Security Management Policy

Policy Information

Policy number: 1138
Classification: Corporate
Supersedes: Version 1.0
Version number: 2.0
Date of Equality Impact Assessment: 27/02/2026

Approval Information

Approved by: Health & Safety Compliance Group
Date of approval: 08.06.2026
Date made active: 10.06.2026
Review date: 08.06.2029

Summary of document:
This policy aims to provide a framework which can be used at all levels across the Health Board to assess and continually strive to improve the level of security at all the Health Board sites.

Scope:
All health board, Clinical Care Groups / Functions and staff.

To be read in conjunction with:
170 – Lone Worker policy – opens in a new tab.
186 – Business Continuity Planning Policy – opens in a new tab.
285 – Violence and Aggression Policy – opens in a new tab.
293 – Smoke Free Policy – opens in a new tab.
323 – CCTV Policy – opens in a new tab.
708 – Control Drugs Governance Policy – opens in a new tab.
749 – Lockdown Policy – opens in a new tab
815 – Counter Fraud, Bribery and Corruption Policy – opens in a new tab.
836 – Information Governance Policy (Data Protection Policy) – opens in a new tab.
837 – Information Communication Technology (ICT) Security Policy – opens in a new tab.
894 'Putting Things Right' Management and Resolution of Concerns Policy (Incidents, Complaints and Claims) – opens in a new tab
982 - Incident, Near Miss and Hazard Reporting Procedure – opens in new tab
1435 – Site Security Standard Operating Procedure (Currently in draft).
Information Governance Policies.

Owning group: Security Management Group Membership *07/04/2026*
Executive Director: Director of Allied Health Professions and Health Science

Reviews and updates:
1 – New policy
2 – Full review 08.06.2026

Keywords
Theft, fraud, access control, keys, violence, aggression, asset, staff safety, prevent, contest, lost keys, lost identification, ID badge, security.

Glossary of terms
Security - The protection of people, information, material activities, reputation and all assets.
Lockdown - The process for controlling movement and access – both entry and exit – of people (NHS staff, patients and visitors) around a Health Board site or other specific Health Board building/area in response to an identified risk, threat or hazard. A lockdown is achieved through a combination of physical and electronic security measures and the deployment of security personnel and other Health Board personnel.
Health Board Identification (ID) Card - A photographic card issued on employment
Access Control / Swipe Card - A card issued with access control to be used on wireless access control systems
Health Board (HDdUHB) - Hywel Dda University Health Board
CNI - Critical National Infrastructure
CPNI - Centre for the Protection of National Infrastructure
SOP - Standard Operating Procedures
SPOC - Single Point of Contact
SA - Security Advisor
SM - Security Manager
CPNI - Critical National Infrastructure
ICT - Information communication technology
MTA - Marauding Terrorist Attack

Table of Contents

Introduction / Overview 4
Statement 5
Scope 5
Aim 5
Objectives 5
Roles and Responsibilities 5
Security Arrangements 9
Access Control / Swipe Card Security Systems & Key Control 10
Department / Local IT Department 10
Control of Keys 10
Control of Security Codes 10
Site Security Management Plans 11
Lockdown Procedures 11
Risk Assessments 11
Lone Working 12
Personal Security 12
Security of Information 13
CCTV 13
Fraud 14
Theft 14
Patient Valuables / Cash 15
Training Requirements 15
Metrics 15
Monitoring and Audit Arrangements 16
References 16
Appendix 1 - Lone Workers Advice 17
Appendix 2 - Security Incident Response Plans 18
Appendix 3 - Malicious Threat - Telephone Call Crib-Sheet 19
Appendix 4 - General Security Advice – All Staff 21

Introduction / Overview

In the context of this policy, 'Security' describes the protection and safety of all those visiting or working on Health Board premises, including those providing, receiving, or accompanying those who are receiving health services. The Health Board recognises that in today's society, healthcare premises and their contents, are as vulnerable as any other premises in respect of theft and damage, either of which, could result in personal injury and/or loss or damage of equipment, confidential records, etc.

A Security Incident may be defined as an unwanted, unplanned and unexpected event which may or may not result in physical injury, loss or damage e.g. theft, burglary, vandalism, and fraud.

The Health Board will endeavour to ensure that staff are provided with the appropriate skills to be able to effectively deal with site and/or personal security issues as required.

The Terrorism (Protection of Premises) Act 2025 (Martyn's Law), which received Royal Assent on 3 April 2025, has introduced statutory duties on operators of publicly accessible premises, including NHS healthcare sites, to strengthen their protection against terrorism. Implementation is subject to a minimum 24-month transition period, meaning duties are expected to apply from 2027 onwards. Under the legal obligations of the Act, the organisation needs to promote effective and coordinated responses to security arrangements on a routine and emergency response level.

