Somerset Partnership NHS
NHS Foundation Trust

# SECURITY MANAGEMENT POLICY

## (including guidance on abusive phone calls, ID badges, bomb threats and siege/hostage taking)

| | |
|---|---|
| Version: | 4 |
| Ratified by: | Senior Managers Operational Group |
| Date ratified: | March 2016 |
| Title of originator/author: | Security Managers |
| Title of responsible committee/group: | Regulation Governance Group |
| Date issued: | **March 2016** |
| Review date: | **February 2019** |
| Relevant Staff Group/s: | All Trust staff |

**This document is available in other formats, including easy read summary versions and other languages upon request. Should you require this please contact the Equality and Diversity lead on 01278 432000**

**DOCUMENT CONTROL**

| **Reference** AS/Mar16/SP | **Version** 4 | **Status** Final | **Author** Head of Corporate Business |
|---|---|---|---|
| **Amendments:** CQC standards updated. New guidance on ID badges, bomb threats, abusive calls and siege/hostage taking. CCTV guidance removed as now separate policy. | | | |
| **Document objectives:** Ensure and promote a secure environment to protect the safety of everyone involved in the healthcare and safeguarding public and private assets against loss, theft, damage and disruption which could be detrimental to the continuation of care. | | | |
| **Intended recipients:** All Trust staff | | | |
| **Committee/Group Consulted:** Health, Safety and Security Management Group; | | | |
| **Monitoring arrangements and indicators:** Health, Safety and Security Management | | | |
| **Training/resource implications:** Inductions, PMVA, Search training and requested training sessions appropriate to the role. | | | |
| **Approving body and date** | Regulation Governance Group | Date: February 2016 | |
| **Formal Impact Assessment** | Impact Part 1 | Date: March 2016 | |
| **Ratification Body and date** | Senior Managers Operational Group | Date: March 2016 | |
| **Date of issue** | **March 2016** | | |
| **Review date** | **February 2019** | | |
| **Contact for review** | Head of Corporate Business | | |
| **Lead Director** | Director of Governance and Corporate Development | | |

**CONTRIBUTION LIST Key individuals involved in developing the document**

| **Name** | **Designation or Group** |
|---|---|
| Andrew Sinclair | Head of Corporate Business |
| Tracey Edwards | Security Manager |
| Group Members | Health, Safety and Security Management Group |
| Group Members | Regulation Governance Group |
| Richard Painter | Head of Safeguarding |

**CONTENTS**

## 1. INTRODUCTION

1.1 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.

1.2 Security is everyone's responsibility. Security involves all groups of staff at all levels and to be effective needs the support of everyone in the organisation. 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.

1.3 Everyone who works in the Trust, must be aware of, and, wherever possible, protected from the risk of illegal acts involving violence, (threatened and actual), harassment, or damage to property and theft.

1.4 The Trust aims to ensure a risk aware culture exists within the organisation and that it has complied with the Secretary of State's Directions in having a Local Security Management Specialist (LSMS) and Security Management Director (SMD).

1.5 Where there are potential safeguarding children or safeguarding adults concerns or there may be staff or public safety considerations, advice must be sought from the Trust's Safeguarding Team.

## 2. PURPOSE AND SCOPE

2.1 The Security Policy supports the Trust's Security Strategy to provide high quality healthcare through a safe and secure environment which protects everyone, including patients, staff, visitors and their property, and the physical assets of the Trust.

2.2 This policy document is intended to ensure the Trust:

- provides direction and help to those managers and staff who are entrusted to deal with the Trust's security provision;
- supports the delivery of high quality clinical and non-clinical services by providing a secure environment;
- complies 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 This policy identifies responsibilities, systems and procedures to ensure a safe and secure environment for staff, patients and their visitors while on Trust premises, and the security of all property contained within those premises.

2.4 The policy ensures appropriate action is taken when Trust security is breached and in the event of a security incident escalating, any action taken is commensurate with action required to be taken in accordance with the Trust Incident Response Plan.

2.5 The policy describes the roles and responsibilities of the Security Management Director (SMD) and the Local Security Management Specialist (LSMS) for Security Management within the NHS.

2.6 This policy applies to all staff, visitors and patients attending or working for the Trust, including contractors and staff working in the community. Volunteers and VIP visit arrangements are set out in the Volunteers Policy.

