CCTV Policy

Name	**Code of Practice on the use of closed circuit television & video**
Summary	**This document sets out how CCTV images will be used, held and accessed within the Board**
Associated Documents	**The Data Protection Legislations; The CCTV Code of Practice produced by the Information Commissioner; The Human Rights Act 1998; The Regulation of Investigatory Powers (Scotland) Act 2000**
Target Audience	**All staff of GJF**
Version number	**4.0**
Date of this version	**May 2019**
Review Date	**May 2022**
Date of fairness test	**February 2019**
Approving committee/group	**Health and Safety Committee**
Document Lead	**David Wilson (H&S)**
Document Author (if different)	

Golden Jubilee Foundation Values Statement

What we do or deliver in our roles within the Golden Jubilee Foundation (GJF) is important, but the way we behave is equally important to our patients, customers, visitors and colleagues. We know this from feedback we get from patients and customers, for example in "thank you" letters and the complaints we receive.

Recognising this, the GJF have worked with a range of staff, patient representatives and managers to discuss and promote our shared values which help us all to deliver the highest quality care and service across the organisation. These values are closely linked to our responsibilities around Equality.

Our values are:

- Valuing dignity and respect.
- A 'can do' attitude.
- Leading commitment to quality.
- Understanding our responsibilities.
- Effectively working together.

Our policies are intended to support the delivery of these values which support employee experience.

1. INTRODUCTION

The purpose of this Policy is to regulate the management, operation, and use of the closed circuit television (CCTV) systems monitored by key individuals within the Golden Jubilee Foundation.

This document sets out the appropriate actions and procedures, which must be followed to comply with the Data Protection Legislations in respect of the use of CCTV surveillance systems managed by the Board.

This policy will assist operators of CCTV systems in the Board to understand their legal obligations whilst also reassuring the public and people using our services about the safeguards in place in relation to compliance with relevant legislation

CCTV will be used to help prevent, detect crime including protection of Board premises and to pursue the prosecution of offenders. In certain clinical situations the use of CCTV may assist in the robust monitoring of areas of our premises that may need observing to maintain levels of safety for people using our services.

2. PURPOSE

Within Board premises CCTV is used for the following purposes only:

- To protect Board premises and assets
- To increase personal safety and reduce the fear of crime
- To support the Police in reducing and detecting crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect staff, patients and visitors
- To provide a deterrent effect and reduce criminal activity
- To assist in the traffic management scheme

3. SCOPE

This policy applies to all persons employed by Board and any other groups, who access the site, i.e. visitors, patients, contractors.

4. DEFINITIONS

Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific, limited set of monitors.

5. PRINCIPLES OF THE CCTV SCHEME

All digital recordings that have been used to record information remain confidential, copyrighted at all times and remain the property of the Board

The system shall be operated fairly, within applicable law, and only for the purposes for which it is established or which are subsequently agreed in accordance with the code of practice.

The system shall be operated with due regard to the privacy of the individual.

The public interest in the operation of this scheme shall be recognised by ensuring the security and integrity of the operational procedures.

The purpose of this scheme is also to safeguard the privacy of individuals; the scheme SHALL NOT be used to invade the privacy of any individual in residential, business or other private premises, buildings or land.

Public confidence afforded by the scheme should be based on effective operating cameras; therefore, at no time will dummy cameras be used.

5.1 Use of CCTV Footage for Disciplinary Purposes

Only in the event that recorded CCTV footage reveals activity that gives rise to concern, then the relevant CCTV footage may be considered during investigatory stages of formal disciplinary process, and later used in formal disciplinary hearings, if relevant to the allegations against the employee.

Activity where CCTV can be requested by the Human Resources Department may include:

- Acts which constitute Gross Misconduct in accordance with the Board Disciplinary Policy
- Practices which seriously jeopardise the health and safety of others
- Inappropriate treatment of people who use our services

If such CCTV footage is identified it will be presented to the employee in the usual way, pursuant to the Disciplinary Policy.

Wherever possible, the employee will be given the opportunity to review the CCTV footage and explain or challenge its content. The employee will also be permitted to make representations with regard to the CCTV footage in any disciplinary hearing.

If the Board identifies CCTV footage relevant to formal proceedings, then the timescale (31 days) for the retention of CCTV footage shall not apply. CCTV footage retained for the purposes of disciplinary processes will be retained until the expiry of two years following the completion of all disciplinary procedures, including any appeals process and statutory reporting to professional bodies.