The Health Board will ensure that contingency plans, including lockdown procedures, are established and implemented in the event of a major security incident. For further details on contingency plans, including the Health Board's Major Incident Plan, please refer to the Health Emergency Planning intranet page (opens in a new tab). Worthy of note is the increasing consideration that health should be considered under the Critical National Infrastructure (CNI) due to its obligations as a Category 1 responder within the Civil Contingencies Act 2004. As such security equipment and security standards should achieve this level of assurance.

This Policy is based upon government advisory circulations that will aid a risk assessment approach to form agreed security standards or processes. The Policy and associated operating procedures will provide the necessary assurance at Strategic, Tactical and Operational levels.

Security improvements will be considered and implemented as far is reasonably practicable, taking into account risk scores, potential impacts and loss as well as financial burdens.

Key to the success of the Policy will be the risk appetite from the Executive Team and Senior Management, underpinned with good practice by all staff engaged with health board duties with specialist support offered from the Security Manager (SM), Information Governance, Estates and Facilities and Digital/Information Technology Department.

Statement

Each Health Board site will have site security plans and Standard Operating Procedures (SOP's) that are informed by risk assessments and specific advice provided by the police or SM. All plans offer protection under business as normal, out of hours and emergency response. The assessment of security risks is applied to all main or critical healthcare locations within the health board area.

Scope

This policy applies to all staff of Hywel Dda University Health Board (HDdUHB). Whilst the policy outlines how HDdUHB will manage its security issues, implementation does not replace personal accountability of all staff in this regard.

Aim

This policy aims to provide a framework which can be used at all levels across the Health Board to assess and continually strive to improve the level of security at all HDdUHB sites.

Objectives

The Health Board will strive to achieve the following objectives:

- To provide protection to staff, patients and all others legitimately on HDdUHB premises;
- To provide protection of assets and information;
- To establish a security-conscious environment;
- To identify problem areas and effect remedial action;
- To determine the size and cost of any existing security problem; and
- To protect the reputation of the Health Board.

Roles and Responsibilities

Director Responsible for Security Management

As the Board member responsible for security, the Executive Director of Allied Health Professions and Health Science has specific responsibilities to ensure that security arrangements are adequate and to ensure the Health Board has suitable and sufficient measures and resources in place to ensure the security of its staff, patients, property and assets.

- Formulation, implementation and maintenance of an effective Security Management Policy;
- To review and amend this policy to ensure compliance with any current legislation;
- Ensuring that all provisions of the CCTV sections of the Data Protection Act are complied with and all systems are registered with the relevant Data Protection Authorities;
- Monitoring the performance of the Health Board and Directorates with regard to the implementation of this policy;
- To provide strategic direction for development of a secure environment.

Directors, Associate Directors and Senior Managers

Active involvement of senior managers is crucial for maintaining and improving security across the Health Board. The role of the Health Board includes the following:

- All Directors and senior managers will be responsible for their own work area's security plan, in terms of providing a safe and secure environment within the parameters of the policy;
- All Directors and senior managers will ensure that effective measures are implemented to establish a safe and secure environment;
- All Directors and senior managers will ensure that all significant security risks are identified and effectively controlled;
- All managers will ensure that staff are issued with and wear identity badges and comply with signing-in procedures where appropriate. They will also ensure that staff who are visiting patients in their homes carry/wear photo identity badges;
- All managers will ensure that staff involved in incidents complete an incident report via the Health Board on-line reporting system (Datix) after every incident or 'near miss' and that the Health Board 894 'Putting Things Right' Management and Resolution of Concerns Policy (Incidents, Complaints and Claims) (opens in a new tab) and 982 - Incident, Near Miss and Hazard Reporting Procedure (opens in new tab) are consulted for guidance when necessary.

Head of Health, Safety and Security

The Head of Health, Safety and Security will:

- Act as the professional lead for security, defining policy, standards, and direction;
- Lead the Health Board's approach to premises security management and oversee risk-based security planning;
- Ensure security risks are accurately captured within the corporate risk register;
- Develop systems to enable the Health Board to progress security management workstreams;
- Provide assurance to the Board / Director Responsible for Security Management that security risks are being effectively managed.