## 3. DUTIES AND RESPONSIBLITIES

3.1 The **Chief Executive** has overall responsibility for the development and maintenance of security throughout the Trust.

3.2 A **Non-Executive** member of the Board is appointed to promote security within the Trust.

3.3 The **Director of Governance and Corporate Development** is the Security Management Director (SMD) and has delegated responsibility for the strategic management of security. The SMD monitors and ensures compliance with directions set out by the Secretary of State on NHS Security Management and is responsible for taking reports and action plans to the Executive Management Team for consideration and implementation. The SMD delegates various responsibilities to the Head of Corporate Business and/or the LSMS.

3.4 The **Head of Corporate Business** is responsible for promoting and maintaining the Security Policy and day-to-day management of security services. .

3.5 Executive **Directors** are responsible for:

- promoting the Trust Security Strategy within their areas of responsibility;
- ensuring adequate protective security measures are in place to minimise risks against people, property and information in their areas of responsibility.

3.6 For the purposes of this policy, the **Security Managers** are defined as the SMD, Head of Corporate Business and LSMS.

3.7 **All Managers** have a specific duty to promote security by implementing this policy and any related procedures and by promoting security awareness ensure:

- their staff are aware of their personal responsibilities and follow this policy;
- there is a procedure to record details of valuable or important property within their department so that an accurate description can be passed to the police in the event of any equipment lost through theft or damage;
- arrangements are made to secure the department out of working hours together with the safe custody of keys;
- there is a procedure for setting of any security alarm or device to protect property out of hours;
- areas containing items of equipment are kept locked when not occupied;

- staff, patients and visitors are aware of security measures and requirements;
- all security-related incidents are recorded on the Datix system and actions to minimise further risks and breaches are recorded;
- records are kept of all keys issued to staff in their department and reporting of all losses of keys through Datix;
- advice from the LSMS is sought so that security is maintained within their service;
- the LSMS is advised of any changes within their department which may adversely affect security;
- all Trust staff have an identification badge and, when appropriate, wear them.
- review and respond to incidents reported by staff via Datix or other means

3.8 The **Local Security Management Specialist (LSMS)** is accountable to the Director of Governance and Corporate Development and responsible to the Head of Corporate Business for implementing this policy by:

- analysing security incidents to identify trends, draw conclusions and make recommendations;
- regular review of the risk registers to ensure local risks are effectively managed;
- applying sanctions by civil, criminal, disciplinary and procedural measures which may include seeking redress through criminal and civil justice systems against those whose actions lead to harm to staff, patients and others or the loss of Trust assets and resources;
- assessing security technology and its application;
- creating proactive security awareness and promoting the deterrence and prevention of breaches of security;
- drafting the annual Security Report for submission to the Board and Security Management Service;
- delivering formal and informal security awareness training through inductions, briefings, updates and ‘bespoke’ sessions to ensure all staff are aware of the risks;
- ensuring victims of crime are supported;
- interpreting primary and secondary legislation and advising on the standards required to ensure compliance;
- investigating breaches of security in a fair, objective and professional manner;
- liaising with external agencies as appropriate, e.g. Security Management Service, police, HM Courts Service;
- promoting a range of proactive and reactive security generic actions;

- providing expert security advice to protect people, property and assets;
- undertaking security risk assessments either as part of a rolling programme or at the request of managers.

3.9 **All Staff** must follow this policy and 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 a Datix 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 security procedures at all times;
- wear an identification badge whilst on duty for the Trust and this also applies to those who work in the community;
- be responsible at all times for the protection and safe keeping of their own property;
- attend security-related training appropriate to their appointment, as required by their manager.

3.10 **Contractors** will adhere to this policy and will report any risks issues to the local Trust manager;

## 4. EXPLANATIONS OF TERMS USED

4.1 **Assault:** The intentional application of force against the person of another without lawful justification, resulting in physical injury or personal discomfort. (NHS Definition);

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

4.3 **DATIX**: electronic database used by the Trust to report Untoward Event Reports, PALS/Complaints, and Local/Corporate Risks;

4.4 **'Defence in depth'**: continually surveyed interdependent and interlocking protective security measures arranged in depth;

4.5 **NHS Protect (NHSP):** the NHS body established by the Secretary of State for Health Directions on NHS Security Management Measures dated 24 March 2004 to protect NHS assets and resources;

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

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

4.8 **Repeat victimisation**: crime frequently returned to the same target because of ineffective design infrastructure, likely quick replacement of losses; previous success or a lack of a previous response.

