Security Policy

Name	Security Policy
Summary	The purpose of this policy is to support the aims of the Golden Jubilee Foundation in the delivery of high quality services through provision of a secure environment.
Associated Documents	Health & Safety Policy; Adverse Event Policy; Lone Worker Policy; Management of Violence & Aggression Policy; CCTV Policy; Controlled Drugs Policy; Fire Safety Policy; Mandatory Training (Training Needs Analysis); Information Security Policy; Whistle blowing policy; Patient's Valuables Policy; Protection of Vulnerable Groups (PVG): Vetting and Barring Scheme – Disclosure Scotland
Target Audience	All staff of GJF
Version number	1.0
Date of this version	November 2018
Review Date	November 2021
Date of fairness test	October 2018
Approving committee/group	Health and Safety Committee
Document Lead	David Wilson (H&S)
Document Author (if different)	

The Golden Jubilee Foundation is the new brand name for the NHS National Waiting Times Centre. Golden Jubilee National Hospital Charity Number: SC045146

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.

i:value

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

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.

CONTENTS

1. **Purpose**
2. **Background**
3. **Introduction**
4. **Aims**
5. **Scope**
6. **Roles and Responsibilities**
   - 6.1 Chief Executive
   - 6.2 Head of Estates & Facilities
   - 6.3 Health & Safety Manager
   - 6.4 Accountable Officer (AO) Controlled Drugs (CDs)
   - 6.5 All Directors, Heads of Nursing, Lead Nurses, Managers and Supervisory Staff
   - 6.6 Human Resources
   - 6.7 All Staff
7. **How Security fits in with Other Organisational Functions**
8. **Building and Refurbishment Projects**
9. **Reporting and Controls**
   - 9.1 Incidents
   - 9.2 Security Incident Data Analysis
   - 9.3 Health and Safety Committee
10. **Specific Areas of Security**
    - 10.1 Security of Employee's Property
    - 10.2 Asset Marking
    - 10.3 Patient's Property
    - 10.4 Lost Property
    - 10.5 Board's Right to Search Property
    - 10.6 Access Control and Board Identification Badges
    - 10.7 Closed Circuit Television (CCTV)
    - 10.8 Security Alarm Systems
    - 10.9 Lockdown
    - 10.10 Security of Motor Vehicles
    - 10.12 Keys and security access devices
    - 10.13 Intruders/ Unauthorised/ Suspicious Persons
11. **Data Protection**
12. **Training**
13. **Communication and Implementation**
14. **Monitoring and Compliance with Policy**
15. **Review**
16. **References**

1. Purpose

1.1 The purpose of this policy is to support the aims of the Golden Jubilee Foundation in the delivery of high quality services through provision of a secure environment.

1.2. The standard for security management is that of supporting the Board's strategy to provide high quality healthcare through a safe and secure environment that protects all users including patients, staff, visitors and their property and the physical assets of the Board.

1.3. Security management in healthcare organisations is the responsibility of senior managers, but security itself is the responsibility of every member of staff and presents very real challenges in a culture where staff members are trained to put the needs of the patient first.

1.4 This policy document is intended to ensure that the Board:

- Provide direction and help to those managers and staff who are entrusted to deal with the Board's security provision.

- Support the delivery of high quality clinical and non-clinical services through the provision of a secure environment.

- Comply with relevant legislation, such as the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999

- Regularly review procedures for the physical security of staff, visitors and patients as well as Board premises, equipment and information, including staffs who work in the community.

2. Background

2.1 The Board is committed to providing a secure environment that protects patients, staff and visitors and their property and the physical assets of the organisation so far as is reasonably practical. This policy is part of the Board's commitment to managing its risk agenda and acknowledges its responsibility to the wider community.

2.2 The Board fully accepts its responsibility for security management matters and compliance with legislation. To this end, the responsibility will lie with the Head of Estates and Facilities Management, who will ensure that security management issues are addressed through the Health and Safety Committee, which will be representative of all services.

2.3 This Policy reflects the requirements of all relevant standards and complies with relevant legislation. The Board also fully accepts its responsibility for other persons who may be affected by its activities. The Board will take steps to ensure that its statutory duties are met at all times.

2.4 The organisation has designated individuals whom staff / contractors may contact confidentially if they suspect a security incident has taken place. The nominated individuals for the Board are the Head of Estates and Facilities, Health and Safety Manager and the local Security Operatives.

2.5 This policy does not make reference to information technology security. Please refer to the Information Security Policy.