Health Board Security Manager

The Health Board Security Manager (SM) will undertake the role of co-ordinating Health Board-wide premises security issues. The SM will:

- Be responsible for ensuring that all security incidents have been suitably investigated and that any appropriate action is taken;
- Provide crime prevention advice, support and assistance in upholding and developing all operational arrangements that affect security;
- Act as Single Point of Contact (SPOC) for all criminal related incidents between the Health Board and the Police;
- Attend regular meetings with the Police and Health Board Teams;
- Develop, implement, and continuously review the Health Board's security strategy, policies, and standards;
- Support corporate risk management related to security and crime prevention;

- Act as the focal point for contact with external agencies with security matters affecting the Health Board;
- Provide support to staff involved in a security incident;
- Assist managers in investigations of breaches or suspected breaches of security and to liaise with the Police where criminal proceedings are being considered;
- Ensure security risk assessments and crime reduction surveys are conducted in Health Board Properties with the Health Board Assistant Security / Violence and Aggression Officers;
- Assist Managers in identifying any security associated risks following a breach or suspected breach in security;
- Advise the Director responsible for Security of any impacts resulting from new legislation or national directions and guidance;
- Ensure appropriate security advice is provided to capital schemes and Health Board projects;
- Provie reports on Security as required.

Health Board Assistant Security / Violence and Aggression Officers

The Health Board Assistant Security / Violence and Aggression Officers (ASVAO) will undertake the role of assisting co-ordinating Health Board premises security issues, including:

- Act as the focal point for contact with external agencies with security matters affecting the Health Board;
- Provide support to staff involved in a security incident;
- Assist managers in investigations of breaches or suspected breaches of security and to liaise with the Police where criminal proceedings are being considered;
- Ensure security risk assessments are conducted in Health Board Properties;
- Assist Managers in identifying any security associated risks following a breach or suspected breach in security;
- Oversee the management of access control, ID cards and CCTV systems;
- Promote a culture where staff feel safe to report Security Issues;
- Ensure site security system faults are addressed promptly with estates/IT teams;
- Assist contracted security staff, ensuring a professional standard and deployment planning;
- Support major events VIP visits protests and public gatherings.

Head of Estates

Duties of the Head of Estates include;

- Ensuring appropriate physical security of Trust premises including making arrangements for premises to be made secure as soon as practicable in the event of damage presenting a security risk;
- Ensuring the maintenance of security related systems such as alarm systems, access control and CCTV installations is carried out where the budget for these systems is held by Estates;
- Assisting the Security Manager, Security & Violence and Aggression Advisors and the Estates & Facilities Team in identifying deficiencies in security systems;
- Liaise with the Security Manager to ensure that new builds and alteration work within the Health Board includes funding for appropriate security measures;

- In consideration of unplanned events Estates staff should be competent in incident response.

Portering Services

The Porters role includes elements of security management in terms of;

- Undertaking patrols as a visual deterrent and at night ensuring windows and doors are secure wherever possible;
- Responding to incidents of a violent and aggressive nature and providing assistance to Health Board staff;
- Locking and unlocking health board premises if required.

Site Safety Officers

Site Safety Officers are currently employed at Withybush General Hospital and Glangwili General Hospital and will be introduced to the other acute hospital sites over time on a time-limited basis to satisfy a Fire Brigade mandate. Their roles are a hybrid of fire warden, site security and portering duties. The elements of the role in terms of security management include:

- Undertaking general security checks whilst carrying out normal duties and to challenge suspicious individuals and those inappropriately smoking on site, as necessary;
- Checking all external doors and window are locked out of hours;
- Patrolling the hospital perimeter and check and patrol hospital residences out of hours;
- Escorting staff to their vehicles during night shift as requested;
- Being present in Accident and Emergency during evening/night shifts;
- Resetting intruder alarms in outlying buildings as necessary;
- Providing controlled restraint of aggressive/violent persons at the request of medical and or nursing staff;
- Searching patients' clothing to establish ID at the request of nursing staff;
- Viewing security camera footage to gain evidence in the event of a security incident taking place;
- Acting on behalf of the Health Board to escort individuals who may be abusive, drunk or violent, from the premises and to assist in personal safety of staff.

All Staff

All staff, irrespective of status, are responsible for:

- Their personal security whilst at work within the Health Board;
- Wearing the Health Board ID badge when in the workplace, except when it may pose an ongoing operational risk to health and safety (e.g. operating theatres);
- Producing the Health Board ID card issued to them on the request of an identified Health Board Manager or any member of the Health Board;
- Not posting copies or photographs of ID cards on social media;
- Maintaining a secure environment for their fellow employees, patients and visitors and ensure, where possible, the protection of their property;

- Maintaining a secure environment for property and all assets belonging to the Health Board;
- Ensuring they are aware of this Security Policy and that they follow its requirements within their workplace;
- Politely challenging anyone in their area that they do not recognise, providing it is safe to do so. If a member of staff sees anyone acting suspiciously, behaving unusually, smoking or is an area that they should not be, they should politely challenge and then must inform their line manager as soon as possible;
- Ensuring that their office doors and windows are shut and locked when they leave work or when they leave their place of work for a period of time;
- Ensuring that when they leave their place of work, expensive equipment and confidential papers, particularly patient records, are locked away and out of sight.

