SECURITY POLICY

This document can only be considered current when viewed via the Trust intranet/internet. If this document is printed or saved to another location, you are advised to check that the version you use remains current and valid, with reference to the review due date

Document Author	*Ric Allhusen, Security Manager*			
Lead Owner	*Security Management Director*			
This Version	5.0		**Status**	*Approved*
Replaces	Security Policy Ver 4			
Approval	Date	13 October 2021	Where	Security Committee
Ratification	Date	13 October 2021	Where	Security Committee
Date of issue	07/10/2021		**Review date**	October 2024
Applies to	All colleagues of the Trust and partner agencies.		**Exclusions**	

CONTENTS

1.0 KEY POINTS

- The Trust is committed to promoting and improving a safe and secure environment for those who work in or use its services so that the highest standards of care are always available to patients.
- Security is the responsibility of all colleagues, not only safeguarding their own wellbeing and personal property, but also that of patients, visitors and Trust property.
- The Trust will ensure effective management of security in the workplace environment and strives to ensure it is managed effectively by:
    - Ensuring risks associated with physical security of premises and other assets, and the personal safety of patients, colleagues (including lone workers) and others are identified, assessed and managed;
    - Ensuring colleagues understand and carry out their responsibilities for the security of other colleagues, patients and visitors effectively;
    - Developing a culture which provides colleagues, patients and visitors with a safe and secure environment;
    - Ensuring all colleagues have support if they are involved in a security incident, and are fully de-briefed after the incident;
    - Having a Security Team on site to respond to all requests for security attendance and who take a proactive view to security;
    - Complying with relative legislation, such as the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999.

SECURITY TIPS

- Report all security-related incidents, or suspicions of such incidents;
- When you are at work - wear your ID badge. Always ask to see someone's identification if you are not sure who they are
- If you see someone acting suspiciously, or they are somewhere you think they should not be, tell your manager, or if it is safe to do so - challenge them.
- Make sure you are aware of anyone who might be trying to gain access or leave a secure area by closely following you as you arrive or leave..
- Call 2222 if you need the Security Guards to attend your department. Please call the Guards if you think something is about to happen as opposed to waiting until something has happened. They are there for your safety and security.

2.0 INTRODUCTION

2.1 The Trust is committed to promoting and improving a safe and secure environment for those who work in or use its services so that the highest standards of care are always available to patients. Security is everyone’s responsibility. Security involves all colleagues at all levels and to be effective needs the support of everyone including colleagues, contractors, visitors and patients. Sensible and cost effective security management initiatives can be taken to reduce risks by establishing a pro-security culture, which aims to prevent criminal activity.

2.2 The Trust will ensure effective management of security in the workplace environment and strives to ensure it is managed effectively by:

- Appointing and training a Security Management Director (SMD) and a Security Manager.
- Ensuring risks associated with physical security of premises and other assets, and the personal safety of patients, colleagues (including lone workers) and others are identified, assessed and managed using the Trust’s Risk Management process;
- Ensuring colleagues understand and carry out their responsibilities for the security of other colleagues, patients and visitors effectively, including attending any necessary training to support them in this;
- Developing a culture which provides colleagues, patients and visitors with a safe and secure environment;
- Ensuring all colleagues carry out their duties in a manner which ensures the safe keeping of the organisation’s property and assets;
- Ensuring all colleagues have support if they are involved in a security incident, and are fully de-briefed after the incident;
- Complying with relative legislation, such as the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999.

2.3 The policy ensures appropriate action is taken when Trust security is breached and in the event of a security incident escalating.

2.4 This policy applies to all Trust colleagues, visitors and patients attending or working for the Trust.

3.0 DEFINITIONS

3.1 **CPTED:** Crime Prevention through Environmental Design. Formally known as Crime reduction to anticipate risks and taking action to remove, reduce or transfer them.

3.2 **‘Defence in depth’**: continually surveyed interdependent and interlocking protective security measures arranged in depth.

3.3 **Physical security**. The hardware and electronic mechanisms deployed to protect Trust assets and resources.

3.4 **Protective Security Management:** used to safeguard people, property and resources against crime, loss, misplacement and costs as a consequence of poor or no security.

3.5 **Ulysses**: electronic database used by the Trust to report Incidents and risks.

4.0 ROLES and RESPONSIBILITIES

4.1 The **Chief Executive** has overall accountability for security and shall ensure:

- Responsibilities for security matters are properly assigned;
- An Executive Director is assigned to lead on the effective and suitable management of security within the Trust.

4.2 The **Chief Nurse** will act as the Security Management Director (SMD) and will ensure:

- The appointment of a competent Security Manager who has undergone appropriate training or has the appropriate experience necessary.
- Implementation and the promotion of security management and compliance with directions set out by NHS England/Improvement and the Secretary of State;
- An annual Security Work Plan is produced;
- Subject to any contractual or legal constraints ensure all colleagues cooperate with the Security Manager.

4.3 The **Security Manager** is responsible for the maintenance of security management arranged within the Trust and will:

- Analyse security incidents to identify trends, draw conclusions and make recommendations;
- Support managers to assess risks to ensure local security risks are effectively managed;
- Oversee and see to ensure appropriate sanctions are considered and applied, where appropriate, including civil, criminal, disciplinary and procedural measures against those whose actions lead to harm to colleagues, patients and others or the loss of Trust assets and resources;
- Assess security technology and its application;
- Create proactive security awareness and promoting the deterrence and prevention of breaches of security;
- Draft the annual Security Report for submission to the Board and Security Committee;
- Deliver formal and informal security awareness training, briefings, updates and ‘bespoke’ sessions to ensure all colleagues are aware of the risks;
- Ensure victims of crime are supported;
- Interpret primary and secondary legislation and advising on the standards required to ensure compliance;
- Investigating breaches of security in a fair, objective and professional manner;
- Liaise with external agencies as appropriate, e.g. police, HM Courts Service;
- Promote a range of proactive and reactive security actions;
- Provide expert security advice to protect people, property and assets;

- Ensure suitable and effective risk assessments are in place for all high risk areas or departments, e.g. Maternity, Emergency Department and Minor Injuries Units and any action plans are monitored;
- Ensure effective and legally compliant CCTV systems are in place and monitored;
- Ensure Body Worn Video (BWV) is controlled as per CCTV policy;
- Provide advice and assistance to colleagues on security management;
- Provide the Police with evidential packages to include witness statements and other material in supports of criminal proceedings, in line with local protocols.