6. DATA PROTECTION IMPLICATIONS

The Board will hold recorded images and these activities fall within the scope of the Data Protection Legislations. The Legislations only applies in circumstances where personal data is processed automatically by reference to a particular individual.

Further guidance on whether specific CCTV activities are covered by the provisions of the Data Protection Act may be obtained from:

Office of the Information Commissioner,
Tel: 0303 123 1113

Information Governance Manager
Tel. No.: 0141 951 5765

The only information, which will be recorded, is the image, date, time, camera number and its reference.

As the Data Protection Legislations provisions cover activities, registration with the Registrar is required in compliance with the Data Protection Principles. These legally enforceable provisions require, amongst other things;

- Processed lawfully, fairly and in a transparent manner,
- Collected for specified and legitimate purposes,
- Adequate, relevant and limited to what is necessary,
- Accurate and where necessary kept up to date,
- Kept for no longer than necessary, and
- Processed in a manner that ensures appropriate security of the personal data.

Directed surveillance is defined in section 1(2) of the Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2009 as,

'Surveillance, which is covert but not intrusive, and undertaken:

a. for the purposes of a specific investigation or specific operation

b. in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of investigation or operation); and

c. otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under the RIPSA to be sought for the carrying out of the surveillance'

The provisions of this code seek to ensure that these requirements are met, and that the Data Protection implications will be assessed when any change in technology or processing activities are considered.

7. DUTIES

7.1 Chief Executive Officer

The Chief Executive Officer has overall responsibility for ensuring that the Board meets its statutory obligations that effective security arrangements are in place and are periodically reviewed.

7.2 **Head of Estates and Facilities**

The Chief Executive has designated the Head of Estates and Facilities with specific responsibility for all security issues, across the Board, with the exception of fraud and corruption.

The Head of Estates and Facilities has nominated responsibility for security matters as defined in the GJF Security Policy. This includes responsibility for ensuring that arrangements are in place to provide an effective and compliant CCTV system.

7.3 **Health and Safety Manager / Nominated Estates Officer**

The Health and Safety Manager and Nominated Estates Officer are jointly responsible for the day to day management of CCTV Systems operated by the Security staff. This includes responsibility for ensuring that the use and management of the system is in keeping with this policy, monitor compliance and report any breaches to the Head of Estates and Facilities.

For the purposes of this policy the Head of Estates and Facilities, the Health and Safety Manager and the Nominated Estates Officer will be referred to as **'Duty Holders'**.

7.4 **Information Governance Manager/Data Protection Officer (DPO)**

Information Governance Officer/DPO shall be responsible for ensuring that all the Board's CCTV schemes are adherent to the Data Protection Legislations and the associated Code of Practice. The Information Governance Manager will also be responsible for updating the Board on any changes in legislation and for ensuring that the Board's registration with the Information Commissioner is accurate and up to date, in line with the General Data Protection Regulation (GDPR).

7.5 **Security Operatives**

Security Operatives will ensure adherence to this Code of Practice. All staff involved in the handling of the CCTV equipment will be made aware of the sensitivity of handling CCTV images and recordings. Staff will be fully briefed in respect of all functions, both operational and administrative relating to CCTV control operation. Familiarisation training by camera installers will also be provided as appropriate.

8. POLICY STATEMENT

In drawing up this policy, the following legislation has been taken in to account:

- The Data Protection Legislations
- The CCTV Code of Practice produced by the Information Commissioner
- The Human Rights Act 1998
- The Regulation of Investigatory Powers (Scotland) Act 2000
- Caldicott Report 1997

All associated information, documents, and recordings obtained by CCTV are held and used in accordance with the Data Protection Legislations and the ICO's Code of Practice 2008

Images obtained from CCTV recordings will not be used for any commercial purpose. Recordings will only be released to the media for use in investigation of a specific crime and with the written consent of the Police. Recordings will not be released to the media for purposes of entertainment.

Archived CCTV images will not be kept for longer than is necessary for the purpose of Police evidence. Once there is no longer a need to keep the CCTV images, they will be destroyed as confidential waste.