Security Arrangements

Sites should optimise their security arrangements by adopting a layered approach to the three main aspects of security:

1. **PHYSICAL SECURITY** – e.g. Doors, traffic routes, barriers, external walls and windows, bins and waste disposal;
2. **SYSTEM SECURITY** – Information Security, IT, CCTV, Access control, Intruder detection systems, fire systems, public announcement, radios and telephone systems;
3. **HUMAN FACTOR** – Knowledge and diligence to ensure that measures as above are not compromised and a pro-security and safety culture is embedded and promoted at all times.

All Hywel Dda University Health Board sites should make sure that they develop an active security culture, which should include:

- **Site inductions** – making sure that all personnel involved in the site are made aware of the security arrangements, responsibilities, response models and smokefree sites requirements;
- **Briefings** – involving all site staff and volunteers in regular briefings about the operation of the site and the associated security arrangements;
- **Awareness** – making time available for site staff and volunteers to undertake relevant security training;
- **Reporting** – creating a culture where site staff and volunteers can easily report any security concerns which they might have and making sure that learning and feedback is shared from these.

General site security is an issue for all staff and a high level of awareness is essential and the following advice should be followed at all times:

- Wearing staff identification is an important part of promoting a secure environment. All staff, contractors, volunteers must ensure that they display their ID cards whilst on Health Board property or business;
- All staff should ensure that their work areas are secured at the end of the working day (where applicable) and that departmental keys and fobs are always held in a secure place;
- The loss of any keys or fobs must be reported to the appropriate ward/line manager;

- Access to certain restricted areas is controlled via security locks and alarms. Access to these areas will be monitored and controlled by the designated manager responsible for that building;
- Security codes should be changed whenever it is felt that the code may have been compromised;
- All personal security, theft, property damage, patient property, fraud incidents and smokefree sites non-compliances should be reported via the Health Board on-line incident reporting system (Datix) and the Security Manager or ASVAOs should be informed.

Access Control / Swipe Card Security Systems & Key Control

Access control systems are in operation at various locations within the Health Board. The purpose of these systems is to ensure that only authorised persons are allowed access into certain areas/buildings or that access is restricted at certain times. The management of access control systems is via the ASVAOs.

Department / Local IT Department

All staff who work/access areas which have access control therefore have a responsibility to:

- Ensure that any faults are reported to the Security Department/Local IT department;
- Be vigilant of tailgaters;
- Never loan their Access Control Swipe card to anyone else;
- Report loss of Access Control Swipe cards to the Security Department/Local IT department immediately so that the card can be deactivated.

Control of Keys

- Key control measures should be in place for all keys held locally in a department/building;
- All departmental keys should be kept in a locked key cabinet;
- There should be a register of all keys held;
- Members of staff/contractors who need to borrow a key must produce ID and sign a key control register when the key is issued/returned;
- Report lost or stolen keys to the Security Department.

Control of Security Codes

- Security code control measures should be in place for all security codes i.e. door codes;
- Only authorised personnel should be provided with security codes;
- Security codes should be changed on a regular basis i.e. every six months and/or following a security concern;
- If a security code needs to be changed, please contact your local Estates Department;
- Facilities should be informed when security codes are changed to ensure emergency access is maintained when required;
- Avoid sharing security codes via unsecured communication channels or in person to anyone not requiring access.

Site Security Management Plans

Locality-specific Site Security Management Plans will be developed by hospital management teams at each acute hospital site to reflect their local security management arrangements. These plans will help improve local levels of security and contribute towards compliance with the Terrorism (Protection of Premises) Act 2025 alongside local terrorism risk assessments. Lockdown procedures (see next section) will form part of the overarching Site Security Management Plans.

Guidance has been provided to hospital management teams on the required content of their local Site Security Management Plans and their development will be overseen be locality-specific Security Management Groups.

Lockdown Procedures

In the event of a security incident or the declaration of a Major Incident, it may be necessary to initiate a 'lockdown' of a part or the whole of a Health Board premises.

What could initiate a Lockdown?

- Terrorist attack including Marauding Terrorist Attack (MTA);
- Child/baby abduction;
- Clinical or human disease outbreak (flu pandemic) etc;
- Flood or another environmental incident;
- Violent attacks/fights in the Emergency Department;
- Chemical, biological, radiological attack;
- Bomb threats;
- Missing or wandering patients.