4.4 The **Trust Security Committee** is responsible for the implementation, monitoring and review of the Trust's Security Policy and for the provision of advice on how best to secure continuous improvement in security risk management throughout the Trust. The Terms of Reference for the Group are available from the Head of Resilience.

4.5 The **YDH Security Team**, within the acute hospital environment, will:

- Maintain a high security profile and presence by supporting and providing advice and assistance to colleagues, visitors and patients to ensure a safe and secure environment at YDH;
- Escorting colleagues to their vehicles (out of hours) if required and dependent on emergency calls;
- Searching for missing patients;
- Gathering evidence to support police or Trust investigations;
- Supporting clinical colleagues to ensure detained patients and those lacking capacity remain onsite to receive care and treatment;
- Using the hospital CCTV system as set out in the CCTV Policy;
- Investigating and reporting thefts and criminal damage;
- Completing incident reports for every incident that they attend prior to the end of their shift;
- Seek professional security advice from the Security manager;
- Regular patrolling of the hospital site to identify and report any identified security and crime risks;
- When requested, providing a service to escort colleagues from offices/departments/wards to other areas of the hospital or to the site's car park during the hours of darkness whenever possible;
- Maintain and foster a good working relationship with the Police and other agencies;
- Attend training to support their role.
- Wear BWV in accordance to the CCTV policy and local procedures (in order to deter violence and gather evidence where needed).

4.6 **Heads of Departments** will:

- Ensure there are robust systems in place to manage the security of colleagues, patients and assets;
- Ensure security risk assessments are carried out and processes are in place to investigate and improve following incidents;
- Ensure arrangements are in place to inform the Executive Team directly in the event of any serious incident occurring in the area under their control. This should be in line with the incident reporting procedures.

4.7 **Managers and Supervisory Colleagues** are responsible for ensuring:

- Risk assessments are carried out with local procedures in place to manage the risk to the lowest level possible;
- All colleagues receive information and instruction in relation to any risk assessment or control measures put in place to reduce / control security risks;
- All colleagues attend relevant training;
- All colleagues are issued with identification badges (ID badges);
- All breaches of security are reported and investigated immediately in accordance with Trust Incident Reporting procedures;
- All colleagues upon leaving the Trust return their ID badges, Trust issued keys and electronic passes;
- Secure, accurate and up to date records are kept of **ALL** Trust keys held by colleagues under their control;
- Advice is sought, as appropriate, from the Security Manager where there is any doubt as to the standards to be applied in following this policy;
- Where appropriate, official visitors or contractors are issued with temporary personal identification cards;
- All security incidents are recorded using the Trust incident reporting system.

4.8 All **Colleagues** have a responsibility to report security concerns and incidents, including those involving violence and aggression' and must:

- Report any security incidents or concerns immediately to their line manager and complete an incident report as soon as possible;
- Be aware of their responsibilities to protect at all times the assets and property of patients, visitors, colleagues and the Trust;
- Abide by specific/local security procedures at all times;
- Wear an identification badge whilst on duty for the Trust and this also applies to all colleagues who work in the community;
- Bring to the attention of their manager any perceived shortcoming / hazard or risks in security arrangements;
- Make full and proper use of personal lockers where provided and take all reasonable care for their own property whilst on Trust premises;
- Attend security-related training appropriate to their appointment, as required by their manager.

4.9 All **Trust Contractors,** including agency colleagues, will follow this policy and any associated procedures at all times and will report any security risks or incidents to the local Trust manager.

5.0 SECURITY RISK MANAGEMENT

5.1 Since security risk can be expensive in terms of resources, time, finance and inconvenience, it is essential security management is effective, efficient and commensurate with the threat.

5.2 The objectives of security management are to:

- Contribute to the smooth, efficient and uninterrupted delivery of health care by disrupting, disturbing and diverting breaches of security and criminal behaviour which could cause harm to the Trust;
- Ensure the personal safety and welfare of patients, colleagues and visitors while on Trust property and when working in the community by developing appropriate security systems;
- Secure Trust property and premises against crime and by highlighting security weaknesses.

5.3 Risk Management is a key element of security management and is concerned with using the information and experience of Trust colleagues, and external expertise as appropriate, and translating that with their help, into positive action which will reduce security risks.

5.4 The Trust will adopt a pro-active approach to risk assessment which:

- Addresses the various activities of the Trust and identifies critical areas for the organisation;
- Identifies the security risks which exist and their potential effects;
- Assesses those risks for potential frequency and severity;
- Eliminates the risks which can be eliminated;
- Identifies how risks can be mitigated/managed;
- Provides measurement and assists target setting for reduction in risks.

5.5 The Trust recognises security risks include:

- Violence and aggression against individuals;
- Vandalism of property;
- Theft ;
- Fire and arson;
- Criminal damage;
- Misuse of Information;
- Terrorism.

5.6 Identification of significant security risks will happen at organisational, directorate and departmental levels and will be recorded on local risk registers and escalated to directorate or corporate registers in line with the Trust's Risk Management Policy.

5.7 The Trust will maintain a Security work plan;

5.8 If new premises or assets are commissioned within the Trust these will be risk assessed prior to their operational use.

5.9 Any actions arising from these assessments, and approved by the Security Committee, will be implemented according to agreed timescales and monitored through quarterly reports to the Group.

5.10 The identification of security risks is a continuous process supported by incident reporting processes; feedback from teams and patients; audit and inspections and guidance from external agencies including the Care Quality Commission, Health and Safety Executive and the Police.

Site Security Risk Assessments

5.11 Annual Site Security Risks Assessment will be completed by the Security Manager with local managers.

5.12 The Site Security Risk Assessment will identify specific security risks and describe agreed actions to minimise and manage those risks.

