

Document level: TW
Code: GR46
Issue number: 3

Camera Surveillance CCTV policy

Lead executive	Medical Director
Authors details	CWP Security Services Manager Corporate Services - 01244 385174

Type of document	Policy
Target audience	All staff
Document purpose	The overall aim of this policy is to ensure compliance with the new Surveillance system operating procedures which are desinged to promote safe environments, protect all users and to assist in the learning process post incident

Approving meeting	Health & Safety Sub-Committee (Chair's Approval)	Date 20-Feb-20
Implementation date	20-Feb-20	

CWP documents to be read in conjunction with	
GR1	Incident reporting policy
MH8	Missing Persons Policy
HR3.3	Trust Disciplinary and procedure policy

Document change history	
What is different?	- Page 4 New quick reference chart 1 - Page 5 New quick reference chart 2
Appendices / electronic forms	Page 10 New formatted CCTV Information leaflet Page 11 New formatted Access information forms Page 14 New Appendix 3 – Internal access record form
What is the impact of change?	<i>Ensure full adherence with new DPA 2018 guidance.</i>

Training requirements	No - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.
-----------------------	---

Document consultation	
Clinical Services	<i>Heads of Service, Modern Matrons, Ward Managers</i>
Corporate services	CWP LEVEN, CWP Estates & Facilities
External agencies	Cheshire Police

Financial resource implications	No
---------------------------------	----

External references	
<ul style="list-style-type: none"> - Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) - Data Protection Act 2018 - Freedom of Information Act 2000 - Traffic Management Act 2004 - The Surveillance Camera Code (2004) 	

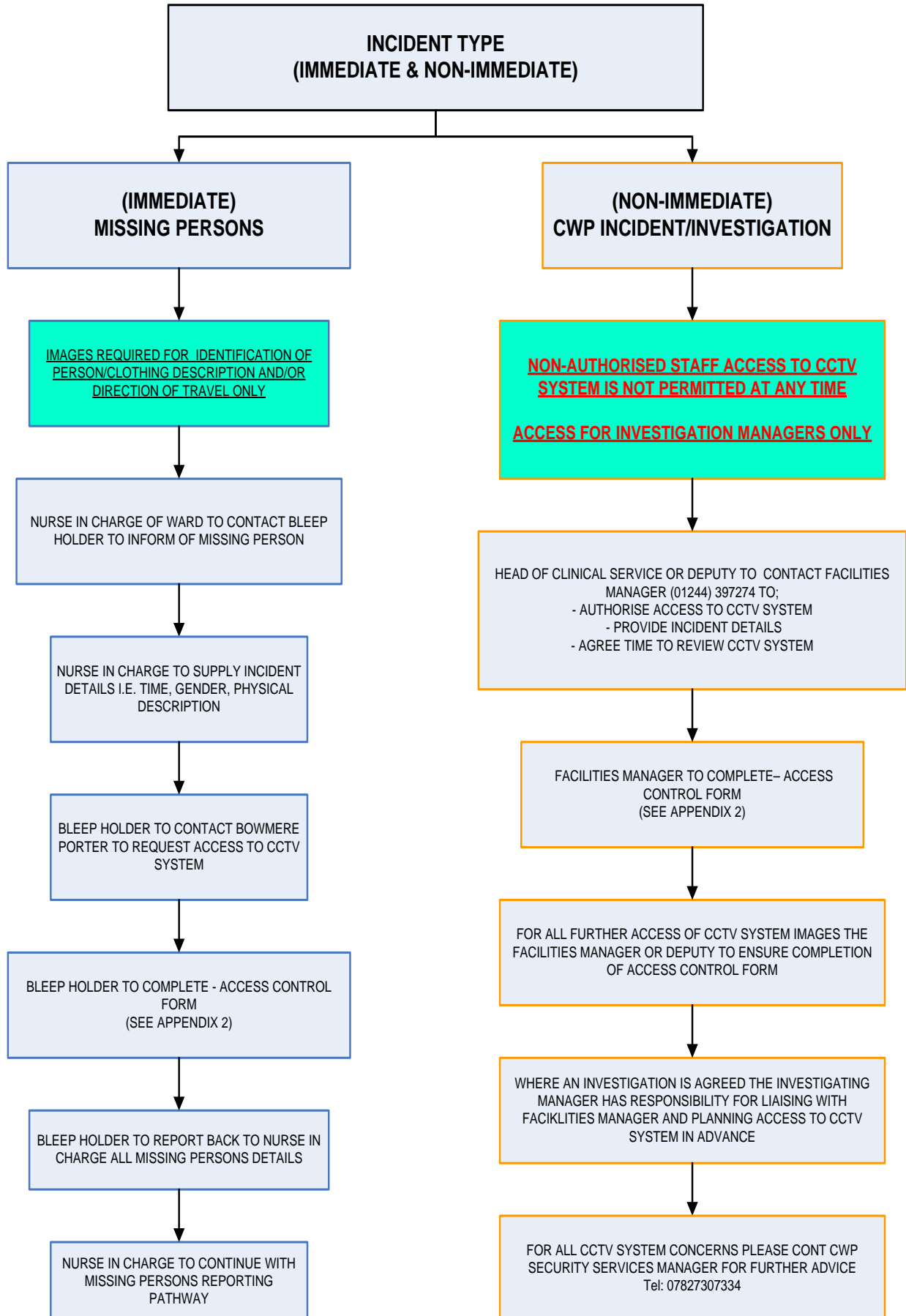
- The Human Rights Act UK (including The European Convention on Human Rights (1998) (2000) (2013))