3. Introduction

3.1 Whilst security management within NHS organisations is the responsibility of senior management, security itself is everyone's responsibility. Security involves all groups of staff at all levels and to be effective it is important to establish at the outset the support of everyone in the organisation. Sensible and cost effective security management initiatives can be taken to reduce risks to all stakeholders by establishing a pro-security culture, which aims to prevent criminal activity. In order to develop appropriate policies and procedures regarding security, co-operation and collaboration with other parties is essential (i.e. other organisations that may use the site, local police, etc.).

3.2 It is therefore important that all those who work in the public sector are aware of, and, wherever possible, protected from the risk of illegal acts involving violence, (threatened and actual), harassment, damage to property or theft.

3.3 The Board already have procedures in place that may reduce the likelihood of breaches of security occurring. These include documented procedures and a system of risk assessment in relation to the physical security of Board premises and assets. In addition, the Board aims to ensure that a risk aware culture exists within the Board and has complied with the general principles outlined within the Security Management Framework for NHS Boards in Scotland.

4. Aims

4.1 The policy seeks to ensure:

- The personal safety at all times of all the Board users;
- The protection of property against fraud, theft and damage, or the potential threat of terrorist activity;
- A safe environment in which the uninterrupted delivery of quality health care can be delivered;
- A partnership with local agencies, e.g. police and local authority for a safe and secure Board environment;
- Staff are provided with appropriate information and/or training on security initiatives and best practice.

5. Scope

5.1 This policy applies to all staff, visitors and patients attending or working for the Board, including contractors and staff working in the community.

6. Roles and Responsibilities

The Board has appointed a number of key employees to have managerial and supervisory responsibilities for ensuring compliance to this policy, legislation and liaison with external stakeholders (e.g. police, NHS Facilities Steering Group).

6.1 Chief Executive

The Chief Executive has overall responsibility for controlling and coordinating security. However, responsibility for management and implementation of this policy is delegated to the Head of Estates and Facilities.

6.2 Head of Estates and Facilities

The Head of Estates and Facilities will:

- Ensure sufficient arrangements are in place for the effective running and delivery of a security service within the Board;
- Be responsible for taking reports and proposed action plans to the Chief Executive and the Executive Team for consideration and implementation;
- May delegate various responsibilities to an appropriate manager and will report any amendments of this policy to the Board.

6.3 Health and Safety Manager

6.3.1 The Health and Safety Manager is responsible for ensuring:

- Effective liaison with persons responsible for security at other local NHS organisations;
- Security staff are adequately trained and provided with the appropriate Personal Protective Equipment (PPE) to allow them to carry out their roles in confidence and as safe as possible;
- Security Officers respond to incidents in the appropriate manner and ensuring that all such incidents are reported via the Board's Datix incident reporting system;
- The effectiveness of the CCTV, intruder alarms, access controls, lighting and key related access processes through monitoring(in conjunction with Estates Management and Security Officers)

6.3.2 Security Officers should be informed of any events and issues; they in turn will notify and report findings to the Health and Safety Manager as appropriate.

6.3.3 Security Officers are responsible for assessing security risk and for immediate action and notification of incidents. Where possible, in the first instance, they are to attempt to dispel and control incidents sufficiently that the risk is reduced and care can continue. In addition, they are the initial liaison for the police etc. should they be requested to attend: following their liaison with the police they must notify the Health and Safety Manager by an appropriate means i.e. telephone, email etc.

6.4 **Accountable Officer (AO) Controlled Drugs (CDs)**

6.4.1 The Chief Pharmacist is the Accountable Officer (AO) for the Board. The AO is ultimately responsible for all aspects of the safe and effective use of CDs within the Board. Any staff concerns about individuals or processes in the handling of CDs should be reported to the AO. See also the Controlled Drugs Policy.

6.5 **All Directors, Associate Nurse Directors, Clinical Nurse Managers, Department Managers and Supervisory Staff**

6.5.1 It is the responsibility of directors and managers to ensure that they and their staff fully comply with the security policy, and follow the incident reporting policy and system when a breach of security occurs.

6.5.2 Security is a responsibility of managers who must undertake preventative measures for the safety of staff, users and property.

6.5.3 Managers should implement a procedure to record details, of any valuable property left in their care, ensuring that arrangements are made to secure the department out of working hours, together with the safe custody of keys.

6.5.4 Managers should keep records of all keys issued to staff and report the loss of keys to the Security Staff.

6.5.5 Managers should advise the security department of any changes within departments that may adversely affect the overall security of the premises.

6.5.6 Managers should ensure all staff employed by the Board, or from other organisations working in the Board, including contractors and visitors, will wear an identification badge/ card at all times.

6.5.7 Managers must ensure that all members of staff are made aware of the above policy and fully understand its content and their responsibility under the policy and that they are required to communicate this to their staff.