5.13 The Site Security Risk Assessment will be shared with Managers and with the Security Committee completion.

5.14 The Site Security Risk Assessments will be reviewed at least annually or at any time if there has been:

- A significant security incident on the site;
- A change to security arrangements;
- A change to the security risk;
- There is any other reason to believe the assessment is no longer valid.

5.15 Department Managers are responsible for identifying, assessing and managing any Department specific risks and will complete the Trust Risk Assessment Template to document the assessment and agreed local arrangements for safety.

6.0 SECURITY PLANNING

Principles

6.1 Security planning is reliant on:

- Analysis of security risk assessments;
- Cost-effective deployment of protective security measures;
- Early consultation in building and refurbishment projects to determine physical security measures;
- Proactive security management.

6.2 An important philosophy in Security Management is Protective Security and Crime Prevention through Environmental Design (CPTED), formally known as *Secure by Design.* Given there is no such concept as pure security and accepting if time, opportunity and persistence are available, any security system (including property, information security, buildings) can be breached, the security planning solution is to develop a series of real and imagined barriers, arranged in depth and mutually supporting so if one fails, other measures either absorb or deflect the impact.

Security of People

6.3 The Security Manager will manage and minimise security risks to colleagues, visitors and patients by:-

- Working to minimise violence and aggression in the workplace by using agreed Trust procedures;
- In all cases the Trust will take a managed approach to any incident of violence or aggression, including instances deemed as hate crime, and will seek to support the criminal prosecution of offenders.
- Ensuring departments are supported when assessing violence and aggression and appropriate actions put in place;
- Ensuring where risks are identified from an individual, a risk assessment is completed and a strategy is agreed for working safely with the individual;
- Ensuring appropriate alerts are shared with colleagues about security risks;
- Working to the Major Incident Response Plans;
- Providing all colleagues with photographic identification;
- Developing a culture in which colleagues feel able to challenge unknown people in their work area (as long as it is safe to do so);
- Working to the Trust's Lone Worker policy;
- Ensuring Departments complete risk assessments for Lone Working and there are locally agreed protocols for safe working;
- Providing adequate physical security (locks, key codes, electronic entry management) to prevent entry to unauthorised visitors;
- Ensuring key codes for work areas/access passes are only shared with those with authority to access areas;
- To ensure lockdown procedures are practiced on a regular basis.

Security of Property

6.4 The Trust will manage and minimise security risks to property owned by colleagues, visitors and patients by:-

- Providing colleagues with somewhere secure to store their personal belongings whilst at work;
- Following the Trust Patient Property policy;
- Limiting access to work areas to ensure that only those with authorisation can access the area or ward.
- Taking all reasonable steps to ensure Trust property remains secure;
- Reviewing property held by departments on a regular basis to ensure all items are security marked where appropriate or to ensure alternative steps are taken;
- Use of Closed-Circuit Television and Body Worn Video as a preventative and protective measure;
- Where possible, securing valuable assets in restricted areas.
- Encouraging colleagues, agency/locum and students to be vigilant and to report unauthorised visitors or suspicious behaviour;

- Requiring colleagues, agency/locum and students to wear their photographic identification at work;
- Ensuring physical security is effective in preventing entry to unauthorised visitors;
- Working to the Trust's Medical Gases procedures;
- Developing a culture in which colleagues, agency/locum and students feel able to challenge 'tailgaters';

Security of Premises

6.5 The Trust will manage and minimise security risks to premises by:-

- Applying the principle of *Last One out, Check* in respect of windows, doors and cabinets at the end of their work or when leaving an area unoccupied;
- Completing Site Security Risk Assessment to identify security risks and agree arrangements to manage and minimise those risks;
- Ensuring that appropriate management of waste on sites;
- Ensuring appropriate management of medical gases on site;
- Using Closed Circuit Television (CCTV) and following the Code of Practice;
- Agreeing appropriate security response arrangements for all Trust sites.

Access Control - Contractors and Visitors

6.6 Trust security planning will adopt the 'hotel security' principles of creating:

- Public access through recognised public access points;
- Interface areas, such as reception;
- Private and clinical areas controlled by physical security measures in which visitors, of any sort, are controlled.

6.7 All contractors and visitors requiring access to colleague-only areas of Trust premises should be issued with identification badges which clearly show them as being authorised to access the area. Any individual on Trust premises in colleague-only areas, who is not identifiable by an appropriate ID badge should be challenged as to why they are in that particular work area, provided that in doing so it does not place the colleague in a position of vulnerability. Any unauthorised access to colleague-only area, or patient treatment areas should be reported to the manager of that area and an incident report completed.

6.8 Trust premises are not public but an area to which the public can have access and are required to conform to Trust policies and procedures. Car parking is allowed in specified areas and access is conditional on the owners or drivers of vehicles observing whatever regulations the Trust make to ensure the orderly flow of traffic and the safety of all concerned. The Trust accepts no responsibility for damage to or theft of vehicles whilst on Trust premises.

6.9 Members of the public are entitled to enter Trust sites in connection with healthcare, be that as patient, carer or visitor, or for business purposes, providing they are fully compliant with the terms and conditions of the Trust Anyone present on Trust sites without due reason should be asked to leave, having in mind personal safety when doing so. If unauthorised visitors refuse to leave colleagues should summon assistance from other colleagues and/or the Security Team as appropriate to the circumstances.

Control of Keys and Electronic Passes

6.10 It is the responsibility of ALL managers to ensure they keep secure, accurate and up to date records of **ALL** Trust keys or swipe cards held by colleagues under their management. Colleagues should be aware of the need to immediately report any loss of keys and that periodic checks will be carried out to ensure they maintain control of all keys issued to them.

Reporting Security Incidents

6.11 The Trust's Incident Reporting System should be used to report any security incidents. In the event of any incident, or if a colleague has reason to believe a security breach or potential breach could or has occurred, they should immediately report it to their Manager and to the Security Team. The Security Manager should also be informed at the earliest opportunity. All assaults, criminal damage and thefts should be reported to the Police and a crime reference number obtained which should be cited on the Trust Incident Report and communicated to the Security Manager.

Bomb Threats

6.12 A bomb threat procedure for the Trust's premises has been prepared (Appendix D). This gives guidance on general precautions, dealing with telephone threats and decisions to search/evacuate the premises.