The list is not exhaustive or prescriptive.

Types of Lockdowns;

- Partial lockdown;
- Portable lockdown;
- Progressive lockdown;
- Full lockdown.

The development of lockdown procedures requires careful planning and assessment of risks, particularly those associated with restricting access and/or egress and how this has the potential to impact on patient care.

Lockdown procedures are likely to be part of an implementation of the Major Incident and Business Continuity Plan. Site Lockdown plans will be written to reflect individual site arrangements and resources and in line with the Health Board 749 Lockdown Policy – opens in new tab.

Risk Assessments

Risk assessments regarding the physical security and assets are undertaken by staff at individual sites in conjunction with the Security Manger and ASVAOs, on request. These risk assessments are

prioritised by reviewing risk profiles and carried out as a rolling programme. Actions arising out of the risk assessments will be monitored by the relevant Clinical Care Group (CCG) or Function.

Lone Working

Lone working poses risks to staff which must be risk assessed by managers in accordance with the 170 Lone Working policy- opens in a new tab. Many NHS staff work on their own, either regularly or occasionally, without access to immediate support from work colleagues, managers or others. These lone workers need to be given organisational support, management and training to deal with the increased risks they face. They must also be empowered to take a greater degree of responsibility for their own safety and security. If lone workers are concerned about their immediate safety they should phone 999 first and then inform their line manager. Lone workers should not be afraid to use 999 if required.

It is the responsibility of line managers of staff who work alone to ensure that appropriate policies and procedures are developed, implemented, monitored and adhered to. The Health Board has implemented the use of the PeopleSafe Lone Working Devices and these can be issued to staff if Violence and Aggression or Lone Working risk assessment identifies a need. Lone workers have a responsibility to follow these policies and procedures for their own safety. A quick guide for lone workers can be found as Appendix 1.

Personal Security

While it is the responsibility of the Health Board to provide a safe and secure environment, it is the responsibility of all staff to take reasonable measures to ensure their own health and safety including personal security. To help achieve this all staff should note the following advice:

- Try to be familiar with your surroundings and be aware of other people;
- Where possible avoid isolated and poorly lit areas;
- Report suspicious activity/behaviour to your line manager in the first instance.
    - For an emergency response from police do not be afraid to use 999;
    - If lone workers are concerned about their immediate safety they should phone 999 first and then inform their line manager.
- If you feel able, having considered support from your line manager or colleagues, question unknown or suspicious activity in a friendly and positive manner. If the individual(s) become argumentative or aggressive, staff are to back-away from the situation;
- Plan your journeys and route, considering vehicle maintenance and fuel, maps and allowing sufficient travel time. Only take items with you that are required as you should not leave valuables in your vehicle or struggle to carry too many items, you will be distracted;
- Park your vehicle in a well-lit area with high volumes of human traffic; also look for areas covered by CCTV or security patrols;
- Walk with confidence even if you are not familiar with your surroundings, look straight ahead with your head held high but do not make eye contact unless necessary and do not draw attention to yourself;
- Ensure your mobile phone is charged up and easily accessible to make an emergency phone call;

- Walk in pairs or more when possible;
- Inform somebody of your whereabouts or destination when travelling and your planned arrival time, along with any means of contacting you;
- Leave valuables at home.

Security of Information

Information and documents are fundamental to healthcare and to Health Board business and are increasingly handled electronically. Information must be kept and shared in a safe manner.

Any incidents relating to a breach in security of patient identifiable information must be reported via the Health Board's on-line incident reporting system (Datix) and referred to the Information Governance Department.

The Health Board will ensure that all staff comply with the Data Protection Act (2018) regarding the confidentiality of personal information and access to medical records. All medical records under the Health Board's care, both on and off Health Board premises, will be securely stored. Access will be restricted to authorised personnel only. For further guidelines, refer to Health Board's 836 – Information Governance Policy (Data Protection Policy) – opens in a new tab.

The Health Board will ensure that all staff comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) regarding the confidentiality of personal information and access to medical records. All medical records under the Health Board's care, both on and off Health Board premises, will be securely stored. Access will be restricted to authorised personnel only. For further guidelines, refer to Health Board's 836 – Information Governance Policy (Data Protection Policy) – opens in a new tab.

In addition, the Caldicott Guardian Principles should underpin information governance across the health and social care services and these are:

- Justify the purpose(s) for using confidential information;
- Use confidential information only when it is necessary;
- Use the minimum necessary confidential information;
- Access to confidential information should be on a strict need-to-know basis;
- Everyone with access to confidential information should be aware of their responsibilities;
- Comply with the law;
- The duty to share information can be as important as the duty to protect patient confidentiality;
- Inform patients and service users about how their confidential information is used.