6.5.8 To enable effective security management, senior managers must monitor and report on the workplace to ensure that the Board is protected. Where security management risks are identified the manager must ensure that these are assessed, eliminated or minimised, so far as is reasonably practicable.

6.5.9 Contractors are expected to adhere to the Board Security Policy and Board staff letting and managing contracts/contractors are responsible for ensuring security is maintained.

6.6 **Human Resources (HR)**

6.6.1 HR will ensure all pre-employment screening is undertaken and a robust vetting procedure is adopted in accordance with NHS requirements.

6.7 **All Staff**

6.7.1 All staff members have a responsibility to report any breaches or incidents of a security nature. The main forum for this will be via the Board’s Incident reporting system (Datix). Where urgency dictates, incidents can be reported via Security

Operatives.

6.7.2 All staff members of the Board have a duty to be aware of the Security Policy and to adhere to it. Staff must co-operate with management to achieve the aims, objectives and principles of the security policy. Great emphasis is placed on the importance of co- operation from staff in observing security measures and combating crime at all levels. Security concerns, incidents including incidents of violence and aggression should be reported immediately to line managers and an incident report should be completed as soon as possible.

6.7.3 Staff should be aware of their responsibilities in protecting at all times the assets and property of patients, visitors, colleagues and other Board users, as well as the safety of the Board's assets and property.

6.7.4 Where specific security procedures exist, staff must abide by them at all times. Where staff know or suspect a breach in security, they must report it immediately to their manager. Once escalated, a Datix report form must be completed detailing the breach.

6.7.5 All staff members are reminded that it is an offence to remove property belonging to the Board without written authority. Failure to seek authority from their line manager could result in disciplinary action or criminal prosecution.

6.7.6 Staff members are required to wear an identification badge whilst on duty for the Board; this also applies to those that are at work in the Community.

6.7.7 Staff members are responsible at all times, for the protection and safe keeping of their own property. The Security Staff will if requested, provide staff with advice on the security of their property, including motor vehicles or other modes of transport. Any theft of private property must be reported to police without delay. If property has been brought on site, it is at the owner's own risk and therefore it is their responsibility to report the incident.

7. How Security fits in with Other Organisational Functions

7.1 The overlapping interests of security with the requirements of Health and Safety legislation and the preventive and protective elements of fire safety are recognised. The Health and Safety Manager will maintain close liaison with the Security Staff, Board Fire Officer (where applicable) and all managers and supervisors to ensure that in implementing security any threat to life, property and the means of escape are fully considered in conjunction with Fire Policy and guidelines.

7.2 Advice on security matters should initially be sought from an immediate supervisor or manager who may refer to the Health and Safety Manager who will have recourse to relevant security manuals. The NHS publishes information on security/personal safety, which will be held and distributed as appropriate by the Health and Safety Manager. Reference should be made to the Fraud/Whistle Blowing and Violence and Aggression Policies where appropriate.

7.3 It is acknowledged that all members of staff have a right, as individuals, to refer to the police if they feel threatened in any way in the course of carrying out their duty. Without seeking to prejudice that right, the automatic involvement of the police may not always be in the interests of involved parties, the Board or the police themselves. Therefore it is suggested that in **non-emergency** situations, staff should consult with their line managers in the first instance. Similarly, it is recommended that, where practical, line managers discuss incidents with the Health and Safety Manager prior to a referral to the police.

8. Building and Refurbishment Projects

8.1 The Board will ensure suitable advice regarding security is sought and that appropriate security measures are incorporated into all buildings projects and developments.

8.2 All capital and revenue projects involving changes to, or the introduction of, security devices will be carefully considered by the Estates Management Team.

9. Reporting and Controls

9.1 **Incidents**

9.1.1 All security incidents should be reported by telephone on 5116 or bleep to the Security Staff (on shift) number 0027. For immediate contact the Security Team are contactable via mobile phones – numbers available via Switchboard.

9.1.2 Incidents should be recorded, by the reporting department, on the Board's electronic Incident Report form (DATIX). The Manager for the area will be required to investigate the incident and the Health and Safety Manager should be alerted.

9.1.3 Security Officers are responsible for completing Board's Incident Report form when an incident has occurred in a public area.

9.2 Security Incident Data Analysis

9.2.1 Individual incidents will be reviewed by the Health and Safety Manager upon receipt to ensure that they have been completed in accordance with this policy.