Equality Impact Assessment (EIA) - Initial assessment	Yes/No	Comments
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
n/a		
Is the impact of the document likely to be negative?	Select	
- If so can the impact be avoided?	Select	
- What alternatives are there to achieving the document without the impact?	Select	
- Can we reduce the impact by taking different action?	Select	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted.		
If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	Low	

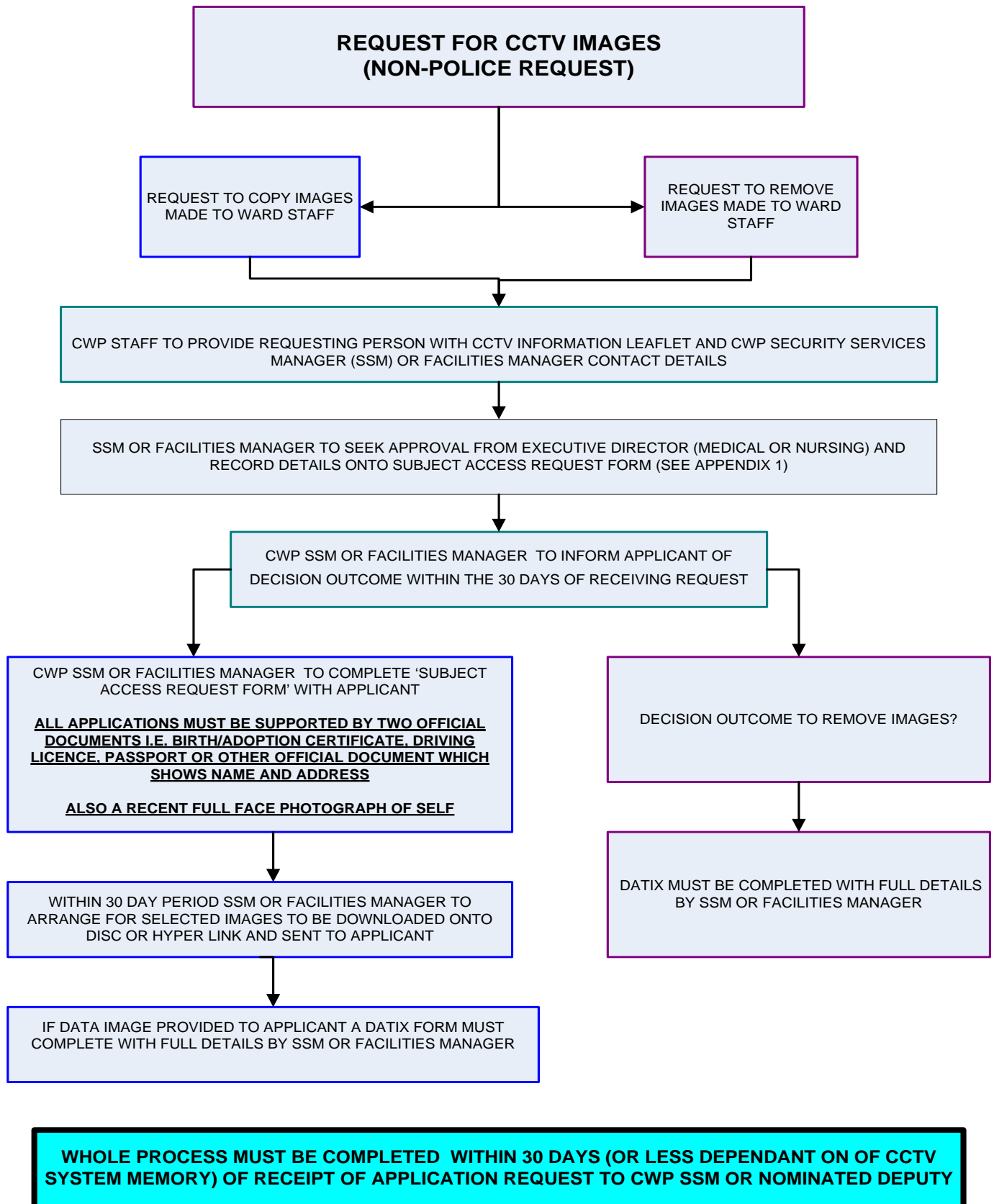
Contents

Quick Reference Flowchart 1 – Actions following an Immediate/Non-Immediate incident.....	4
Quick reference flowchart 2 - External request to access CWP CCTV system.....	5
1. Introduction	6
2. Background.....	6
3. Procedure	7
3.1 Inpatient areas	7
3.3 Missing service users (also refer to MH8 Missing Persons policy).....	7
3.4 Internal incident/investigation reviews (see quick reference chart 1)	7
3.6 The Police and CCTV system	9
3.7 CWP Car Parks.....	9
3.8 CWP premises and signage.....	9
3.9 Complaints.....	9
3.10 Unauthorised access and use	10
3.11 Surveillance image storage and access	10
3.12 CCTV data storage	10
3.13 Equality, Diversity & Inclusion	11
3.14 Definitions	11
Appendix 1 - Application for access to recorded images (subject access request).....	12
Appendix 2 – CCTV system access record.....	15
Appendix 3 - CCTV Information leaflet.....	16

Quick Reference Flowchart 1 – Actions following an Immediate/Non-Immediate incident



Quick reference flowchart 2 - External request to access CWP CCTV system



1. Introduction

Cheshire and Wirral Partnership (CWP) prioritises the safety and security of all service users, staff and visitors and will always ensure to provide environments that are safe and secure. CWP will also work closely with integrated partners where the health, safety and welfare have shared ownership, to ensure co-operation at all levels. To assist in the provision of safe and secure environments the use of surveillance systems such as Closed Circuit Television systems (CCTV) are used across its services. It is therefore essential that any system installed and operated within CWP premises complies with all legal and regulatory requirements and that this is clearly set out within a policy framework.

These guiding principles are designed to provide a framework for operators and users of surveillance systems so that there is proportionality and transparency in their use of surveillance, and systems are capable of providing good quality images and other information which are fit for purpose. A failure on the part of any staff to act in accordance with any provision of this code does not itself make that person liable to criminal or civil proceedings. This code is admissible in evidence in criminal or civil proceedings, and a court or tribunal may take into account a failure by a relevant authority to have regard to the code in determining a question in any such proceedings.