Cameras monitor activities on Board premises, car parks and other public areas to identify criminal activity whether occurring, anticipated, or perceived in order to enhance the safety and wellbeing of staff, patients, and visitors. All Security Officers have been made aware of this requirement.

Except when specifically authorised by the Head of Estates and Facilities, using specific Directed Surveillance as stipulated in the Regulation of Investigatory Power Act 2000 (RIPA), staff must not direct cameras at an individual, their property, or a specific group of individuals.

The planning and design of CCTV systems has endeavoured to ensure maximum effectiveness and efficiency but cannot guarantee to cover or detect every incident occurring within the areas covered.

Warning signs, as required by the Code of Practice of the Information Commissioner are displayed at all access routes to areas covered by the GJF CCTV.

9. OPERATION OF THE SYSTEM

9.1 Vetting of Staff who may operate CCTV

All Security Operatives are subject to enhanced vetting via Disclosure Scotland.

9.2 Control and Operation of Cameras

All CCTV Systems will be administered and managed by the Duty Holders, in accordance with the principles and objectives expressed in the Data Protection Legislations and the Commissioner's Code of Practice.

- Operators of camera equipment will act with the utmost probity.

- Only staff with responsibility for using the equipment will have access of the scheme as developed in training and specific operational instructions to staff, and shall comply with the code of practice.

- Cameras shall not be used to look into private property. The Board has adopted operational procedures and technological measures that impose restraints upon the use of cameras with these parts of the code.

- All camera operators are made aware that recordings are subject to routine audit and that they may be required to justify their interest in a member of the public or premises
- The day-to-day management of site wide CCTV will be the responsibility of the Duty Holders.
- Any additional CCTV systems on site are to be managed by the Department in which the systems are located.
- The CCTV system will be operated 24 hours a day, 365/6 days a year.

- Adjustment and alteration to citing or use of cameras should only be made by those with the appropriate authority. Data protection principles should be considered during this process. A record will be kept of all camera locations.

9.3 Viewing of (Live and Recorded) Images by Staff

Viewing of live images on monitors must be restricted to the operator unless specifically authorised by the Duty Holders or Information Governance Manager.

9.4 Covert Recording

Covert recording of CCTV will not be undertaken without the written authority of the Duty Holders with the guidance of the Information Governance Manager.

9.5 Positioning of Cameras and Signs

The location of the equipment must be carefully considered; the following points must be taken into consideration before installing either a new CCTV camera or a full CCTV system.

- Equipment should be situated so they can only monitor the area that is intended to be monitored.
- Equipment should be situated so they can only monitor for the predefined purpose.
- Cameras cannot be positioned in areas where it would be considered private e.g. toilet, changing room, private office. (There maybe exceptions to this in cases of suspicion of serious crime whereby there is a Police involvement)
- If the CCTV area borders private property every effort should be made to ensure the private area cannot be viewed.
- Signs that CCTV cameras operating shall be displayed at the perimeter of the area covered by the scheme and at other key points.
- The signs shall inform the public that cameras are in operation and allow people entering the site to make a reasonable approximation of the area covered by the scheme.
- Signs shall identify the Board and give an official address.

Disclosure of the list of camera locations within this document would put the location of the cameras into the public domain, which would consequently identify where no cameras exist. This would decrease the security of the premises by exposing the vulnerable points, thereby endangering the safety of both patients and staff.

9.6 New Installations

No part of the CCTV system should be initiated, installed, moved or replaced without prior approval by the Duty Holders to approve such schemes. The Information Governance Manager must also be informed.

All schemes are required to meet all the following standards and must be formally approved (as above) prior to any installation;

- Assess the appropriateness of and reasons for, using CCTV or similar surveillance equipment.
- Document this assessment process and the reasons for the installation of the scheme.
- Establish and document the person(s) or organisation(s) that are responsible for ensuring the day-to-day compliance with the operational requirements of such schemes and this policy. This must be done jointly by the Duty Holder and the Information Governance Manager.

9.7 Quality of Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. Upon installation, an initial check should be undertaken to ensure that the equipment performs properly.

The medium on which the images have been recorded should not be used when it has become apparent that the quality of images has deteriorated.

If the system records features such as the location of the camera and/or date and time reference, these should be accurate. When installing cameras, consideration must be given to the physical conditions in which the cameras are located e.g. infrared equipment may need to be installed in poorly lit areas.