Colleagues Working in Non-Trust Premises

6.13 Trust colleagues working within sites not owned by the Trust must ensure they know what they need to for their own safety and the safety of others and must comply with the site owners' security policies, procedures and/or guidelines.

7.0 PREVENT

7.1 Should any colleague have concerns relating to an individual's behaviour which indicates they may be being drawn into terrorist-related activity, they will need to take into consideration how reliable or significant the indicators are. All colleagues must raise their concerns through the PREVENT Lead in the Trust's Safeguarding Team and seek advice on how to address them in accordance with NHS PREVENT.

7.2 Colleagues must seek advice through the Trust's Safeguarding Team via the Safeguarding Single Point of Contact number 0300 323 0035. Out of hours advice can be sought via the Trust's On Call Senior Manager.

7.3 Where colleagues believe concerns may need to be escalated, the PREVENT Lead in the Trust's Safeguarding Team will assist in determining whether the matter needs to be referred.

8.0 TRAINING/COMPETENCE REQUIREMENTS

8.1 The Trust recognises the need for effective training of colleagues to deal with security related issues and will, through the Academy, ensure security advice and training, is provided on:

- Preventing and Managing Violence and Aggression (PMVA) training to reduce the likelihood of assault;
- Personal security and safety within the working environment;
- Responding promptly and effectively to all security incidents.

8.2 Specific areas where training is required will be identified through a training needs analysis; however, these should include a minimum of:

- Conflict Resolution training, up to breakaway, for all colleagues who interact with the public;
- How to report incidents;
- Physical intervention and assault avoidance skills (where required by risk assessment);
- Security/crime awareness;
- Lone working safety (community based colleagues who conduct home visits).

8.3 All colleagues must ensure they have undertaken PREVENT training as part of their mandatory Safeguarding training programme. All colleagues are mapped to receive the appropriate level of PREVENT training i.e. Basic Prevent Awareness Training (BPAT), which is included in Level 1 safeguarding adults training or the Workshop for Raising Awareness Training (WRAP) which is included within the Level 2 Safeguarding Adults training.

9.0 MONITORING

Element of policy for monitoring	Section	Monitoring method - Information source (e.g. audit)/ Measure / performance standard	Item Lead	Monitoring frequency / reporting frequency and route	Arrangements for responding to shortcomings and tracking delivery of planned actions
Duties	**4.0**	Carry out a review to ensure that key colleagues named as having responsibilities in this policy are carrying out their duties. This will be a verbal interview with colleagues and assessed by matching knowledge against policy requirements.	Security Manager	Annual; Security Committee	Where deficiencies are identified an action plan is developed by the Operational Lead. Security Committee will be responsible for agreeing the action plan and checking progress on action completion and assuring the Quality Assurance Group of improvements
Risk assessment	**5.0**	Annual monitoring of risk assessments in 10 areas Assessed for suitable & sufficient:	Security Manager	Annual; Security Committee	

		In date (reviewed annually) Hazards identified Risk scored Action plan in place (this will also include risks of violence and aggression, assessed against the same criteria)			
Arrangements for actions	**5.0**	Annual monitoring of risk assessments in 10 areas Actions progressed Evidence that action has been taken	Security Manager	Annual; Security Committee	

10.0 REFERENCES.

10.1 Relevant National Requirements

Mental Health Act Code of Practice (2015) HMSO

Violence Prevention and Reduction Standards 2020-2021.

Secretary of State Directive on Measures to Deal with Violence against NHS Colleagues dated 20 November 2003.

Secretary of State for Health Directions on NHS Security Management Measures dated 24 March 2004, under Sections 716d, 17 and 126(4) of the National Health Service Act 1977.

NHSLA Risk Management Standards 2012-2013 for NHS Trusts providing Acute, Community, or Mental Health and Learning Disability Services and Non-NHS Providers of NHS Care

Care Act 2014 Computer Misuse Act 1990

Health Service Circular 1999 No 226

Home Office Crime Prevention Manual Section 6.

National Association for Health Authorities and Trusts Security Manual

NAHAT NHS Security Manual

NHSE Controls Assurance - Security

Regulation of Investigatory Powers Act 2000

NHS ‘Directions to NHS Bodies on Security Management Measures 2004’

10.2 References

Home Office Crime Prevention Manual, Section 6.

Secretary of State Directive on Measures to Deal with Violence against NHS Colleagues dated 20 November 2003

Secretary of State for Health Directions on NHS Security Management Measures dated 24 March 2004, under Sections 16d, 17 and 126(4) of the National Health Service Act 1977.

Security Management Service: A Professional Approach to Managing Security in the NHS.

SMS Secured By Design – Hospitals; April 2005

Data Protection Act 2018

Information Commissioner's Codes of Practice

Mental Health Act Code of Practice

Regulation of Investigatory Powers Act 2000

Human Rights Act 1998

Data Protection Commissioner Codes of Practice

Private and Voluntary Health Care Regulations 2001

10.3 Trust Policies and Procedures

CCTV Policy

EPRR Strategic Policy and Tactical Plans

Risk Management Policy and procedures

Lockdown Policy and plans

Evacuation Policy and plans

Counter fraud Policy

ID Badge Policy

Violence and Aggression Policy

Employee Relations Policy

Standard Operating Procedure for Acceptable Behaviour

Standard Operating Procedure on Discovering Illicit Substances

Searching of Patients Policy

Missing Patients Policy

Standard Operating Procedure for the Investigation and Reporting of Crime

ANNEX A – EQUALITY IMPACT ASSESSMENT TOOL

SOMERSET EQUALITY IMPACT ASSESSMENT

BEFORE COMPLETING THIS EIA PLEASE ENSURE YOU HAVE READ THE EIA GUIDANCE NOTES – AVAILABLE FROM YOUR EQUALITY OFFICER

ORGANISATION PREPARED FOR	**YEOVIL DISTRICT HOSPITAL**		
VERSION	**5.0**	**DATE COMPLETED**	**07/10/2021**

DESCRIPTION OF WHAT IS BEING IMPACT ASSESSED

SECURITY POLICY

EVIDENCE

What data/information have you used to assess how this policy/service might impact on protected groups? Sources such as the Office of National Statistics, Somerset Intelligence Partnership, Somerset's Joint Strategic Needs Analysis (JSNA), Staff and/ or area profiles,, should be detailed here

Health & Safety at Work Act 1974

Who have you consulted with to assess possible impact on protected groups? If you have not consulted other people, please explain why?