2. Background

As part of the Government's work to strengthen the UK's data protection laws and make them fit for the digital age the General Data Protection Regulation Laws have been amended. The Data Protection Act (2018), which covers CCTV systems, states that all data controllers must have one of six legal bases for their processing activities:

- Consent is one such basis.
- Contractual necessity;
- Vital interest;
- Legal obligation;
- Public interest and
- Legitimate interest.

The Information Commissioners Office (ICO) recommends that all public bodies including health providers who operate and use surveillance camera systems should aim to voluntarily adopt the Surveillance Camera code and comply with its guidance as an example of good practice.

- The public have the right to see CCTV images of them-selves and to ask for a copy of them. CWP must provide them within one calendar month. This is called a Subject Access Request. A requesting person will need to provide details i.e. proof of identity to help the operator to establish the identity of the person in the pictures, and to help them find the images on their system.
- CCTV operators i.e. CWP are not allowed to disclose images of identifiable people to the media - or to put them on the internet - for entertainment. Images released to the media to help identify a person are usually disclosed by the police.
- CWP may need to disclose CCTV images for legal reasons - for example, crime detection. When CWP have given the images to another organisation, then that organisation must adhere to the Data Protection Act (2018) in their handling of the images.
- Public authorities are subject to the Freedom of Information Act 2000. This Act allows members of the public to request official information by writing to the public authority, who must respond within 20 working days. If the images are those of the person making the request, then the request would be handled under the Data Protection Act as a Subject Access Request. If,

however, other people are identifiable in the CCTV pictures, then the images would be considered personal information and it is likely they would be exempt from the Freedom of Information Act.

- CWP should have a retention policy. They should only keep the images for as long as necessary to meet the purpose of recording them

3. Procedure

The use of surveillance systems within clinical areas is not intended as a substitute to or to replace good clinical practice. The use of the systems is intended to support staff and services to promote safe environments. To achieve this, the code of practice sets out guiding principles that should apply to all surveillance camera systems in public places. This policy does not allow for covert / secret surveillance or any activity that would fall to be considered covert surveillance as defined in Regulation of Investigatory Powers Act 2000 (RIPA). The use of covert video or audio devices by NHS organisations when tackling any type of criminal activity will need to fully comply with RIPA Protection of Freedoms Act 2012, for further details please contact CWP Security Services Manager ken.edwards1@nhs.net or tel: 07827307334.

All CWP surveillance camera systems will have effective capability to capture, process, analyse and store images and information at a quality which is suitable for its intended purpose. This includes crime prevention, detection and investigation, and will be capable through processes, procedures and training of system users, of delivering images and information that is of evidential value to the criminal justice system. All exported images and information will preserve the quality of the original recording and any associated metadata e.g. time, date and location. CWP Security Services Manager is responsible for ensuring organisational compliance with Data Protection Standards (CCTV only) and can be contacted for further information.

3.1 Inpatient areas

Where a decision is made to install surveillance systems into inpatient areas or local environment all service users and staff must be advised of its intended purpose and benefits. All new service users must be informed of the surveillance system on admission and must also form part of an induction package for all new staff to the wards or service.

At no time will any surveillance system monitor internal service user bedrooms, toilets or staff rooms. The positioning of cameras will only be situated to allow coverage of general main community areas and corridors. This is to ensure that the system is operated responsibly and effectively, and the likelihood of any breach of individual privacy is not breached.

3.2 Low Secure Services (LSU'S)

As above all LSU's should be referring to this policy for the overall management of their CCTV systems.

3.3 Missing service users ([MH8 Missing Persons policy](#))

If a Missing Persons incident occurs the surveillance system can be accessed by the bleep holder to assist in compiling information to support their safe return or location. (see [quick reference chart 1](#)) The bleep holder must also complete the Internal CCTV systems access record (see [appendix 2](#)).