Cameras should be properly maintained and serviced to ensure that clear images are recorded. They should be protected from vandalism in order to ensure that they remain in working order. If a camera is damaged, there should be clear procedures for defining the person responsible for making arrangements for ensuring the camera is fixed within a specific time. The quality of the maintenance work should be monitored.

10. CONTROL ROOM

Images captured by the systems will be monitored on-site, in the Security Control Room. Unauthorised personnel or visitors should not be able to see the monitors.

Arrangements for the control room shall include the following requirements to ensure that the control room is secure at all times:

- Access to the CCTV Control Room will be restricted to authorised personnel only.
- Contractors and other visitors requesting entry to the Control Room will be subject to specific arrangements.
- Technical repairs, cleaning and similar activities should be carried out in controlled circumstances.
- Police visits to the Security Incident Control Room shall be pre-arranged and be made in order to interview staff or collect or return recorded discs. Any other visits by police shall comply with the provisions of the code of practice, or the purpose of the visit to be established and confirmed with a liaison officer at the police station and approved by the Duty Holder.
- Any manager outside of direct responsibility to the operation of the control room who requests to view recorded images for any other purpose than that for which the scheme was designed must be directed to the Duty Holder who will seek appropriate authorisation. If this occurs out of normal working hour's access to view should politely be denied or the request should be redirected to the Senior Manager on duty who must consult with and adhere to this policy.
- To ensure that the operation of CCTV systems is managed with the minimum of disruption, casual and non-essential visits by non-security personnel will not be permitted. All visitors must obtain permission to enter from the Security Operatives and must be accompanied throughout the visit.
- Any visit may be immediately curtailed by the Security Operatives if operational requirements deem this to be necessary (i.e. Incident occurring).
- In the event of an out of hours equipment failure requiring access to the CCTV Control Room, the Security Operatives must confirm the identity and purpose of contractors before allowing entry.

11. MANAGEMENT OF HARD DRIVE

The hard drive system automatically stores footage for up to 31 days which is then automatically erased. This helps to ensure that images must not be retained for longer than necessary. In certain circumstances it may be considered appropriate to retain data for a longer period. This will be based on risk assessment conducted by the duty holders. Incidents can be recorded in 'real time' where necessary.

12. MANAGEMENT OF REMOVABLE MEDIA

In order to maintain and preserve the integrity of recordings for use in any future proceedings, the following procedures for use and retention must be strictly adhered to:

- Any CDs used must be identified by a Name, Date, Time, Camera Location and Recording equipment used.
- The CD must be sealed, signed by the controller, dated, witnessed and stored in a designated secure unit.
- A log will be maintained in the Control Room detailing the release of CDs to the Police or other authorised applicants, and a register will be available for this purpose.
- Viewing of data images within the Control Room by the Police must be recorded in writing. Requests by the Police to view images can only be actioned under section 29 of the Data Protection Legislations and the Police and Criminal Evidence Act (PACE 1984)
- If a CD is required as evidence, a copy may be released to the Police.
- The Police may require the GJF to retain stored CD's for possible future evidence. Such CD's will be indexed and securely stored until they are required to be produced as evidence.
- Applications received from external agencies (e.g. solicitors) to view archives/recordings must in the first instance be made to the Head of Estates and Facilities. If appropriate CDs will only be released where satisfactory documentary evidence is produced confirming legal proceedings, a subject access request, or in response to a Court Order.

Still photographs of CCTV images should not be taken as a matter of routine. The taking of each photograph must be capable of justification (prevention of detection of crime), and only done so with permission from the Duty Holder.

All still photographs of CCTV images shall remain the property of the Board. A record is to be kept of the reason for production of the photograph, date, and time, the particulars of production of a live photograph, and information identifying the control room staff member responsible for producing the photograph.

Still photographs of CCTV images released to the Police shall be dealt with by the Police as an exhibit and shall at no time be used for anything other than the purpose specified and identified when released to the police.

Still photographs of CCTV images shall not be kept for longer than is necessary for the purpose of Police evidence. Once there is no need to keep the CCTV images, they must be destroyed as confidential waste.

If images are to be specifically retained for evidential purposes i.e. following an incident, break-in etc.; then these will be retained in a secure place to which access is controlled

13. DISPOSAL OF IMAGES

At the end of their useful life, all DVDs will have their images magnetically erased and disposed of as confidential waste and spot checked for erasure prior to being

destroyed or disposed of. Confidential waste should be shredded or placed in the appropriate bag where Security Operatives will remove the waste.