We ratify and approved the policy and actions within the policy through the YDH Fire, Health & Safety and Security Committee which involves Trades Union representatives

ANALYSIS OF IMPACT ON PROTECTED GROUPS

THE PUBLIC SECTOR EQUALITY DUTY REQUIRES US TO ELIMINATE DISCRIMINATION, ADVANCE EQUALITY OF OPPORTUNITY AND FOSTER GOOD RELATIONS WITH PROTECTED GROUPS. CONSIDER HOW THIS POLICY/SERVICE WILL ACHIEVE THESE AIMS. IN THE TABLE BELOW, USING THE EVIDENCE OUTLINED ABOVE AND YOUR OWN UNDERSTANDING, DETAIL WHAT CONSIDERATIONS AND POTENTIAL IMPACTS AGAINST EACH OF THE THREE AIMS OF THE PUBLIC SECTOR EQUALITY DUTY. BASED ON THIS INFORMATION, MAKE AN ASSESSMENT OF THE LIKELY OUTCOME, BEFORE YOU HAVE IMPLEMENTED ANY MITIGATION.

Protected group	**Summary of impact**	**Negative outcome**	**Neutral outcome**	**Positive outcome**
Age	•	☐	☒	☐
Disability	• Restricting access to services and premises for security reasons	☒	☐	☐
Gender reassignment	•	☐	☒	☐
Marriage and civil partnership	•	☐	☒	☐

Pregnancy and maternity	•	☐	☒	☐
Race and ethnicity	•	☐	☒	☐
Religion or belief	•	☐	☒	☐
Sex	•	☐	☒	☐
Sexual orientation	•	☐	☒	☐
Other, e.g. carers, veterans, homeless, low income, rurality/isolation, etc.	•	☐	☒	☐

Negative outcomes action plan
Where you have ascertained that there will potentially be negative outcomes, you are required to mitigate the impact of these. Please detail below the actions that you intend to take.

Action taken/to be taken	Date	Person responsible	How will it be monitored?	Action complete
Develop Violence, Prevention and Reduction standards to include all groups with protective characteristics.	07/05/2021	Ric Allhusen	Constant review and feedback from staff	☐

If negative impacts remain, please provide an explanation below.

There may be times when security risk assessments require specialist care plans to be put in place which restricts access to some services and premises. This may be due to restrictions under the Mental Health Act for persons under section and / or in the case of the Mental Capacity Act where an assessment has been made under the Deprivation of Liberty Safeguards.

Completed by:	**Adrian Pickles (Fire, Health & Safety Manager) / Ric Allhusen (Security Manager)**
Date	**07/10/2021**
Signed off by:	**YDH Fire, Health & Safety and Security Committee**
Date	**07/10/2021**
Equality Lead/Manager sign off date:	**Ric Allhusen**
To be reviewed by: (officer name)	**Security Manager**
Review date:	**07/10/2024**

APPENDIX A: SECURITY OF KEYS, FOBS AND COMBINATION LOCKS GUIDANCE

The loss and poor maintenance of keys, key fobs, swipe cards and combination settings leads to inconvenience, expense and increased risk. It is important managers have effective controls to ensure people, property and resources are safeguarded. Failure to do so may have significant consequences in excess of those originally considered.

Terminology

- **Combination Settings.** A series of coded numbers or letters that releases a lock when inserted sequentially;
- **The 'last key'** - The key to a key press;
- **Key Fob** - Electronic locking device;
- **Key** - The manual device used to lock and unlock a lock;
- **Key Press** - A box containing keys. Ideally should be fitted with a simple combination lock to avoid secreting the 'last key';
- **Primary key** - The key in use;
- **Spare keys -** Secondary and triplicate keys;
- **Swipe Card** - Electronic locking/unlocking device swept through an electronic field.

Aim

The aims of key, key fob, swipe card and combination lock settings controls are to ensure people and Trust property are protected and unauthorised direct access to locking devices is denied.

Key, Key Fob and Swipe Card Controls

Keys, key fobs and swipe cards are accountable items. Their locations must be known at all times. They must be stored securely when not in use.

The locations of spare (duplicate and triplicate) keys, key fobs and swipe cards are to be recorded and held by the manager so if one is misplaced it may be temporarily or permanently replaced.

The circumstances of missing keys, key fobs and swipe cards are to be reported as an untoward event.

Managers will record the issue and return of keys, key fobs and swipe cards in a Key Register.

Holders of keys, key fobs and swipe cards will ensure they know where the items can be found at all times.

The Key Register

Managers must ensure a key register is kept for their department with the following information:

- Property Address;
- Name and signature of issuing person;
- Name and signature of recipient;
- Date issued;
- Date returned;

- Areas, type and number of items issued;
- Areas, type and number of items returned.

Losses

If a key, key fob or swipe card is lost, it must be considered compromised and the loss must be reported in an incident. This may result in a security investigation.

The manager must complete a risk assessment to calculate the level of damage and the necessity for all or some key locks to be replaced.

Losses caused by deliberate and reckless damage may incur a replacement cost to the holder.

Security Keys

Security keys are defined as those which:

- Secure containers with sensitive and vulnerable information and material, such as patient information, drugs and petty cash;
- Secure doors to buildings that contain vulnerable patients, colleagues, information and material.

Security keys should be kept separate to general purpose keys and assigned only to colleagues with authority to have to them.

Key Control

It is important managers develop robust safeguards and procedures to protect keys, key fobs and swipe cards. Regular 'snap' audits should be carried out using the Key Register.