CCTV

Across the Health Board there is a network of CCTV coverage which has a range of functions. Refer to the Health Board's 323 - CCTV Policy (opens in a new tab) which outlines the responsibilities the Health Board has to its employees, patients, visitors and external agencies.

With regards any requests made from any images to be downloaded, refer to the specific Standard Operating Procedure for the specific site.

Fraud

One of the basic principles of public sector organisations is the proper use of public funds. It is therefore important that all those who work in the public sector are aware of the risks and means of enforcing the rules against fraud and corruption. The Health Board is committed to maintaining an honest and open atmosphere within the Health Board. All NHS organisations are required to ensure that members of staff have an opportunity to raise concerns whenever they are justified.

Suspected cases of fraud or corruption will be rigorously investigated. Any reasonably based suspicions of fraud should be reported in confidence to the Health Board Local Counter Fraud Officer. For more detailed advice, refer to the 815 Counter Fraud, Bribery and Corruption Policy – opens in a new tab. If there is any suspicion of fraud, then the Security Manager will decide, in conjunction with the Local Counter Fraud Officer, what action will be taken and whether to inform the Police.

Theft

It is well known that individuals will seek to steal items from hospitals, clinics and other Health Board premises. The items could be standard IT equipment, needles or other physical items and routine security measures are needed to secure premises against theft. It is possible that individuals may seek to steal vials of medication and staff should be aware of the need to take special care of such items. Many Health Board assets have value within criminal activities.

Any item that has the potential to cause harm to others, undermine health programmes, contains personal and sensitive data or is classed as an asset must be protected from loss or misuse, including waste using the layered security approach model. All critical assets should be afforded higher levels of security to protect against service failures or disruption.

Patient and personal items should always be kept securely so as to reduce the levels of criminal appeal and displace behaviours away from sites that cause distress together with lengthy investigative process and potential adverse publicity and reputational harm to the organisation.

In the event of theft, the Security Manager or ASVAOs should be informed of all incidents via the Health Board on-line incident reporting system (Datix). The Security Manager or ASVAOs may decide to involve the Police if, in light of the circumstances, it is appropriate to do so. The Health Board will actively support prosecution where theft is related to property belonging to other persons e.g. patients, visitors and contractors, where the police will normally be advised.

Damage to Health Board Property

In the event of damage to Health Board property, the line manager responsible for that particular building, ward or department will be responsible for informing Estates and Facilities, the Security Manager or ASVAOs and the Police if, in light of the circumstances, it is appropriate to do so. The Health Board will actively support prosecution of individuals that cause damage to Health Board property.

Patient Valuables / Cash

The Health Board will not accept responsibility or liability for patients' property brought into in-patient and residential units unless it is handed in for safe custody and a copy of an official patient's property receipt is obtained. All property accepted for safe custody must be placed in the ward security container/safe or forwarded directly to the Cashier's Office.

Patients who decline the Health Board's offer to deposit their property for safe keeping should sign a disclaimer stating that any property/monies brought into the hospital and not deposited for safe keeping are held at their own risk.

In the event of accidental damage by a member of staff to patient's property, a Health Board on-line incident report (Datix) must be completed giving full details of the damage caused and any action taken.

Training Requirements

Security Management training is included within the Manager's Health & Safety Induction course.

Porters currently receive training from the Health Board's Reducing Restrictive Practice Team. This involves a three-day course with annual refresher courses.

Metrics

Security arrangements will be monitored via data metrics received monthly by the Health and Safety Compliance Group. The relevant metrics include:

- Number of violence and aggression (V&A) incidents;
- Number of security incidents;
- Number of Reducing Restrictive Practice (RRP) incidents;
- % RRP training compliance;
- % V&A Module A e-learning training compliance;
- % of V&A/Security risk assessments in place for reported incidents;
- % of high-risk areas with active CCTV;
- % of sites with Security Plans in place;
- Number of absconding patients;
- Number of police call-outs;
- Number of security risks / calls to ward;
- Number of Corporate and Operations risk register risks and their current scores;
- Policies and Procedures within date.

Monitoring and Audit Arrangements
Managers will be responsible for monitoring their own security risk assessments and associated protocols and procedures.

This policy will be monitored and reviewed on a three-year basis or as deemed necessary by the Health and Safety Committee or Health and Safety Compliance Group.