9.2.2 Incident figures will be collated through the Board's incident reporting procedures The Health and Safety Committee will review summaries of security incidents and trends analysis on a consistent basis. Where this review identifies areas at a high risk of incidents, further support, including advice and additional training will be provided by the Health and Safety Manager**.**

9.2.3 Significant risks will be recorded and placed on the Risk Register with appropriate controls and risk treatment plans in operation within the directorate, who will ensure adequate business planning to reduce or remove the risk, so far is reasonably practicable.

9.3 Health and Safety Committee

9.3.1 The Board has an established Health and Safety Committee with representatives from all areas of the Board. The Group has agreed terms of reference and will:

- Receive information and reports from the Health and Safety Manager in the form of a security report on incidents and all security matters when requested and any significant information will be included within the annual Health and Safety Committee report.
- Jointly identify any anticipated need for action or, where applicable, escalate issues for discussion at Board level through the chair of the Health and Safety Committee.
- Review current policy and processes with a view to upgrade or improve security measures and hardware.

10. Specific Areas of Security

10.1 Security of Employee's Property

10.2.1 Employees are advised not to bring large amounts of money, valuables to work or any item that might present a security threat/ risk to work.

10.2.2 Where changing facilities are provided for employees, the room should be kept locked to prevent unauthorised access. Lockers, when available, should be used for all personal property. In the event of deficiencies or un-serviceability, the Estates & Facilities Help Desk should be informed via the line manager.

10.2.3 All instances of theft of property should be reported immediately to the manager and on an Incident Report form (Datix).

10.2.4 All staff members are to be made aware that all money and valuables are brought onto Board premises at the owner's own risk. Staff have a duty to take reasonable steps to ensure the security of their personal belongings whilst at work, and take consideration of personal items that they bring into the work environment

10.3 Patient's Property

10.3.1 Patients' property should be handled in accordance with the Board's arrangements for managing patient's valuables policy and secured accordingly.

10.3.2 No responsibility can be accepted by the Board for the loss of personal property that is not stored securely.

10.3.3 Suitable and sufficient documentation should be completed to record personal items of patients while on Board premises. In addition, guidance should be given to patients by the Board and individual departments on the suitability of bringing valuable items onto Board premises. However, it is the responsibility of the patients, visitors and contractors to make sure that their personal property is secure.

10.4 Lost Property

10.4.1 All found property should be immediately handed to the Security Staff. Compliance to the Boards' Standing Financial Instructions for lost property shall be implemented

10.5 Board's Right to Search Property

10.5.1 Legally the Board is entitled to authorise trained security operatives with powers to search lockers, property etc. following declaration of an incident where an item (of any description) is reported missing.

10.5.2 Security Officers have the right to ask for staff to empty pockets, bags, lockers etc. to rule out any alleged offence on Board premises.

10.5.3 Security Officers do not have the right to frisk, touch or physically search a person. This function is the sole responsibility of the Police. Should security operatives suspect a person is concealing an item on their person, the police will be informed and requested to attend for a search.

10.5.4 Security Operatives are not to compromise any situation where a crime scene scenario may apply: crime scene integrity must be retained for the police. If at any time the Security Operatives suspect a crime has taken place, the Operatives must notify the Health and Safety Manager to secure the crime scene and preserve evidence.

10.5.5 Board employees have the right to refuse a search of their property or to empty pockets etc., but in doing so this will lead to HR and police contact to conduct a search. The purpose of the search is for the protection of staff to minimise the risk of allegations made by patients, members of the public and other staff.

10.6 Access Control and Board Identification Badges (Appendix 2)

10.6.1 Up to date photographic identification should be worn at all times when on site. A computerised photo ID badge scheme combined with access control proximity card operates in the Board. Staff responding to a major incident must bring photographic ID with them, as this will be needed to access the hospital as access may be restricted by the police.

10.6.2 Staff members who are not wearing an identification badge should be challenged and requested to wear their badge. Failure to visibly wear a personal ID badge is a disciplinary matter.

10.6.3 The Health and Safety Manager in consultation with the Head of Estates and Facilities and Nursing Managers are able to determine levels of security access to buildings and internal areas throughout the Board.

10.6.4 Identification badges are the property of the Board and under no circumstances should they be worn by, or transferred to, any other person than the holder. Staff members are not to allow any other individual to use their access card/fob at any time and should not allow any other person passage through any access point. All staff entering a restricted area are required to present their card prior to entry.

10.6.5 Staff members are not to leave controlled doors open or unattended at any time. Visitors needing access to restricted areas should be escorted at all times.

10.6.6 Persons not wearing an identification badge and those whose identity is unknown must be challenged and asked to account for their presence. This should be done politely and quietly and in a helpful manner. Suspicious incidents must be reported to Security as soon as possible and an Incident Report completed.