All relevant documentary evidence, i.e. Access Request forms, monitoring forms etc will be held by the Duty Holders for a minimum of three years. All documentation will then be disposed of as confidential waste.

Any discs or similar passed over to police or third parties will be signed over with a signed agreement that such images will only be used in connection with the reasons stated in the enquiry and when the images are no longer required they (the receiver) will ensure they are returned or that copies received are destroyed. They will also agree not to make any additional copies of the CCTV images, distribute the CCTV images or transfer the CCTV images to any third party without written agreement of the GJF.

14. BREACHES OF THE POLICY

Any breach of the CCTV policy should be reported using the Board's Adverse Incident Form. It will be initially investigated by the Duty Holder, and may result in disciplinary action.

Investigations following breach of the CCTV policy will result in recommendations to remedy the breach where appropriate.

The Board reserves the right to take disciplinary action against any employee who breaches this policy in accordance with the Board's disciplinary procedures.

As a major purpose of these schemes is in assisting to safeguard the health and safety of staff, patients and visitors, it should be noted that intentional or reckless interference with any part of any monitoring equipment, including cameras / monitors/back-up media, may be a criminal offence and will be regarded as a serious breach of Board policy.

15. COMPLAINTS

Any complaints concerning the Board's CCTV system should be addressed in the first instance to the Feedback and Legal Co-ordinator who is based in Clinical Governance. They will review any complaints and issues raised and discuss these with the Head of Estates and Facilities. Both will work together to resolve any issues raised following due process.

16. ACCESS TO DIGITAL IMAGES

16.1 Requests from the Data Subject

The Data Protection Legislations provides Data Subjects (individuals to whom "personal data" relates) with a right to access data concerning them, including data obtained by CCTV. This is known as a Subject Access Request.

Subject Access Requests can be made verbally by the individual or we can ask them to complete the appropriate application form available from the Duty Holder, although verbal requests are now acceptable under GDPR.

The request will then be reviewed by the Duty Holder and the Information Governance Manager to ensure due process is followed when disclosing this information review. There is a duty of care to protect the images of any third parties, taking advice from the Information Governance Manager, or formal legal advice as necessary.

Occasionally people may request to just view the images requested rather than receiving a copy. These requests will always be dealt with on a case by case basis.

Areas which would normally result in permission for access to the viewing area being refused include:

- Where the person wishing to view is not the data subject and/or has no connection with the incident or has no management role relating to an incident.
- Where viewing is purely salacious.
- Where the performance of a member of staff not relating to crime, fraud or the investigation of untoward incidents is involved.
- For occurrences that relate to damage to private property for which the Board has no responsibility.

All accessing or viewing of recorded images will only occur within a restricted area and other employees will not be allowed to have access to that area or the images when a viewing is taking place.

Due to the time and resources needed to view and extract information related to CCTV requests, speculative requests for footage will not be processed.

All Subject Access Requests are free of charge, however, GJF will charge a ‘reasonable fee’ if a request is manifestly unfounded or excessive, particularly if it’s repetitive. The fee will be based on the administrative cost of providing the information.

16.2 Requests from the Police

Police requests may be granted and will arise in a number of ways, including:

- Requests for a review of recordings, in order to trace incidents that have been reported;
- Immediate action relating to live incidents e.g. immediate pursuit;
- Individual police officers seeking to review digital images.

Requests for access to, or for copies of digital images will be requested to the Duty Holder. If the Duty Holder has concerns about the request, it should be discussed with the Information Governance Manager.

At times when immediate action is required out of hours; the Security Operative on duty at the time will act as the first point of contact. If a request is made by the Police or any other person to view or copy digital images, a record will be made of the request and any subsequent viewing or copying of the digital image recorded in the log.

If the police make a request to either view or have a copy of a digital image the Duty Holder must be informed and if appropriate, the incident should be referred through the serious adverse events procedure.

When the police or other investigating authorities wish to seize CCTV evidence they will normally require the original copy (best evidence). If the images are recorded digitally the normal process would be to copy the footage onto disc. In this case a second copy should be made and retained by the Board. In serious cases, the police may wish to seize the hard drive. In such circumstances the Duty Holder should be contacted. Any digital storage devices handed to the police must be recorded in the log and the details and signature of the recipient obtained.