References

- Terrorism (Protection of Premises) Act 2025;
- Mental Health Act (2007);
- Mental Capacity Act (2005);
- The Health and Safety at Work Act (1974);
- Management of Health and Safety at Work Regulations 1999;
- Manual Handling Operations 1992;
- Control of Substances Hazardous to Health Regulations 2002;
- Display Screen Equipment Regulations 1992;
- Provision and Use of Work Equipment 1998;
- Personal Protective Equipment Regulations 1992;
- Criminal Justice and Immigration Act (2008);
- Data Protection Act (2018);
- UK General Data Protection Regulation;
- Major Incident Plan.

Appendix 1 - Lone Workers Advice

Familiarise yourself with the Health Board's 170 Lone Working policy – opens in a new tab.

All staff have a legal duty to take reasonable care of their own safety.

Make sure you have received up-to-date training in the prevention and Management of violence (e.g. conflict resolution and lone worker personal safety).

Know the risks of aggressive and violent behaviour by patients/service users and the appropriate measures for controlling these risks.

Ensure you can access the appropriate safety equipment (e.g. lone worker alarm devices where deemed necessary by risk assessment) and know how to use and maintain it.

Remember the importance of thorough planning – be aware of the risks and do everything you can in advance to ensure your safety.

Always leave an itinerary with your manager or your colleagues and keep in regular contact with your base.

Risk assessments should be completed for all lone working situations and know the circumstances under which visits can be terminated. Never put yourself or colleagues in danger. If you feel threatened, withdraw immediately.

For further support, advice and guidance contact the Health, Safety and Security Department.

Appendix 2 - Security Incident Response Plans

The actions and responses shown are a guide to cover all types of incident.

Minor incidents will only require a limited response compared to those for more serious events.

Initial Response

- Identify the type of incident;
- Raise the alarm;
- Detain suspect if personal safety is not put at risk;
- Alert Security Department, telephone operators, Police and Health Board personnel as appropriate;
- Initiate procedure to secure area, building or clinical area;
- Isolate and protect the scene of crime (if necessary move patients);
- Obtain and circulate suspect's description within the location;
- Seek information from staff, patients and visitors.

Consolidation

- Keep a timed record of all actions;
- Record details of all witnesses and others in the unit/location at the time of occurrence;
- Protect and support victims;
- Check all personnel are aware of their roles;
- Arrange effective communications with incident management team;
- Police, emergency services etc.

Recovery

- Continue support and counselling of staff;
- Fully de-brief all involved;
- Prepare report of the incident and its outcome.

Return to Normality

- Reassure all patients, visitors and staff. Ensure that premises/individual working practices are returned to normal as soon as possible;
- Provide feedback to staff on outcome of incident;
- Review security incident response plans and make amendments where necessary;
- Review security equipment and crime prevention procedures.

Appendix 3 - Malicious Threat - Telephone Call Crib-Sheet

DO NOT PUT DOWN THE RECEIVER OR CUT OFF THE CALLER.

OBTAIN AS MUCH INFORMATION AS YOU CAN AS YOU GO ALONG (if the call is not being recorded).

Ask questions as detailed below.

THREAT MESSAGE (Exact Words).

……

……

……

……

……

……

……

……

Where is the threat?	
If an incendiary device, what time is it set to go off?	
What does it look like?	
What kind of device is it?	
What will cause it to go off?	
Did you place the device yourself?	
Why are you doing this?	
Who do you represent?	
Is there some way we can contact you?	

Other information to gather if possible:

Telephone extension number where call was received	
Date and time of call	
Duration of call	
Details of caller – Male/Female	
Approximate age	
Language – e.g. Well-spoken, Foul, Irrational, Taped, Reading a message etc.	
Callers Voice – e.g. Calm, Angry, Slow, Loud, Laughing, Slurred, Disguised, Accent, Stutter, Lisp, Familiar	
If familiar, who did it sound like?	
Background Noises – e.g. Interruptions, Street noises, Voices, Music, Machinery, Children, Animal, Motors etc.	
Any other Remarks	
Name of Person Receiving Call	
Extension no:	Ward/ dept:

Appendix 4 - General Security Advice – All Staff

Workplace:

- Ensure security training is refreshed – security and cyber threats change regularly, make sure you are aware of these;
- Do not add stickers or write keypad lock number onto the rear of ID cards;
- Lock rooms when not in use and/or keep a clear desk process. Medical records and sensitive documents should be secured and kept out of sight;
- Sensitive or personal information including passwords must not be written on office whiteboards. Consider a pulldown screen to conceal less sensitive information;
- Supervisors and managers should regularly check their workplace areas to review security measures – 'walk the floor'.