Procedures for key control are:

- On receipt of office furniture and taking over buildings and offices, managers will separate the bunches of keys and assign primary keys to colleagues;
- Spare keys are to be centralised in a key press;
- Keys are not to be stored in desk drawers or secreted elsewhere;
- Changing of key codes must be logged and approved by a senior manager;
- When not in use, keys should be placed on numbered or identified hooks in the key press;
- Keys should be marked or tagged with a name, number or simple identification code to identify the lock;
- Only a minimum number of keys should be in use at any one time;
- Primary, secondary and triplicate keys should be alternated to allow fair wear and tear of the key and its lock;
- Local key holders are identified for buildings, other than inpatient wards;
- Managers should, if possible, require handover of keys and key fobs prior to colleagues departing at the end of a period of work.

Combination Settings

Another form of control of access is combination locks. These are safer than keys because the ‘last key’ is the combination and this is stored as a setting, nevertheless controls are required to ensure the integrity of the lock:

- Managers will issue combination settings only to those who need to know;
- Managers must ensure a record of settings is held in separate envelopes under secure arrangements;
- Settings should be changed:
    - When the combination arrives from the supplier; it will normally arrive with a standard factory number;
    - When the combination is returned from repair;
    - When a setting has been compromised;
    - When a colleague no longer requires access;
    - Annually.
- When a lock leaves a department, the setting should be returned to the manufacturer’s setting;
- Combination lock settings should be changed on a regular basis;

Any difficulties with issues around keys, fobs and combination lock settings should be referred to the Head of Estates.

APPENDIX B: GUIDANCE FOR DEALING WITH AGGRESSIVE, ABUSIVE AND OFFENSIVE TELEPHONE CALLS

Introduction

Most telephone calls are made and received by the Trust are made in a courteous and reasonable manner, however there are some calls which are or become aggressive, abusive and offensive. These require special measures. Such calls can originate from landline, mobiles and text messaging.

Definition

Aggressive, abusive and offensive calls are those which cause alarm and/or distress to the recipient by virtue of the vocal tone of the caller, the content of the call, or its length.

The reasons for such aggressive, abusive and offensive calls vary:

- Dissatisfaction with the service;
- Dissatisfaction with a member of colleagues;
- The health of the caller.

Silent calls are also classified as offensive.

Aim

Since a consistent approach by all colleagues employed by the Trust to aggressive, abusive and offensive telephone calls is essential, this procedure aims to resolve such calls by either de-escalating the call to a reasonable tone and language or progressively terminating the call.

The Communication Act 2003

The Communication Act 2003 was introduced so that individuals, commercial organisations and public bodies could have access to secure communications and to ensure that transmissions should not cause alarm and distress and be used to harass, threaten, bully and record images of an offensive and criminal nature. Equipment includes fixed and mobile telephones using voicemail and messaging, e-mail and Internet. Since Facebook and other social networking sites also use the Internet, transmitted information is also covered by the Act. The Act applies equally to private equipment as it does to public equipment. Punishment can be extensive and includes fines, community penalties and imprisonment.

Two Sections are relevant. A person is guilty who sends or causes to be sent under

- *S.127 (1) – offensive, indecent, obscene and menacing messages (to the recipient*)**.**

  Examples are a single call of extreme or obscene language.

- *S.127 (2) - false messages/persistent use of communications network for the purpose of causing annoyance, inconvenience or needless activity.*

  Examples are persistent silent calls, hoax calls to private and public organisations resulting in disruption or anxiety and single hoax calls resulting in major disruption or substantial fear. Security Policy V4 - 24 - March 2016

In order to identify and pursue crime it is essential to record or retain the evidence. It is therefore very important victims save, ideally record, text messages and images and comments on social networking sites so an evidential case can be built. Without the evidence, crime cannot be proven.

It is strongly recommended in correspondence with individuals about their telephone manner reference is made to the Act.

Aggressive, abusive and offensive calls

On receiving a call which is abusive, aggressive or offensive, the following procedure will be adopted.

Step One

If the caller is or becomes abusive, aggressive or threatening, interrupt, if necessary and inform the caller:

> *I realise you may be angry/upset, however the manner in which you are speaking to me is unreasonable and I am therefore asking you to stop speaking to me in that manner'*

Consideration should be given to asking for the caller's number with a view to returning the call after a suitable 'cooling off' period of about ten minutes. It is important the call is returned within the given period and that colleagues refer to Step Four:

- Note the name being given by the caller;
- Note the time of the call;
- Record what is being said if possible.

Step Two

If the abusive, aggressive, offensive language or attitude continues, politely advise the caller:

> *Unless you stop being offensive/abusive/aggressive, I shall end this call immediately.'*

Step Three

If the behaviour continues, give the caller a FINAL warning:

> *You are taking note of my warning and I am therefore ending this call. Goodbye.*

Disconnect immediately.

Step Four

If the call is returned OR the caller calls back, remind the caller:

> *I expect you to be courteous and reasonable. If this does not happen, and I hope that it will, then I shall terminate the call immediately.*

It is strongly recommended the four Steps be extracted from this procedure, printed on coloured paper and posted near telephones as an aide-memoir.

Silent Calls

In silent calls, listen for and note noises and sounds in the background that may help to identify the caller or location from which the call is being made.

Text Messaging

In the event that abusive text messages are received, these should be saved as evidence.

Reporting

Report abusive telephone calls to your manager and complete an Incident form and clinical note if appropriate.

If colleagues are distressed by the call, or have concerns about handling future calls from the same individual, inform your manager, who may contact the Security Manager for advice on further actions that may need to be taken.

APPENDIX C: GUIDANCE ON THE PRESERVATION AND MANAGEMENT OF A SCENE FOR GATHERING FORENSIC EVIDENCE FOLLOWING A SERIOUS INCIDENT

Introduction

In the evidence chain beginning at an incident scene, this evidence must be listed, packaged and secured to prove integrity and admissibility in any future court proceedings.

Management of Evidence

Evidence management is critical to the outcome of criminal prosecutions or fact gathering, therefore is essential that measures are adopted to preserve its integrity, particularly in the early phases of an incident.

Failure to do so could reduce its quality and therefore jeopardise an inquiry, investigation or prosecution. It is important evidence is:

- Collected in a fashion which does not compromise the nature of the evidence;
- Kept in a fashion which maintains the nature of the evidence;
- Handled in a fashion which allows no doubt that the evidence could not have been accidentally or deliberately altered or substituted.