3.4 Internal incident/investigation reviews (see [quick reference chart 1](#))

Where an incident occurs which may have been recorded on the surveillance system the CCTV footage may form part of an internal review or investigation. Authorisation to access the footage can

only come from the head of clinical services, or deputy head, who must request the footage from the CWP security services manager or facilities manager. Where an investigation is being undertaken only designated CWP staff or the investigative authority such as the Police must be allowed to access and view any stored images. Each time the CCTV images are reviewed a local record should be kept of all details i.e. who, why and when (see appendix 2). At no time must any member of the public have access to any image or be able to view images when the system is operating. Any breach of privacy must be reported as an incident in accordance with CWP policy (please see GR1 incident reporting and management policy).

3.5 Requests for CCTV system disclosure (see [quick reference chart 2](#))

Requests by individuals

The Data Protection Act (2018) affords individuals the right to make a 'subject access request' to obtain copies of media upon which their image may be stored. When a subject access request is made by an individual seeking to view any data image held by CWP, CWP must respond promptly, and in any event, within one calendar month. No charge must be made on any person requesting to have copies of any data images, unless the request is manifestly unfounded or excessive, in which case CWP will be entitled to charge a 'reasonable fee'. CWP are also entitled to charge a 'reasonable fee' following requests for further copies of information/footage previously. (Please see the application form - [appendix 1](#)).

Individuals making a request must provide sufficient proof of identity (see [appendix 2](#)) to satisfy CWP that:

- a) They are the individual purported to be making the request; and
- b) They are the individual within the relevant footage.

If sufficient proof of identity is not provided, CWP are not obliged to provide the footage requested.

All decisions to disclose images / information must be made with regards to safeguarding all persons concerned and / or who may be affected by disclosure of information. If the requested data images involve other identifiable persons CWP are not obliged to comply with the request and should withhold the images. Unless, the other individual has consented to the disclosure of the footage to the individual making the request, or it is reasonable in all of the circumstances to comply with the request. Where this occurs a discussion should take place with the senior nurse to help resolve any outstanding issues. If staff are unsure as to the appropriate response to a request, legal advice should be obtained.

Any persons (non-CWP/Police) requesting access to images held on CWP surveillance systems should be asked to contact CWP security services manager Ken Edwards by email: ken.edwards1@nhs.net or telephone: 07827307334. Authorisation for releasing image must be sought from an Executive either the Medical Director or Director Nursing and Therapies and details recorded onto application form (see [appendix 1](#))

Requests by authorities:

All requests made by the authorities for investigatory purposes must be authorised by the Head of Clinical Service. The Head of Clinical Service has the discretion to refuse any unreasonable request for information unless there is an overriding legal obligation such as a court order or information access rights. Once they have disclosed an image to another body, such as the police, then the

recipient will become responsible for their copy of that image, and must have regard to the various laws and regulations with regards to the data held, including the Data Protection Act 2018 and Human Rights Act 1998

Anyone who makes a request for information regarding CWP surveillance systems should be given an information leaflet explaining the CWP's CCTV procedure process (see [appendix 3](#)).

3.6 The Police and CCTV system

Where it is alleged that a crime has been captured on the surveillance system CWP staff must not attempt to view the images as this may prejudice any investigation by the Police. Where this type of incident occurs the Police must be notified, and any requests to access CCTV images must be processed in line with this policy (see [quick reference chart 1](#)) which takes steps to protect potential evidence to ensure the integrity of images and information should they be necessary for use as evidence in future legal proceedings.

3.7 CWP Car Parks

CWP does not have the power to enforce civil parking enforcement functions as described under the Traffic Management Act 2004. The primary purpose of any surveillance camera system used to monitor car parking areas must be for the safe and efficient operation of the health site by deterring staff from parking inappropriately and also to identify risks to all site users.