Visitors:

Verify the identity of all visitors and consider:

- A physical check of ID card – is it just paper or card? NHS lanyards and card holders can be purchased via Amazon and other public suppliers;
- Does the photograph match and is it current? Has the ID card expired?;
- If in doubt request secondary identification – driving licence or credit card etc;
- Stethoscopes and high-visibility (yellow) jackets on their own are not accepted forms of identification. A current ID card is also required;
- Contact the visitor's department or company to verify identity. Legitimate visitors will understand any short delay while you confirm;
- Consider escorting any visitor to their destination or arrange for them to be met at reception;
- Be prepared to politely challenge and call security if you are suspicious.

Security of IT Equipment:

Any equipment, particularly computers and laptops must be kept secure:

- Do not allow ANY equipment to be removed unless you can verify the reason and the identity of the person taking;
- Be prepared to politely challenge and call security if you are suspicious;
- Never disclose any passwords or other sensitive/personal information;
- Lock rooms when not in use and/or keep a clear desk process. Laptops and sensitive documents should be secured and kept out of sight;
- Desktop and laptop computers should be logged off when not in use;
- Ensure you refresh your security training – security and cyber threats change regularly, make sure you are aware of these.

Appendix 5 - Request for Issue of Identification (ID) Badge

REQUEST FOR ISSUE OF IDENTIFICATION (ID) BADGE

INTRODUCTION

In accordance with the Security Management Policy (1138) all Hywel Dda University Health Board employees (as well as individuals volunteering and/or on work experience) should wear identification (ID) badges whilst on health board premises/business.

Whilst this is primarily a security requirement, it is also in keeping with the spirit of the Patients' Charter which states that name badges should be worn by all staff who are in direct contact with patients.

POLICY

Health Board employees, volunteers and those on work experience will be issued with an ID badge by the Health Boards Workforce & OD department which will bear the holder's photograph. On employment, or when requesting a new ID badge applicants will be asked to provide a colour passport type photograph.

Line Managers will be responsible for ensuring that employees, work experience and volunteers are issued with ID Badges on commencement of employment as applicable.

ID badges are the property of the Health Board. It is the responsibility of Line Managers to retrieve them on cessation of employment and to destroy immediately.

Stolen or lost identification badges are to be reported immediately by Line Managers to the Health Board's Security Officer. It will be the Manager's responsibility to arrange the issue of a replacement badge.

On receipt of an identification badge, the holder:

- must not give the ID badge to any unauthorised person;
- must report loss immediately to their Line Manager;
- must exchange the ID badge for a new one on being employed in a different skill or profession within the Health Board;
- must surrender the ID badge, card holder and lanyard to their Line Manager on ceasing employment/volunteering/work experience.

PART A

To be completed by Appointing/Line Manager:

Will you please arrange the issue of an ID badge to the following employee/volunteer/work experience:(Please complete the following in CAPITAL letters)

Please Note: The ID badge will be sent to the Managers address.

FULL NAME	
PREFERRED NAME ON BADGE	
PREFERRED PRONOUNS eg: he/him, they/them, she/her (Optional) (English)	
PREFERRED PRONOUNS eg: ef/ei, nhw/eu, hi/ei (Optional) Welsh	
STAFF / PAYROLL NUMBER or NI NUMBER	
JOB TITLE (English)	
JOB TITLE (Welsh)	
DEPARTMENT (English)	
DEPARTMENT (Welsh)	
CONTACT NUMBER / EMAIL	
DATE OF COMMENCEMENT or REASON FOR ISSUE OF BADGE	
MANAGERS NAME	
MANAGERS DESIGNATION	
MANAGERS WORK EMAIL & FULL POSTAL ADDRESS **(Capitals Please)**	
MANAGERS SIGNATURE	
DATE	

Please submit this completed form WITH A PHOTO (head and shoulders) to
ID.Badges.HDD@wales.nhs.uk
or post it with a passport sized photo to:
Hywel Dda University Local Health Board
Recruitment Team
Block C
Government Buildings
Picton Terrace
Carmarthen
SA31 3BT

PART B

To be completed by employee in presence of Line Manager on receipt of identification badge.

I acknowledge receipt of an ID badge and understand that:

1. I must not give the ID badge to an unauthorised person and will report losses without delay to my Line Manager.

2. In the case of loss of my ID badge, I will provide additional photographs as required.

3. I must exchange the ID badge for a new one on being employed in a different skill or profession within the Health Board.

4. I must surrender the ID badge, card holder and lanyard to my Line Manager on ceasing employment/volunteering/work experience.

5. Line Manager will destroy the ID Badge on receipt.

FULL NAME	
JOB TITLE	
STAFF / PAYROLL NUMBER / NI NUMBER	
DATE	

THIS FORM IS TO BE RETAINED ON EMPLOYEES PERSONAL FILE