures – Operational 1 January 2011

All Public Sector bodies have a legal duty to undertake an equality impact assessment (EqIA) as a requirement of the equality legislation.

EqIA's provide a systematic way of ensuring that legal obligations are met and are a practical means of examining new and existing policies and practices to determine what impact they may have on equality for those affected by the outcomes.

The process itself ensures that individual staff, managers and teams think carefully about, and record, the likely impact of their work on staff, patients and other members of the community.

The need for collection of evidence to support decisions and for consultation mean the most effective and efficient EqIA is conducted as an integral part of policy development, with the EqIA commenced at the outset.

The documentation consider the effects that decisions, policies or services have on people on the basis of their gender, race, disability, sexual orientation, religion or belief, age, Welsh Language and human rights. Assessing impact across a broad range of equality dimensions (not just those required by law), helps organisations to embed equality and human rights and assist them in the delivery of their services.

Policies will not be approved by the Board/Sub Committee of the Board without a completed EqIA Report.

For further information or advice, contact the Diversity, Equality & Standards Manager on 01443 744800.

Form 1: Preparation

Part A must be completed at the beginning of a Policy/function/strategy development or review, and for every such occurrence. (Refer to the Step-by-Step Guide for additional information).

Step 1 – Preparation		
1.	**Title of Policy** - what are you equality impact assessing?	Closed Circuit Television (CCTV) Policy
2.	**Policy Aims and Brief Description** - what are its aims? Give a brief description of the Policy (The What, Why and How?)	To ensure compliance with existing legislation, helping ensure that good practice standards are applied to all CCTV systems in use within the organisation
3.	**Who Owns/Defines the Policy?** - who is responsible for the Policy/work?	Chief Operating Officer
4.	**Who is Involved in undertaking this EqIA? -** who are the key contributors and what are their roles in the process?	Facilities managers
5.	**Other Policies** - Describe where this Policy/work fits in a wider context. Is it related to any other policies/activities that could be included in this EqIA?	• Data Protection Act (2018); • CCTV Code of Practice (September 2017); • Human Rights Act 1998; • Regulation of Investigatory Powers Act 2000; • Private Security Industry Act 2001; • Security Industry Authority; • Traffic Management Act 2004; • Surveillance Camera Code of Practice 2013;
6.	**Stakeholders** - Who is involved with or affected by, this Policy?	All users of University Health Board sites where CCTV is operated
7.	**What might help/hinder the success of the policy?** These could be internal or external factors.	

Form Two – Information Gathering

Is the policy relevant to the public duties relating to each equality strand. Tick as appropriate.							
	Race	Disability	Gender	Sexual Orientati	Age	Religion Belief	Welsh Language
Is the policy relevant to "eliminating discrimination and eliminating harassment?"	√	√	√	√	√	√	No
Is the policy relevant to "promoting equality of opportunity?"	NO	NO	NO	NO	NO	NO	NO
Is the policy relevant to "promoting good relationships and positive attitudes?"	√	√	√	√	√	√	NO
Is the policy relevant to "encouragement of participation in public life?"	NO	NO	NO	NO	NO	NO	NO
In relation to disability, is the policy relevant to "take account of difference, even if it involves treating some individuals more favourably?		NO					

The Human Rights Act contains 15 rights, all of which NHS organisation have a duty to act compatibly with and to respect, protect and fulfil. The 7 rights that are particularly relevant to healthcare are listed below. For a fuller explanation of these rights and other rights in the Human Rights Act please refer to Appendix A: The Legislative Framework.

Consider the relevance of your Policy to these Human Rights and list any available information to suggest the Policy may interfere with, or restrict the enjoyment of these rights.

The right to life
There is no evidence to suggest a link between this Procedure and the restriction or interference of this human right**.**

The right not be tortured or treated in an inhuman or degrading way
There is no evidence to suggest a link between this Procedure and the restriction or interference of this human right**.**

The right to liberty
There is no evidence to suggest a link between this Procedure and the restriction or interference of this human right**.**

The right to a fair trial
There is no evidence to suggest a link between this Procedure and the restriction or interference of this human right**.**

The right to respect for private and family life, home and correspondence
There is no evidence to suggest a link between this Procedure and the restriction or interference of this human right**.**

The right to freedom of thought, conscience and religion
There is no evidence to suggest a link between this Procedure and the restriction or interference of this human right**.**