Where there are alleged traffic or vehicle related incidents on CWP premises these should be treated as civil matters unless the incident has been reported to the Police for a criminal pathway. If the matter has been reported to the Police and they request access to CWP CCTV system, the request must be processed in line with 3.5 of the policy.(see [quick reference chart 1](#)).

3.8 CWP premises and signage

CWP premises are classified as public areas as such all service users and visitors can expect to be the subject of surveillance in a public place. All service users therefore can rightly expect surveillance in public places to be both necessary and proportionate, with appropriate safeguards in place.

All service users, visitors and CWP staff must be made aware whenever they are being monitored by a CCTV system, who is undertaking the activity and the purpose for which that information is to be used (see [appendix 1](#)). This is an integral part of overt surveillance and is a legal obligation under the 2018 Data Protection Act. Furthermore, such awareness on the part of the public supports and informs the concept of surveillance by consent. Where appropriate, within all areas, signage indicating the use of CCTV and also its primary purpose for safety of all service users and staff must be clearly displayed.

3.9 Complaints

Any person making a complaint regarding CWPCCTV systems must be made aware of the organisational complaints procedures and how to access this through the organisational internet site. Once a complaint has been concluded information must be provided to the complainant about any regulatory bodies that may have jurisdiction in that case such as the Information Commissioners Office (see [appendix 1](#))

Where a complaint is made or, information comes to the attention of a relevant authority or other system operator, indicating that a criminal offence may have been committed in relation to a surveillance camera system. CWP must refer the matter to the appropriate body, such as the police or the Information Commissioners Office (ICO) for any offences under the 2018 Data Protection Act.

If it is believed that that this type of incident may have occurred staff are advised to complete a Datix form and to contact CWP Security Services Manager for further advice.

3.10 Unauthorised access and use

The use or processing of images and information should be consistent with the purpose for deployment, and images should only be used for the stated purpose for which collected. Any staff member who is found to have misused the surveillance system or any image contained on the system will be liable to disciplinary action (please see [HR3.3 Trust Disciplinary policy and procedure](#)).

3.11 Surveillance image storage and access

All CWP surveillance systems must be operated in accordance with The Surveillance Camera Code of Practice 12 guiding principles:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need;
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified;
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints;
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used;
- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them;
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged;
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes;
- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards;
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use;
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published;
- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value;
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

3.12 CCTV data storage

Some CWP surveillance systems have a maximum 28 day rolling loop recording capability. This means that captured images, unless removed in accordance with agreed purposes, will be erased after 28 days. Any images removed for investigatory purposes must be stored securely in accordance with CWP HR Investigations policy.

3.13 Equality, Diversity & Inclusion

CWP is committed to ensuring that, as far as it is reasonably practicable, the way we provide services and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on the basis of age, disability, ethnic origin, gender, gender reassignment, marriage & civil partnership, pregnancy & maternity, religion & belief or sexual orientation.

3.14 Definitions

Surveillance Camera systems has the meaning given by Section 29(6) of the Protection of Freedoms Act 2012 and is taken to include: (a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c)¹.

Public place in accordance with Section 16(b) of the Public Order Act 1986 and is taken to include any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.

Appendix 1 - Application for access to recorded images (subject access request)

Approving Executive details	
Name:	Date of approval:

Section 1 - About yourself
The information requested below is to help <name of health body> to satisfy itself as to your identity and find any data held about you.

Title	Mr	<input type="checkbox"/>	Mrs	<input type="checkbox"/>	Miss	<input type="checkbox"/>	Ms	<input type="checkbox"/>	Other	<input type="checkbox"/>
Preferred title (Pronouns/Dr/Rev)										
Surname / family name										
First name/s										
Maiden name / former name										
Sex (tick box)	Male	<input type="checkbox"/>	Female	<input type="checkbox"/>	Other	<input type="checkbox"/>				
Height										
Date of Birth										
Place of Birth	Town		County							

Your current home address (to which we will reply)			
A telephone number will be helpful in case you need to be contacted	Postcode		
	Tel No:		