4.9 **Threat**: the illegal and unacceptable activities which seek to disrupt or cause distress to people and property.

## 5. SECURITY 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 divert breaches of security and criminal event that could cause harm to the Trust;
- ensure the personal safety and welfare of patients, staff and visitors while on Trust property and when working in the community by developing appropriate security systems;
- secure Trust property and premises against security breaches and the effects of environmental conditions by highlighting security weaknesses.

### Security Risk Assessments

5.3 Internal and external evaluations of security risks must be undertaken to assess the security risks.

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

5.5 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 that exist and what would be their effect;
- assesses those risks for potential frequency and severity;
- eliminates the risks which can be eliminated;
- identifies how risks can be mitigated/managed;
- provides current measurement and assists target setting for reduction in risks.

5.6 Security risks identified will be recorded on team and service risk registers and escalated to divisional or corporate risks in line with the Trust's Risk Management Policy.

5.7 The Trust will maintain a Security Strategy and annual work programme which includes pro-active security risk assessment of Trust premises and assets. Each assessment will be summarised in a report which will be shared with the relevant senior and local managers and reported to the Health, Safety and Security Management Group. The report will include a summary of risks assessed for potential impact and likelihood and a proposed action plan to eliminate and/or mitigate the risks identified.

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 Health, Safety and Security Management Group, will be implemented according to agreed timescales and monitored quarterly reports to the Group.

**Reporting and Recording**

5.10 In line with the Trust's Untoward Event Reporting Policy, all staff must ensure all security incidents or "near-miss incidents" are reported. All untoward events must be reported using the Trust's Datix system.

5.11 The Security Managers will have access to all Datix security reports, including violence and aggression, theft, damage to property/equipment and all other security incidents which may result in prosecution.

5.12 The Security Managers will use Datix reports and other information to inform any requirement for more detailed security risk assessments. The following are sources of information which the Security Managers will use to inform risk assessments and action plans:

- daily review of DATIX reports;
- reviews of the Risk Registers;
- formal surveys, inspections and unannounced visits;
- investigation into breaches of security to draw conclusions and make recommendation for remedial action;
- information from NHS Protect;
- national and local legislation and policies and NHS communications affecting the management of security.

5.13 Action plans developed from reactive risk assessments will be developed and monitored in line with the process set out in paragraphs 5.6 – 5.8 of this policy.

5.14 Reports to NHS Protect will be made by the Security Managers through the Physical Assaults Records (PARS) system.

## 6. SECURITY PLANNING

**Principles**

6.1 Security planning is reliant on:

- analysis of security risk assessment;
- cost-effective deployment of protective security measures;
- early consultation in building and refurbishment projects to determine physical security measures;
- pro-active security management.
- making cost effective and sensible recommendations.

**Control of Access**

6.2 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.

6.3 Access into non-public areas by anyone without the appropriate authority or without good reason will be challenged and the event recorded on DATIX. Managers will support staff with challenges, if necessary by intervention.

6.4 Services will maintain a Visitors' Log which will be retained for a minimum of six years after which it must then be disposed of securely.

6.5 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.

**Maintenance**

6.6 Local managers must be notified by the estates department before starting maintenance or contract work e.g. window cleaning, telephone repair. In secure mental health wards, the work should be closely supervised. All maintenance contractors in line with the Control of Contractor Policy must report to site in the first instance.

6.7 Local managers will ensure the security of patients, staff, equipment and property. This is particularly relevant in areas occupied by vulnerable patients and during the hours of darkness.

**Key, fob, swipe card and combination lock security.**

6.8 Keys, fobs and combination settings impact on the management of security. *See* Appendix A - Security of Keys, Fobs, Swipe Cards and Combination Settings.

**ID badges**

6.9 ID Badges do not authorise automatic access, irrespective of status and profession. Staff will report losses and damage using DATIX**.** See Appendix C - Procedures for the application of an ID Badge.

## 7. STAFF SAFETY

**Training**

7.1 All staff must receive induction and familiarisation training in methods to prevent and reduce crime.

**Lone working**

7.2 All staff will apply and adhere to the Lone Working Policy as it applies to them.

**Violence and aggression**

7.3 Procedures for dealing with incidents of violence and aggression can be found in the Prevention and Management of Violence and Aggression Policy. See Appendix D – Procedure for managing Abusive, Aggressive and Offensive Telephone Calls.