Procedure

If life is at risk, this should be paramount and dealt with appropriately;

Ensure the scene is not accessible to anyone until given permission by either the police or senior colleague by locking the doors containing the scene or placing a person at the scene to protect the evidence:

- Mark the scene with barriers if locking is not possible;
- Report the event to senior colleagues and relevant external agencies;
- Ensure any items removed from the scene, for whatever reason, are noted and reported to the investigating team;
- Ensure all colleagues involved receive appropriate support in dealing with serious incidents.

The nature and seriousness of an incident may necessarily inconvenience Trust services.

If in doubt at any stage of this process, colleagues should contact the Security Manager (during office hours) or the On Call Manager (out of hours).

APPENDIX D: GUIDANCE – BOMB THREATS ANDSUSPECT PACKAGES

- A bomb or incendiary device is easily disguised, and is designed to cause damage by blast or fire. They can be concealed in a briefcase, handbag and flask or in the case of incendiary devices, in a cigarette pack or similar container. Litterbins and toilets have been favoured for depositing devices in the past.
- Report to a senior colleague any object/person you see which you consider is suspicious. Don't hesitate or think twice about it. No one will criticise you for a false alarm.
- Do not touch or attempt to move a suspicious item.
- Notify the police immediately giving your name, job title, your exact location and contact telephone number.
- Remain at a safe distance from the object and keep others away. Turn off radios / mobile phones within close proximity of the bomb or suspect package.
- The police and bomb disposal team will want to talk to you so make yourself known to the Emergency Services. Your first-hand account of what you have seen is essential.
- After a safe evacuation from the premises, please ensure all colleagues, contractors and visitors remain outside of the premises and a sufficient distance away from the building concerned. A minimum distance is 100 metres from the location of the incident but this will also depend upon police advice and other information available at the time of the event.

Please be aware that fire evacuation assembly points may be too close to the property in question.

- A check of all personnel should be conducted by managers or senior member of colleagues present to ensure everyone has evacuated the premises.
- **Colleagues should not go to their cars** nor remove their cars from the car park; this will take too much time and will lead to confusion.
- **Do not let anyone re-enter the building** until instructed the building is safe.
- The priority is the safety of colleagues and public and to minimise the risk of injury.
- If you notice a package, about which you are suspicious, consider the relevant risk to both colleagues and patients within the premises and similar actions to those listed above in this section. If you have a serious concern about a package then, do not touch it and instigate the emergency evacuation procedure. Do not use mobile phones, personal radios or similar electrical devices in close vicinity of such suspect devices.
- The person receiving the notification of a bomb, or similar alert, is the key to dealing with the incident and will be a key liaison for the police and Security Manager with whom to make contact with. The details of the threat received, and its accuracy, are key to dealing with the threat.

- A decision to reoccupy the building should only be taken once instructed to do so by the Police.

Postal Bombs – Possible signs and appropriate action to be taken.

Any one of the following signs should alert members of colleagues to the possibility a letter or package may contain an explosive device:

- Grease marks on the envelope or wrapping;
- Unusual odour such as marzipan or machine oil;
- Visible wiring or tin foil, especially if package is damaged;
- Envelope or package may feel heavy for its size;
- Weight distribution may be uneven;
- Contents may be rigid inside a flexible envelope;
- May have been delivered by hand from unknown source;
- If a package, it may have excessive wrapping;
- There may be poor handwriting, spelling or typing;
- It may be wrongfully addressed or from an unexpected source;
- There may be too many stamps for the weight of the package.

Initial action for dealing with a package that may contain an explosive device:

- Put down gently and walk away from it;
- Evacuate the immediate area and raise the alarm;
- Call 2222 and call The Security manager.

(*Immediate area may mean a room, department or building and will depend upon the size and type of building*)

- Inform the police via the 999 system.
- Inform your manager.
- Prevent anyone from re-entering the premises.
- Do not place the package into anything (e.g. water) or place anything on top of it.
- Do not tamper with or open the package.
- Make a description of the article and its location within the room (e.g. size, shape, lettering on it).
- Establish if possible, whether the person to whom the package is addressed is expecting the package.
- Complete an Incident form.

Dealing with Telephone Warnings of a Bomb Threat

In all cases telephone the police immediately via 999 system with as much information as possible.

There are three key rules:

- Keep calm;

- Obtain as much information as possible for the caller – make notes;
- Keep the line open even after the caller has hung up.

Report the call to the police and your manager.

If you receive a threat about a bomb at an alternative address then you should:

- Contact the police immediately, by dialling 999, and inform them clearly and concisely, of the information you have received;
- Attempt to get in touch with the premises to which the threat has been made in order for them to instigate their evacuation procedure;
- Contact the Security Manager or other Trust senior manager to inform them of the threat you have received and the actions you have taken.

It is advised all receptionist colleagues within the Trust should receive a direct copy of this procedure, which should be kept by them, at all times, within their work area. Any new receptionist colleagues, including bank colleagues, should receive a copy of this procedure,

APPENDIX E: GUIDANCE - SIEGE OR HOSTAGE TAKING INCIDENTS

Any person held against their will by force or threat of force (expressed or implied) must be considered a hostage. The taking of hostages is used in an attempt to secure total control over another person in order to gain compliance with the wishes of the hostage-taker(s) in order to bring about the hostages release.

Hostage taking is a serious crime defined in law as:

A person whatever his nationality, who in the United Kingdom or elsewhere,-

(a) detains any other person ('the hostage'), and

(b) *in order to compel a state, international governmental organisation or person to do or abstain from doing any act, threatens to kill, injure or continue to detain the hostage, commits an offence.*

(Contrary to: The Taking of Hostages Act 1982, Section 1).

Confusion or mishandling of a hostage incident could lead to avoidable serious consequences.

Primary objectives during a hostage situation are to:

- Preserve life;
- Maintain the safety of colleagues and the public.

Contacting the Police

The taking of hostages is always a matter for the police and every area of the United Kingdom has officers on call who are specifically trained in hostage negotiation techniques. The police must therefore be called using 999, as soon as possible. The colleague making this call should make it perfectly clear there is a suspected hostage situation. At the same time a senior member of Trust colleagues available must be informed.