If you have lived at the above address for less than 10 years, please give your previous addresses for the period			
Previous address			
Dates of occupancy	From		To
Dates of occupancy	From		To

SECTION 2 - Proof of Identity
To help establish your identity your application must be accompanied by TWO official documents that between them show your name, date of birth and current address.
For example, a birth / adoption certificate, driving license, medical card, passport or other official document that shows your name and address.
Also a recent full face photograph of yourself.
Failure to provide this proof of identity may delay your application

SECTION 3 - Supply of Information
You have a right, subject to certain exceptions to receive a copy of the information in a permanent form. Do you wish to (please select):
<input type="checkbox"/> View the information and receive a permanent copy
<input type="checkbox"/> Only view the information

SECTION 4 - Declaration
DECLARATION (to be signed by the applicant)
I have read and understood the accompanying leaflet explaining (health body) in relation to the

SECTION 4 – Declaration

purpose of the CCTV surveillance and the arrangements for access to recorded images.

I certify that the information that I have supplied in this application is true and accurate and I am the person to whom it relates.

I understand that it is necessary for (health body) to confirm my identity and it may be necessary to obtain more detailed information in order to locate the correct information.

Signed by		Date	
-----------	--	------	--

WARNING A PERSON WHO IMPERSONATES OR ATTEMPT(S) TO IMPERSONATE ANOTHER MAY BE GUILTY OF AN OFFENCE

NOW – Please complete Section 4 and then the CHECK box (section 5) **before** returning the form

SECTION 5 - To help us find the information

If the information you have requested refers to a specific offence or incident, please complete this section.

Please complete a separate box in respect of different categories / incidents / involvement, continue on a separate sheet, in the same way if necessary.

If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section.

Were you (tick below)

A person reporting an (alleged) offence or incident	<input type="checkbox"/>	
A witness to an (alleged) offence or incident	<input type="checkbox"/>	
A victim of an (alleged) offence	<input type="checkbox"/>	
A person accused or convicted of an offence	<input type="checkbox"/>	

Other – please explain

Date(s) and time(s) of incident

Place incident happened

Brief details of incident

Before returning this form, please check:	<ul style="list-style-type: none"> - Have you completed ALL sections in this form? - Have you enclosed TWO identification documents? - Have you signed and dated the form? - Included a stamped addressed envelope for the return of proof of identity / authority documents (where appropriate).
---	---

NOTE: The <health body> reserves the right to obscure or suppress information relating to other third parties (under the terms of the Data Protection Act 1998)

Further Information

These notes are only a guide. The law is set out in the Data Protection Act 1998. Further information and advice may be obtained from the

Information Commissioner

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113

Please note that this application for access to information must be made direct to <health body> and **NOT** to the Data Protection Commissioner.

Signed by		Date	
-----------	--	------	--

A written response to your application will be made within one calendar month.

Please send completed forms to;

CWP Security Services Manager
Churton House
Bowmere Hospital,
Countess Health Park,
Liverpool Road
Chester
CH2 1HJ

Appendix 3 - CCTV Information leaflet

If you require translation services or a copy of this document in other languages, audio tape, Braille or larger print, please speak to a member of CWP staff or e-mail cwp.info@nhs.net

আপনার অনুবাদ পরিষেবা বা অন্য ভাষায় এই ডকুমেন্টের একটি কপি, অডিও টেপ, অক্ষর ব্যক্তির লিখনাদির প্রণালী বা বড় আকারের মুদ্রণ প্রয়োজন হলে, অনুগ্রহ করে CWP কর্মীর একজন সদস্যের সাথে কথা বলুন বা cwp.info@nhs.net এ ইমেল করুন

Os oes angen gwasanaethau cyfieithu neu gopi o'r ddogfen hon arnoch mewn ieithoedd eraill, tîp awdio, Braille, neu brint brasach, siaradwch ag aelod o staff CWP neu e-bostiwrch cwp.info@nhs.net