## 8. SECURITY CONSIDERATIONS

8.1 Damage to and the loss of property owned by, leased by or lent to the Trust can have serious financial and operational consequences. All staff will make every effort to protect all property. All criminally damaged property will be reported to the police.

**Work area security**

8.2 Staff will apply 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. If an investigation can prove that a breach of security has occurred as result of these principles not being followed, disciplinary procedures may be a consequence.

**Staff responsibility**

8.3 All staff have a responsibility for the security and the prevention of the theft of property issued to them by the Trust as part of their work.

8.4 Staff working in the community must ensure their Trust equipment, such as clinical bags, patients' notes and laptops are secured at all times. Staff will adopt basic vehicle crime prevention by not leaving Trust property in sight or in vehicles overnight.

8.5 Managers have a responsibility to collect ALL property loaned to employees, such as ID badges, uniforms, electronic equipment and keys, on termination of their employment with the Trust.

**Staff property**

8.6 Within all Trust areas, staff are advised against bringing cash or personal belongings, in excess of their personal daily needs, whilst on duty, and any cash and personal belongings should where possible remain with the member of staff at all times. If this is not possible all personal belongings and cash should be stored in a secure area within the work place.

8.7 The Trust will not be responsible for loss of staff property, cash and belongings. Each service area is expected to take the most appropriate measures possible to ensure work areas remain as secure as possible and that appropriate storage facilities are provided to staff.

8.8 Although the Trust accepts no responsibility for the loss of personal belongings, staff are encouraged to report any loss of their property and cooperate in any enquiry which may result in connection with the loss.

8.9 Managers are encouraged to remind staff of the advisability of insuring personal property and that the Trust accepts no responsibility for its loss.

8.10 Where changing facilities are provided for employees, the room should be

kept locked to prevent unauthorised access. Lockers, when available, should be used for all personal property. In the event of deficiencies or un-serviceability, Estates and Facilities should be informed via the line manager

8.11 Advice can be sought from the LSMS on appropriate security measures to be implemented within work areas to ensure the protection of personal belongings.

**Patient property**

8.12 The loss of a patient's property can be particularly stressful, can affect treatment and may damage the reputation of the Trust. Every effort will be made to safeguard patient property, particularly that belonging to people who are vulnerable or lack capacity.

8.13 Patients' property should be handled in accordance with Trust policy for managing patient's valuables policy and secured accordingly.

8.14 No responsibility can be accepted by the Trust for the loss of personal property that is not stored as per 8.13.

8.15 Suitable and sufficient documentation should be completed to record personal items of patients while on Trust premises, in line with the Trust's policy on Inpatient Property Management. In addition, guidance should be given to patients by the Trust and individual departments on the suitability of bringing valuable items onto Trust premises. However, it is the responsibility of the patients, visitors and contractors to make sure their personal property is secure.

**Drugs and medicine security**

8.16 The Trust has established practices to ensure FP 10 prescription pads, medicines and drugs are handled appropriately (see the Medicines Policy). It is the responsibility of the Head of Medicines Management and managers of clinical teams to ensure they are followed. See Appendix E – Managing A Scene for the Collection of Evidence following a Serious Incident.

**Access Control - Contractors and Visitors**

8.17 All contractors and visitors requiring access to staff 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 staff 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 member of staff in a position of vulnerability. Any unauthorised access to staff only areas, or patient treatment areas should be reported to the manager of that area and an incident report completed.

8.18 Trust premises are private and there is no right of way. 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.

8.19 Members of the public are entitled to enter Trust sites in connection with healthcare, be that as patient, carer or visitor for business purposes.

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 staff should summon assistance from porters, other members of staff, or the police as most appropriate in the circumstances.

**Identification Badges**

8.20 An Identification Badge (ID Badge) is an accountable document designed to establish the identity of the holder. It is not a permit that gives the holder the right to enter controlled areas.

8.21 The security benefits of an ID Badge system are to:

- assist patients to identify members of staff, a need highlighted in the Francis Report;
- prevent and deter bogus medical officials or health workers from impersonating Trust staff;
- assist staff in confirming identification of other members of staff when handing over drugs, valuables and property and other material;
- distinguish easily Trust staff from the staff of other agencies, contractors, maintenance staff and visitors working on Trust premises.