The right not be discriminated against in relation to any of the rights contained in the Human Rights Act
There is no evidence to suggest a link between this Procedure and the restriction or interference of this human right**.**

Equality Strand	Evidence Gathered
Race	CCTV makes a positive impact on all target groups as it does not discriminate on any particular group and serves to reduce crime, prevent crime and reduce the fear of crime
Disability	CCTV makes a positive impact on all target groups as it does not discriminate on any particular group and serves to reduce crime, prevent crime and reduce the fear of crime
Gender	CCTV makes a positive impact on all target groups as it does not discriminate on any particular group and serves to reduce crime, prevent crime and reduce the fear of crime
Sexual Orientation	CCTV makes a positive impact on all target groups as it does not discriminate on any particular group and serves to reduce crime, prevent crime and reduce the fear of crime

Age	CCTV makes a positive impact on all target groups as it does not discriminate on any particular group and serves to reduce crime, prevent crime and reduce the fear of crime
Religion or Belief	CCTV makes a positive impact on all target groups as it does not discriminate on any particular group and serves to reduce crime, prevent crime and reduce the fear of crime
Welsh Language	CCTV makes a positive impact on all target groups as it does not discriminate on any particular group and serves to reduce crime, prevent crime and reduce the fear of crime

Form 3: Assessment of Relevance and Priority

Equality Strand	Evidence: Existing evidence to suggest some groups affected. Gathered from Step 2. (See Scoring Chart A)	Potential Impact: Nature, profile, scale, cost, numbers affected, significance. Insert one overall score (See Scoring Chart B)	Decision: Multiply 'evidence' score by 'potential impact' score. (See Scoring Chart C)
Race	1	2	2
Disability	1	2	2
Gender	1	2	2
Sexual Orientation	1	2	2
Age	1	2	2
Religion or Belief	1	2	2
Welsh Language			
Human Rights	1	2	2

Scoring Chart A: Evidence Available

3	Existing data/research
2	Anecdotal/awareness data only
1	No evidence or suggestion

Scoring Chart B: Potential Impact

-3	High negative
-2	Medium negative
-1	Low negative
0	No impact
+1	Low positive
+2	Medium positive
+3	High positive

Scoring Chart C: Impact Decision

-6 to -9	High Impact (H)
-3 to -5	Medium Impact (M)
-1 to -2	Low Impact (L)
0	No Impact (N)
1 to 9	Positive Impact (P)

FORM 4: (Part A) Outcome Report

Policy Title:	Closed Circuit Television (CCTV) Policy
Organisation:	Cwm Taf UHB
Name: **Title:** **Department:**	
Summary of Assessment:	This Policy has been subject to a full equality assessment and no impact has been identified.
Decision to Proceed to Part B Equality Impact Assessment:	**No** **Please record reason(s) for decision** **The only impacts identified are positive**

Action Plan You are advised to use the template below to detail any actions that are planned following the completion of Part A or Part B of the EqIA Toolkit. You should include any remedial changes that have been made to reduce or eliminate the effects of potential or actual adverse impact, as well as any arrangements to collect data or undertake further research.					
	Action(s) proposed or taken	**Reasons for action(s)**	**Who will benefit?**	**Who is responsible for this action(s)?**	**Timescale**
What **changes** have been made as a result of the EqIA?					
Where a Policy may have differential impact on certain groups, state what arrangements are in place or are proposed to **mitigate** these impacts?					
Justification: For when a policy may have adverse impact on certain groups, but there is good reason not to mitigate.					
Describe any **mitigating actions** taken?					
Provide details of any actions planned or taken to **promote equality**.					

Date:	
Monitoring Arrangements:	
Review Date:	
Signature of all Parties:	

Appendix B - Training Impact Assessment

If training requirements are identified a policy training impact assessment is to be completed and forwarded to the Workforce and Organisational Development Directorate

1. Will training be required as a result of the policy?

Yes	Proceed to question 2
No √	Operationally, only a very small number of people within the organisation have access to cctv systems. They must go through a formal application process and on installation are fully briefed on the policy and its implications.

2. Please complete the following information relating to training

Course/ policy title	
Course type	
Reference to KSF/NMC Dimensions	
Target Audience (refers to scope of policy)	
Course / policy training objectives	
Course / policy training content	
Duration of course / programme	
Name of trainer (or policy lead)	
Approximate cost of providing training	
Please embed lesson plan, link to e-learning, presentation or other relevant learning material	