Where the situation includes threats of explosives or other hazards, the guidance given on dealing with bomb threats above must be considered.

The police will benefit from the following information where available:

- The exact location of the incident including access points;
- Details of the hostage-taker including clinical condition and events leading up to the incident;
- Details of hostages;
- A suitable rendezvous point for police arrival, where they will be met by appropriate members of colleagues;
- Any known weapons or items being used as such;
- Any known injuries to any party.

Primary Action

The following provides guidance only until the arrival of police officers who, upon arrival, will take over the control of the situation. The first five to ten minutes of any hostage situation are critical to setting the stage for the subsequent outcome, and tensions will be highest at this stage. It must be understood the police have overall responsibility for the incident.

Prior to the arrival of the police, no attempt should be made to enter into any form of discussion with the hostage-taker, unless failing to do so would place the hostage at greater risk. No negotiation should be undertaken and no requests granted. If confronted by the hostage-taker(s) it must be stated you do not have the authority to grant any of their demands.

No attempt at intervention should be made whatsoever, if there is any doubt as to its success or places the safety of those concerned. No intervention involving the use of force must be used unless:

- Life is in immediate danger;
- Forcible intervention has a high probability of success.

If possible and it is safe to do so, the situation should be carefully assessed (for example, through the use of CCTV) in order to determine:

- The number of hostages;
- Physical descriptions, especially of the hostage-taker(s);
- Any specific demands or statements. Make written notes. It is useful to keep a log of times and actions taken for the information of the police;
- Behaviour patterns;
- Types of weapons;
- Any other potentially useful facts.

Steps must be taken to ensure the police are contacted as soon as possible together with details of any action taken. This should be done in a quick, quiet and discreet manner out of sight and hearing of the hostage taker(s).

Where possible, relevant colleagues should be directed to secure the location by establishing an exclusion perimeter around the incident site at an appropriate distance relative to the risk presented. This will prevent the accidental incursion of unwary colleagues, patients and visitors into the incident scene. The exclusion area should also ensure the immediate access route to the scene is secure, unobstructed and preferably unobserved from the incident location.

All non-essential colleagues and mobile patients should be withdrawn from the area, ensuring this is done in a manner which will not cause alarm to the colleagues themselves or exacerbate the hostage situation. If this cannot be done without risk of inflaming the incident, no action should be taken. Where practicable, colleagues and patients should be protected by the securing of doors to relevant areas.

Arrangements should be made for all calls into and out of the hostage area to be diverted and for dedicated lines of communication to be made available to relevant parties.

Consideration should be given to greater risks than those currently present (i.e. access to hazardous materials) and, where it is safe to do so, steps should be taken to prevent access.

Secondary Action - Siege or hostage Situation

Witnesses to the incident should be asked to remain close to hand in order to provide the best information to the police when they arrive. Consideration should be given to arranging suitable support, such as access to counselling services, for those who may have been traumatised by the incident.

Information held pertaining to hazardous materials and fire hazards present on the site should also be made available to the emergency services.

The Trust may consider invoking its Incident Response Plan by declaring a major incident.

No one should talk to the media unless the police press officer, who would have obtained the agreement of the police senior investigating officer in charge of the incident, approves the text. The hostage-taker(s) may be listening and could react adversely to media attention. The Security Manager or appropriate senior personnel should arrange for the communications manager to be briefed on the incident and they will liaise with the police press office, as appropriate.

Ancillary Action - Siege or Hostage Situation

Consideration should be given to the location of other buildings in relation to the security incident, and whether any action needs to be taken in respect of these (i.e. managing unwanted onlookers).

Appropriate personnel and medical records of all parties involved should be made available to the police upon request.

The notification of next of kin for those held hostage is a matter for the police, unless specifically instructed by them otherwise.

Post Incident Management and Review

As soon as possible after the event, a meeting should be convened between all the agencies involved. The purpose of this debrief is to learn from the experience and to afford the revision of local and national guidelines or procedures in the light of that experience.

Guidance for Colleagues if Taken Hostage

The sudden occurrence of a hostage situation can cause fear and panic, but it is important to try and remain as calm and as rational as possible:

- If you need medication, ask for it;
- Otherwise, do not say or do anything that may put you or others at further risk;
- Do not lose hope and avoid an open display of despair;
- Initially, do not speak to anyone unless spoken to;
- Try to calm the hostage-taker;
- Do exactly what you are told and do not make suggestions;
- Try to appear calm but do not turn your back towards the hostage taker;
- Under no circumstances argue with the hostage-taker;
- Be observant, you may be released at any time;
- Expect noise and lights if a rescue attempt is made;
- In the case of a rescue attempt drop to the floor and stay there until told otherwise by one of the rescuers.

APPENDIX F: GUIDANCE FOR COLLEAGUES ENCOUNTERING ANY SORT OF WEAPON/FIREARMS IN A PATIENT'S HOME

- Do NOT ask questions but try to observe as much detail as you can about the weapon. Execute exit strategy (professional excuse if necessary) as a priority.
- Once in a safe place (away from the property) call line manager/colleague/buddy to make them aware of the weapon and to confirm you are in a safe place.
- If necessary call the Police.
- Document in full and submit an Incident Form
- Contact the Security Manager.
- Consider putting an alert on the system so other colleagues are aware of the hazard in the patient's home. Discuss at team handover to ensure colleagues are also aware.
- Review the care plan immediately to protect colleagues from the hazard. Future home visits may not be considered appropriate until the risks are addressed.
- The Security manager will liaise with the Police who will advise on any actions they can take and on an appropriate response.
- Convene a meeting with the Security manager and Departmental managers if required to discuss any appropriate actions and review care plan for future treatment.
- The patient may need to be communicated with and told to lock the weapon away as per license requirements (if it is a shotgun or a firearm – different license for each).
- Lone working procedures should be discussed and reviewed.

BETTER TO BE SAFE THAN SORRY – IF YOU SUSPECT IT IS A WEAPON THEN MAKE SAFE EXIT ASAP, GET TO A SAFE PLACE AND RAISE THE ALARM.