8.22 It is the policy of the Trust:

- all staff, volunteers and other authorised contractors/ visitors are clearly identifiable as such whilst on duty by displaying an Identity Badge. This is particularly relevant in clinical areas where there is frequent contact with patients and the public;
- identification must be worn in such a way any patient, visitor or other member of staff may easily verify name and area of work within the Trust;
- the only exception permitted is where Health and Safety considerations prevent safe use;
- patients are to be advised not to accept treatment from anyone failing to display a valid ID Badge.

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

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

8.25 Lost or stolen identification badges and all problems relating to the proximity card system (including lost, missing or stolen cards) must be reported to the line manager and a Datix report completed.

8.26 When a staff member leaves employment in the Trust, it will be the

responsibility of the manager to retrieve the identification badge and arrange for its deactivation and destruction.

8.27 The Trust ID Badge Application Form is provided in Appendix B of this policy and is also available on the Intranet.

**Security of Motor Vehicles**

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

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

## 9. PREVENT

9.1 Should any member of staff 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 staff 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.

9.2 Staff must seek advice through the Trust's Safeguarding Team, and out of hours advice can be sought via the Trust's On Call Senior Manager.

9.3 Where staff 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 on.

## 10. TRAINING REQUIREMENTS

10.1 The Trust recognises the need for effective training of staff to deal with security related issues and will, through the Learning and Development Department and the LSMS, ensure security advice and training, is provided:

- Conflict Resolution Training to reduce the likelihood of assault;
- personal security and safety within the working environment;
- responding promptly and effectively to all security incidents.

10.2 Specific areas where training is required will be identified in individual policies; however, these should include a minimum of:

- Conflict Resolution Training for all staff who interact with the public;
- physical intervention and assault avoidance skills (where required by risk assessment);
- security/crime awareness;
- lone working safety (community based staff who conduct home visits).

## 11. EQUALITY IMPACT ASSESSMENT

11.1 All relevant persons are required to comply with this document and must demonstrate sensitivity and competence in relation to the nine protected characteristics as defined by the Equality Act 2010. In addition, the Trust has identified Learning Disabilities as an additional tenth protected characteristic. If you, or any other groups, believe you are disadvantaged by anything contained in this document please contact the Equality and Diversity Lead who will then actively respond to the enquiry.

## 12. MONITORING COMPLIANCE AND EFFECTIVENESS

**Responsibilities for conducting the monitoring.**

12.1 The Health, Safety and Security Management Group will be responsible for undertaking monitoring and reporting quarterly to the Regulation Governance Group.

**Methodology to be used for monitoring**

12.2 The following will be used:

- DATIX untoward event reports/near misses;
- annual Violence and Aggression Statistics (VAS) to NHS Protect;
- visits and requests from NHS Protect;
- review of corporate and local risk registers;
- scheduled and unscheduled internal security surveys;
- Security Strategy and accompanying Work Plan
- Annual Security Report to the Board and NHS Protect.
- Annual Work Plan
- quarterly Reports to the Health, Safety and Security Management Group.

**Process for reviewing results and ensuring improvements in performance occur.**

12.3 A quarterly Security Report will be presented to the Health, Safety and Security Management Group identifying critical incidents, incidents of good practice, action points and lessons learnt. This Group will be responsible for ensuring improvements, where necessary, are implemented. A regular Security Brief will be provided to staff to raise awareness through the staff newsletter: What's On@SomPar

## 13. COUNTER FRAUD

13.1 The Trust is committed to the NHS Protect Counter Fraud Policy – to reduce fraud in the NHS to a minimum, keep it at that level and put funds stolen by fraud back into patient care. Therefore, consideration has been given to the inclusion of guidance with regard to the potential for fraud and corruption to occur and what action should be taken in such circumstances during the development of this procedural document.