The name and identification will be printed in the log along with the date and time removed and the date and time returned (if applicable). The removal of DVD copies of digital Images will normally be permitted only for a fixed period which will be long enough only for authorised third parties to view them or - where they may be required for evidence - no longer than a court may require them. Digital images that may be required by the Police are to be retained securely until it is confirmed that they are not required, or no longer required for evidential purposes. DVD copies of digital Images will not be released except in these circumstances.

All DVD copies of digital images, which have been viewed by third parties, or are no longer required for evidence, will be retained by the Security Department for appropriate disposal.

16.3 Requests from the public (data subjects)

Individuals (or parties acting on their behalf) seeking access to CCTV footage of themselves should complete an application form (see appendix 2) outlining the day, time and location they wish to view. The Duty Holder should be suitably assured of the identity of the individual before releasing any personal data. The Board must ensure that, before disclosing any personal data, the images do not show any other individuals who may be identifiable.

Where an image does show another individual we must redact that information by blurring the images to disguise the other identifiable persons in order to protect their identity. In the absence of redaction software where others in the footage may be compromised, i.e. have not given consent, the request may be refused. An alternative option may be to provide a written transcript.

17. POLICY DEVELOPMENT & CONSULTATION

This policy was first authorised by the Partnership Forum in 2009 and most recently by the Health and Safety Committee in 2019.

17.1 Changes to the code

Any major changes shall take place only after consultation with relevant interested groups and upon the agreement of organisations with a participatory role in the operation of the scheme.

Any minor change shall be agreed by the Duty Holders in consultation with the Information Governance Manager.

A major change is that which might have a significant impact upon the code of practice or upon the operation of the scheme. A minor change is that which might be required for clarification and shall not have a significant impact. The Information Governance Manager will advise of the implication regarding any proposed change.

18. IMPLEMENTATION

This policy is implemented throughout the Board and is available on Share point.

19. MONITORING

The Board is responsible for ensuring that the scheme is evaluated periodically by a competent person.

Evaluation should be conducted independently or carried out according to independently established criteria.

Evaluation of the scheme should include as a minimum:

- Assessment of impact upon crime;
- Assessment of areas without CCTV;
- Operation of the code of practice;
- Whether the purposes for which the scheme was established still exist;
- Resources committed to the scheme to be taken into account in the future functioning, management and operation of the scheme.

The Health and Safety Committee will monitor the effectiveness of this policy.

Where monitoring has identified deficiencies, recommendations and action plans will be developed and changes implemented accordingly.

All cameras will be maintained and serviced regularly ensuring that the software is up to date.

Management, supervision, and audit of the scheme shall pay particular regard to those aspects of the scheme, which are intended to address individual privacy.

The Duty Holder will carry out audits of the digital recordings, to check that appropriate uses of cameras are being maintained. This will be in addition to a regular random check programme. Audit details are shown in Appendix C.

20. APPENDICES

The following appendices are attached to support the policy

Appendix A – Subject Access Request Form

Appendix B – Provision of Image to 3rd Party or Police

Appendix C - CCTV System Annual Monitoring Checklist

21. REVIEW

This policy will be formally reviewed every 3years, or earlier depending on the results of monitoring, changes in legislation, recommendations from National bodies, or as a result of incident or accident, complaints or claims data analysis or investigation.

CCTV Subject Access Request Form – Appendix A

Please us this form t request any personal information you think may have been recorded on a CCTV camera that the Golden Jubilee Foundation (GJF) is responsible for. Please note that footage is only retained for a specified period, therefore you may wish to contact us before submitting your request.

The Data Protection Act gives anyone the right to ask the GJF for a copy of the personal information that it holds about them for the purposes of providing services to them. This includes CCTV footage. You are not entitled to see information about a third party without their consent. For your protection and the security of the data, the GJF will need to confirm that you are the person whom the data is about and will require proof of your identity before it releases the data. If you ask someone to act on your behalf, the GJF will need proof of this and the person's identity. We may contact you to confirm that you have authorised someone to do this.

When the data subject has provided all the information required to process the subject access request, we will aim to respond promptly and within 30 days of receiving the required information as prescribed under the DPA.