10.6.7 Lost or stolen identification badges and all problems relating to the proximity card system (including lost, missing or stolen cards) must be reported to the Line Manager and Security Staff immediately.

10.6.8 When a staff member leaves the employment of the Board, it will be the responsibility of the departmental manager to retrieve the identification badge and arrange for the deactivation and destruction of the card

10.6.9 The operational management and control of this system is kept within Estates and Facilities. The protocol for effective management is followed. In addition, alterations to the permissions of access may be altered dependent on need.

10.7 Closed Circuit Television (CCTV)

10.7.1 The Board will comply with legislation such as the Data Protection Act and other related legislation that ensures full compliance with the law. This will be controlled by the Estates and Facilities directorate to ensure that propriety and professional use is maintained.

10.7.2 In addition the Health and Safety Manager in conjunction with the Estates Managers will assist and ensure that the Board's protocol for controlled use of the CCTV systems throughout the Board premises is followed in accordance with the Boards' CCTV policy.

10.8 Security Alarm Systems

10.9.1 It is the responsibility of Heads of Department or a designated member of staff to activate their local alarm system on leaving the building or deactivate the alarm on re-entering the building. Switchboard will notify the Security Operative should an alarm be activated within a specified area.

10.10 Lockdown

10.10.1Lockdown is the process of controlling the movement and access, both entry and exit, of people (NHS Staff, patients, visitors and public) around Board sites or other specific Board buildings or areas in response to an identified risk, threat or hazard that might impact upon the security of those on site or the capacity of the organisation to continue to operate. A lock down is achieved through a combination of physical security measures and the deployment of security personnel.

10.10.2 The Health and Safety Manager in conjunction with the Estates Management Team and Security Staff will co-ordinate an electronic system to establish up-to-date site, buildings and security profiles.

10.11 Security of Motor Vehicles

10.11.1 All motor vehicles used by employees, patients, and visitors along with other outside agencies must park in the authorised parking areas which have been provided by the Board.

10.11.2 The security of motor vehicles owned by employees, patients and visitors is the responsibility of the owner of the vehicle. Whilst the Board provides parking facilities, it does not accept liability for any theft, loss or damage to motor vehicles or their contents when they are parked on the Board sites.

10.12 Keys and security access devices

10.12.1 Keys and security access devices are important security items and must be kept on the person at all times. Under no circumstances should these be left unattended e.g. on desks, in key holes of doors, or borrowed by unauthorised personnel.

10.12.2 Managers have a responsibility to ensure that their department is locked when unoccupied and for ensuring that only named members of staff have keys to that site.

10.12.3 Duplicate keys and security access devices should be held in a locked cupboard/cabinet.

10.12.4 Arrangements must be made to ensure that adequate arrangements are in place for opening and closing of departments, which are cleaned by domestic staff outside normal working hours.

10.12.5 Replacement keys are only to be obtained via the Estates department and must not be replicated locally. Reimbursement for replacement keys will be met by the requesting department.

10.12.6 The issue of Master suited key systems and keys and devices should be severely limited and only issued to those staff responsible for whole areas of a building.

10.12.7 Staff members who hold access devices must also be made aware that losing them could be a high security risk and they are accountable for them.

10.12.8 If access devices are lost, staff may be charged for their replacement, dependent upon the circumstances of the loss.

10.13 Intruders/ Unauthorised/ Suspicious Persons

10.13.1 If an unauthorised person/s is found on the premises, Security Officers have the authority to ask them to leave, escort them from the premises or to notify the police, depending on the situation presented at the time.

11. Data Protection – Staff should refer to the list of information governance and information security policies available on Q-Pulse.

12. Training

12.1 The requirement for Security related training, information and instruction will be determined by the Health and Safety Committee and/or on an individual department basis justified by risk assessment and reflected within the training needs analysis.

13. Communication and Implementation

13.1 The policy will be made available on Q-Pulse.

13.2 The approved policy will be notified to relevant staff groups and committees.

14. Monitoring and Compliance with Policy

14.1 Policy effectiveness will be monitored by Health and Safety Committee through feedback from Committee members and security representatives.

15. Review

15.1 This policy will be reviewed in 3 years or earlier as a result of staff change, local or national initiatives.

16. References

- The Health and Safety at Work Act (etc.) 1974 (2) and (3)
- Management of Health and Safety at Work Regulations 1999
- Reporting of Injuries Diseases and Dangerous Occurrence Regulations 2013
- Security Management Framework for NHS Boards in Scotland – Health Facilities Scotland 2008
- Security Services Standards for NHS Scotland
- Not Alone- guidance for the better protection of lone workers in the NHS