## 14. RELEVANT CARE QUALITY COMMISSION (CQC) REGISTRATION STANDARDS

14.1 Under the **Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (Part 3), the fundamental standards** which inform this procedural document, are set out in the following regulations:

| | |
|---|---|
| Regulation 9: | Person-centred care |
| Regulation 10: | Dignity and respect |
| Regulation 12: | Safe care and treatment |
| Regulation 15: | Premises and equipment |
| Regulation 17: | Good governance |
| Regulation 18: | Staffing |
| Regulation 20: | Duty of candour |

14.2 Under the **CQC (Registration) Regulations 2009 (Part 4)** the requirements which inform this procedural document are set out in the following regulations:

| | |
|---|---|
| Regulation 11: | General |
| Regulation 18: | Notification of other incidents |

14.3 Detailed guidance on meeting the requirements can be found at http://www.cqc.org.uk/sites/default/files/20150311%20Guidance%20for%20providers%20on%20meeting%20the%20regulations%20FINAL%20FOR%20PUBLISHING.pdf

14.4 **Relevant National Requirements**

Mental Health Act Code of Practice (2015) HMSO

Secretary of State Directive on Measures to Deal with Violence Against NHS Staff 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.

Speculative requirements required by the SMS.

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

## 15. REFERENCES, ACKNOWLEDGEMENTS AND ASSOCIATED DOCUMENTS

15.1 **References**

Home Office Crime Prevention Manual, Section 6.

Secretary of State Directive on Measures to Deal with Violence Against NHS Staff 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 Security Manual.

SMS Secured By Design – Hospitals; April 2005

Data Protection Act 1998

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

15.2 **Cross reference to other procedural documents:**

Safeguarding Adults at Risk Policy

CCTV Policy

Controlled Drugs Policy

Control of Contractors Policy

Counter Fraud Policy

Financial Procedures Guidelines

Health and Safety Policy

IM & T Policy

Locked Door and Door Control Policy

Lockdown Policy

Lone Working Policy

Medicines Policy

Patients Property Policy

Prevention and Management of Violence and Aggression (PMVA) Policy

Record Keeping and Records Management Policy

Risk Management Policy and Procedure

Serious Incidents Requiring Investigation Policy

Standing Financial Instructions

Untoward Event Reporting Policy and Procedure

Use of Personal and Trust Vehicles for Work Purposes Policy

All current policies and procedures are accessible in the policy section of the public website (on the home page, click on 'Policies and Procedures'). Trust Guidance is accessible to staff on the Trust Intranet.

## 16. APPENDICES

16.1 For the avoidance of any doubt, the appendices in this policy constitute part of the body of this policy and shall be treated as such.

| | |
|---|---|
| Appendix A | Security of Keys, Fobs and Combination Settings. |
| Appendix B | ID Badge Application Form |
| Appendix C | Procedure for Dealing with Aggressive, Abusive and Offensive Telephone Calls. |
| Appendix D | Preserving and managing a scene for evidence following a serious incident |
| Appendix E | General Guidelines – Bomb Threats and Suspicious Packages |
| Appendix F | General Guidelines – Siege or Hostage Taking |

**APPENDIX A**

## SECURITY OF KEYS, FOBS & COMBINATION LOCKS GUIDANCE

Since the compromise, loss and poor maintenance of keys, key fobs, swipe cards and combination settings lead to inconvenience, expense and increased risk, it is important that Ward/Team managers have effective controls to ensure that people, property and resources are safeguarded. Failure to do so may have consequences in excess of assessments originally considered. (See Locked Door and Door Control Policy).

### 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

#### Accountability

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 maybe temporarily or permanently replaced.

The circumstances of missing keys, key fobs and swipe cards are to be reported on DATIX 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 keep a key register 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.

The Head of Corporate Business is responsible for the management and administration of commercial key holding contracts.

**Losses.**

If a key, key fob or swipe card is lost, it must be considered compromised and the loss must be reported via Datix. 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, staff, information and material.

Security keys should be kept separate to general purpose keys and assigned only to staff 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 will be using the Key Register.

Procedures for key control are:

- on receipt of office furniture and taking over buildings and offices, ward/team managers will separate the bunches of keys and assign primary keys to users;
- spare keys are to be centralised in the department key press;
- each department must have a key press;
- keys are not to be stored in desk drawers or secreted elsewhere;
- 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;
- the location of all keys will be recorded so in the event that the primary key is mislaid or lost, work routine will not be disrupted;
- local key holders are identified for buildings, other than inpatient wards;
- all other staff should not take keys home in case the circumstances of an employee change (e.g. sudden sick leave) so difficulties are not experienced in recovering relevant keys;
- the manager should, if possible require handover of keys and key fobs prior to staff 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 member of staff no longer requires access;
  - annually.
- when a container leaves a department, the setting should be returned to the manufacturer's setting;
- the compromise of a setting(e.g. settings written on a notice board)and the requirement to access the record of settings must be recorded on DATIX;
- combination lock settings should be changed on a regular basis;
- any difficulties with issues around keys, fobs and combination lock settings can be referred to the LSMS.