જો તમને ભાષાંતર સેવાઓની જરૂર હોય અથવા અન્ય ભાષાઓ, ઑડિયો ટેપ, બ્રેઇલ અથવા મોટા અક્ષરોમાં આ દસ્તાવેજની નકલ જોઈતી હોય તો કૃપા કરીને CWP સ્ટાફના સભ્ય સાથે વાત કરો અથવા cwp.info@nhs.net પર ઇ-મેલ કરો

Jeśli wymagane jest tłumaczenie, lub kopia niniejszego dokumentu w innym języku, na kasecie audio, alfabetem Braille'a lub druk większą czcionką, prosimy o skontaktowanie się z członkiem personelu CWP (Organizacja partnerska krajowego systemu zdrowia regionów Cheshire i Wirral) lub przez pocztę elektroniczną: cwp.info@nhs.net

如果您需要翻译服务或者需要该文件的其它版本、录音磁带、盲文或大字体、请和CWP的一位员工提出、或者发电邮至cwp.info@nhs.net

यदि आपको अनुवाद सेवाएँ, या इस दस्तावेज़ की प्रति किसी अन्य भाषा, ऑडियो टेप, ब्रेल या बड़े अक्षरों में चाहिए, तो कृपया CPW स्टाफ के सदस्य से बात करें या cwp.info@nhs.net पर ईमेल करें

All requests for access to any CCTV image must initially be made to CWP Security Services Manager.

For further information please contact;
E - ken.edwards1@nhs.net
T- 07827307334

The law on CCTV systems is set out in the Data Protection Act 2018.

Further information and advice may be obtained from the:
Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113

The information in the leaflet was valid at the date of production 01/11/9 and is due for review in 01/11/21



© Copyright CWP NHS Foundation Trust (DATE)



CWP Surveillance Systems

Closed Circuit Television (CCTV) Systems Information Leaflet

Helping people to be
the best they can be

Introduction

All Surveillance Systems / CCTV used by CWP comply fully with the Data Protection Act 2018 and CCTV Code of Practice.

- Lawfulness
- Fairness
- Transparency

CWP has a policy (GR46) which sets out compliance with all regulatory requirements and also provides further advice regarding access and controls. Please access CWP internet page;

<http://nww.cwp.nhs.uk/Pages/home.aspx> to access a copy of the GR46 Surveillance (CCTV) policy.

CWP has installed CCTV systems within inpatient areas across Cheshire and Wirral. CCTV will only be used in main ward community areas and not in bedrooms or bathroom areas. These systems help support the provision of safe environments which is key for both a service user recovery and also for staff to work within.

The CCTV systems are to be used for the following purpose:

- To help make all health premises safer for those people who visit, work and live in the hospital
- The detection, deterrent and prevention of crime
- To assist in any internal or external investigation process
- To support learning from incidents and CWP Zero Harm strategy

Key points

CWP CCTV systems will only be employed in main ward areas and not in any bedrooms or bathrooms.

CWP CCTV images will only be used to promote safe environment's and will not be used for any other purpose other than that registered with the ICO and noted above.

CCTV system is not monitored and all images will normally be erased after a 28 day period has expired.

Requests for CCTV images to be accessed may be made, please speak to the nurse in charge for further guidance.

Images will not normally be disclosed to third parties unless the provisions Images will not normally be disclosed to third parties unless the provisions of section 29(3) of the Data Protection Act are met. Such circumstances may include:

- The investigation of crime
- The apprehension or prosecution of offenders;
- Where the disclosure is required by or under any enactment;
- By rule of law or by order of the court;
- In connection with legal proceedings (including prospective legal proceedings);
- Is otherwise necessary for the purposes of establishing, exercising or defending legal rights

To contact the Surveillance Camera Commissioner;

2 Marsham Street, 1st Floor, Peel, London SW1P 4DF

<https://www.gov.uk/government/organisations/surveillance-camera-commissioner>

E: scc@sccommissioner.gsi.gov.uk