Please send you request to the Security Department, The Golden Jubilee Foundation, Agamemnon Street, Clydebank, Glasgow, G81 4DY.

Note, all personal information provided to GJF will be held and treated in confidence in accordance with the Data Protection Legislation. It will only be used for the purposes of obtaining the requested CCTV footage.

Requester Details	
Name	
Telephone Number	
Job Title/Department (if GJF staff)	
Date Requested	
Address (if member of public)	
Email address	

Note

All images retained within the CCTV system are governed by the Data Protection Act and as such access should only be for specified purposes and not shared for any other reason. Currently our reasons for recording images are for the following:

- To reduce the fear of crime and reassure staff and public.
- To help secure a safer environment for those people, who work, visit and stay in both the hospital and hotel.
- The detection, deterrent and prevention of crime such as:

a. Providing assistance in the prevention of crime
b. Deterring and detecting crime
c. Investigation of fraudulent activity
d. Helping to identify, apprehend and prosecute offenders
e. Providing the Police and the Board with evidence to take criminal and civil action in the courts.
f. Assisting in aspects of traffic management

Information Requested

Date to be reviewed		Location
Time Range	From	To

Reason for Request

Description of what will be reviewed (scope of request)

Identification required
For members of public (non staff) the following information is required: Up to date photograph of the data subject, i.e. the person captured on the footage; Two proofs of identify, e.g. passport, utility bill.

Data subject's agent
This section to be completed only if a person(s) is acting on behalf of the data subject. I can confirm that I am acting on behalf of: …..……..…..…….. And have submitted proof of my authority to do so. Full Name: …..……..…..…….. Address: …..……..…..…….. Post Code: …..……..…..…….. Telephone: …..……..…..……..

Approve / Rejection Information (for official use only)			
Name of Approver		Department	
Job Title		Date	
Approve / Reject			

Reason for Approval / Rejection

Provision of Image to 3rd Party or Police for Legal Proceedings – Appendix B

Date of Incident		Description
Time of Incident		
Camera Identifier		
Operator		

Issued Copy of Image

Reason for Provision			
Date of Creation	Time of Creation	Operator	Tape/CD/DVD Identifier
Crime No/Incident No/		Reason for Access	
Police Officer's Name & Badge No.		3rd Party's Name	
Police Station		3rd Party's Address	
Telephone Number		Telephone Number	
Method of Destruction			
In compliance with the Data Protection Act 2018, I agree to provide safe storage for the CCTV images while in my care and only use them in connection with and for the reason stated in the Enquiry Details above. When the CCTV images are no longer required I will ensure that they are returned or that copies of the CCTV images received are destroyed. I will not make any additional copies of the CCTV images, distribute the CCTV images or transfer the CCTV images to any third party without the written agreement of NHS Golden Jubilee Foundation.			
Signature			
Date of Handover			

Monitoring checklist for users of limited CCTV Systems – Appendix C
(to be completed every 12 months)

We (.....) have considered the need for using CCTV and have decided it is required for the prevention of crime and for protecting the safety of people who use our services. It will not be used for other purposes.

This CCTV system and the images by it are controlled by (insert authorised Manager) ..... who is responsible for how the system is used for notifying the Information Commissioner about the CCTV system and its purpose which is a legal requirement of Data Protection Legislations. Equipment and the images recorded by it are controlled by the Systems Manager who is responsible for how the system is used.

The Information Governance Manager is responsible for notifying the Information Commissioner about the CCTV system and its purpose (this is a legal requirement of the Data Protection Legislations).

Once complete this checklist must be retained by the Duty Holder

	Checked Date	By	Date of next review
Notification has been submitted to the Information Commissioner through the Information Governance Manager and the next renewal date recorded			
There is a named individual who is responsible for the operation of the system			
A system is in place which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can be easily taken from the system when required.			
Cameras have been sited so they provide clear images.			
Cameras have been positioned to avoid capturing images of persons not visiting the premises			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s)			
Images from this CCTV system are securely stored, where only a limited number of authorised person may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images are not provided to third parties.			
Cameras have not been recited or moved or tilted unless discussed and agreed by the Duty Holder.			
The Duty Holders and key staff know how to respond to individuals making requests for copies of their own images. If unsure the Duty Holders and key staff know to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks have been carried out to ensure that the			

system is working properly and produces high quality images.			
The system has been serviced in the last 12 months.			