**APPENDIX B**

## ID BADGE APPLICATION FORM

# ID BADGE REQUEST FORM

***PLEASE MAKE SURE THIS APPLICATION FORM IS TYPE WRITTEN & NOT HAND WRITTEN***

❑New Badge ❑Job Title/Location Change ❑Name Change ❑Loss/Damage

| | | | |
|---|---|---|---|
| Existing Badge Number (if applicable) | | JPEG Photo attached | Yes / No |
| First Name | | | |
| Last Name | | | |
| Job Title (max. **25** characters per line, max. **2** lines, including spaces) | | | |
| Full forwarding address for badge (Not home address) | | | |

**ID BADGE APPLICANT AGREEMENT**

- My photograph will only be used for Trust ID Badge purposes unless I agree otherwise.
- I will take responsibility for the security of the ID Badge(s) issued to me. I shall notify my manager if I either lose or damage my ID Badge and will complete a Trust DATIX Untoward Event incident reporting form.
- If my circumstances change, (e.g. change of name, change of role), I will reapply for a new ID Badge.
- I will return my ID Badge to my manager on leaving Trust employment.

***SEND TO YOUR MANAGER BY E-MAIL FOR AUTHORISATION***

***YOUR REQUEST WILL NOT BE ACCEPTED UNLESS YOUR MANAGER HAS AUTHORISED***

**After authorisation, the manager to send this form as an email attachment along with your photograph in a JPEG format to ask@sompar.nhs.uk**

| | |
|---|---|
| Manager's Name | |
| Manager's Signature | |
| Manager's Contact Number | |
| Date | |

## DATA PROTECTION ACT 1998

- Somerset Partnership NHS Foundation Trust takes all necessary steps to comply with the Data Protection Act 1998 and relevant information subordinate to the Act.
- All information relating to the application form and photo will be protected, as reasonably practical, against loss and unauthorised disclosure.
- It is the responsibility of the applicant to advise the Trust if information is no longer required.
- It is the responsibility of the applicant to take reasonable steps to keep ID Badges safe from theft and damage and to formally report such occurrences immediately to their manager.
- Employees will not use their ID Badges for any other purpose than when officially acting of the Trust.

**APPENDIX C**

## PROCEDURE 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 staff;
- the health of the caller.

Silent calls are also classified as offensive.

### Aim

Since a consistent approach by all staff 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.

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 that 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 staff 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 a Datix report and RiO note, if appropriate.

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

**APPENDIX D**

## PRESERVATION AND MANAGEMENT OF A SCENE FOR EVIDENCE FOLLOWING A SERIOUS INCIDENT

### INTRODUCTION

In the chain beginning at an incident scene, through investigation and on to Court room or HM Coroner's enquiry, evidence must be listed, packaged and secured to prove integrity and admissibility.

### 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 staff 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 staff and relevant external agencies;
- ensure any items removed from the scene, for whatever reason, are noted and reported to the investigating team;
- ensure all staff involved receive appropriate support in dealing with serious incidents.

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

If in doubt at any stage of this process, staff should contact the Head of Division or Head of Corporate Business/LSMS (during office hours) or the On Call Manager (out of hours).

**APPENDIX E**

## GENERAL GUIDELINES – 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 manager or head of service 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 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 staff, 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 staff present to ensure everyone has evacuated the premises.
- **Staff 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 staff 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 staff 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 LSMS 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 staff 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;

  (*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 Trust Datix Report Form and forward a copy to the Local Security Management Specialist.

**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 four 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 LSMS or a Trust senior manager to inform them of the threat you have received and the actions you have taken.

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

**APPENDIX F**

## GENERAL GUIDELINES - SIEGE OR HOSTAGE TAKING

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 staff 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 staff member making this call should make it perfectly clear there is a suspected hostage situation. At the same time a senior member of Trust staff 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 staff;
- 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 staff 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 staff, 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 staff and mobile patients should be withdrawn from the area, ensuring this is done in a manner that will not cause alarm to the staff themselves or exacerbate the hostage situation. If this cannot be done without risk of inflaming the incident, no action should be taken. Where practicable, staff 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.

LSMS or appropriate senior personnel should arrange for the communications manager and NHS SMS 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 Staff 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.