Livewell Southwest

Security Management Policy

Version No. 4

Review: April 2018

Notice to staff using a paper copy of this guidance

The policies and procedures page of LSW intranet holds the most recent version of this document and staff must ensure that they are using the most recent guidance.

Author:	**Head of Health, Safety & Security**
Asset Number:	**274**

Reader Information

Title	Security Management Policy V4
Asset number	274
Rights of access	Public
Type of paper	Policy
Category	On clinical
Document purpose/summary	To provide information and guidance enabling a safe and secure working environment for all employees, patients and visitors, and to prevent criminal acts from being undertaken on, or to, Livewell Southwest 's occupied property and assets owned or used by LSW employees.
Author	Head of Health, Safety & Security
Ratification date and group	18th March 2015. Policy Ratification Group.
Publication date	29th April 2015
Review date and frequency (one, two or three years based on risk assessment)	Three years after publication, or earlier if there is a change in evidence.
Disposal date	The PRG will retain an e-signed copy for the archive in accordance with the Retention and Disposal Schedule. All copies must be destroyed when replaced by a new version or withdrawn from circulation.
Job title	Head of Health, Safety & Security
Target audience	All employees employed by Livewell Southwest.
Circulation	Electronic: LSW intranet and website (if applicable) Written: Upon request to the PRG Secretary on ☎ 01752 435104. Please contact the author if you require this document in an alternative format
Consultation process	Health, Safety & Security Committee
Equality analysis checklist completed	Yes
References/sources of information	• Counter Fraud Security Management Service. • 'A professional approach to managing security in the NHS' Dec 2003. • Health and Safety at Work Act 1974 & Management of Health and Safety at Work Regulations. • NHS Protect Standards for Providers 2014/15 – Security Management and Fraud, Bribery and Corruption. • National Health Service Act 1977. • The Occupiers Liability Act 1984. • Prevention of Crime Act 1953. • NHS Litigation Authority Risk Management Standards 2013: 4.1 – Secure Environment. • Health and Social Care Act (2012).

	• Equality Act (2010). • Police and Criminal Evidence Act 1984. • Children's Act 1989.
Associated documentation	• Cash and Cheques Handling Procedure. • Health and Safety Policy. • Incident Reporting & Investigation Policy and Procedure. • Information Technology Security Policy. • Lockdown Policy. • Locked Door Policy. • Lone Working Policy. • Major Incident Plan including the Response to Suspect Packages and Bomb Threats, & Business Continuity Response. • Media Policy. • Patients' Monies and Property Policy. • Health and Corporate Record Management & Record Keeping Policy. • Risk Management Strategy. • Safe and Security Handling of Medicines Policy. • Searching Property and Person Policy. • Serious Incident Requiring Investigation (SIRI) Policy. • Violence and Aggression Management Policy. • Whistleblowing Policy.
Supersedes document	All previous versions.
Author contact details	By post: Local Care Centre Mount Gould Hospital, 200 Mount Gould Road, Plymouth, Devon PL4 7PY. Tel: 0845 155 8085, Fax: 01752 272522 (LCC Reception).

Document review history

Version no.	**Type of change**	**Date**	**Originator of change**	**Description of changes**
For previous review history please contact the PRG secretary.				
3	Ratified	18/02/2010	Policy Ratification Group	
3.1	Minor Amendment	25/02/2011	Health Safety & Security Management Advisor	Minor addition with Hostage Situation Guidance
4	Full review	16/12/2014	Head of Health, Safety & Security	Full review and transfer of hostage info to Lockdown Policy. Hyperlinks added.

Security Management Policy

1 Introduction

1.1 Livewell Southwest (hereafter referred to as "LSW") recognises its responsibilities to provide safeguards to protect employees, the prevention of crime and the loss of, or damage to property and equipment within the organisation.

1.2 The primary aims for security within the LSW are to maintain;

a) Personal safety of patients, employees and visitors.
b) Security of personal property of patients, employees and visitors.
c) Security of Hospital property, buildings and equipment.

1.3 In addition to LSW's responsibilities, effective security also depends on all employees being aware of their responsibilities including:

a) Duty to be observant and report security incidents and suspicious circumstances.
b) To cooperate with security arrangements put in place by the organisation.
c) Not to take actions that may compromise the security of premises, themselves or others.

1.4 The aim of the Security Management Policy is to deliver a secure environment for the protection and safety of everyone receiving or providing health and social care, and safeguarding public and private assets against loss, theft, damage and disruption that could be detrimental to the continuation and development of LSW.

2 Definitions

2.1 **Fraud** - a deception deliberately undertaken to secure unfair or unlawful gain.

2.2 **Theft** - the dishonest appropriation of property belonging to another with the intention of permanently depriving the other thereof.

2.3 **Corruption** - the offering, giving, soliciting or acceptance of an inducement or reward that may influence the action of any person.

2.4 **Threat** – the illegal and unacceptable activities that seek to disrupt or cause distress to people and property.

2.5 **Physical Assault** - the intentional application of force to the person of another, without lawful justification, resulting in physical injury or personal discomfort.

2.6 **Non-Physical Assault** - the use of inappropriate words or behaviour causing distress and/or constituting harassment, which includes:

• Offensive language, verbal abuse and swearing, which prevents employees from doing their job or makes them feel unsafe. • Loud and intrusive conversation. • Unwanted or abusive remarks. • Negative, malicious or stereotypical comments. • Invasion of personal space. • Brandishing of objects or weapons. • Unsuccessful physical assaults. • Offensive gestures.	• Threats or risk of serious injury to a member of employees, fellow patients/clients or visitors. • Bullying, victimisation or intimidation. • Stalking. • Spitting. • Alcohol or drug fuelled abuse. • Unreasonable behaviour and non-cooperation such as repeated disregard of hospital visiting hours. • Any of the above linked to destruction of or damage to property.

2.7 **Work related violence** (Health and Safety Executive definition (Aug 2013)): "Any incident in which a person is abused, threatened or assaulted in circumstances relating to their work. This can include verbal abuse or threats as well as physical attacks."

2.8 **Lockdown** - the process of controlling movement and access, both entry and exit, of people (LSW employees, patients and visitors) around LSW occupied sites or buildings in response to an identified risk, threat or hazard that might impact upon the security of patients, employees and assets or the capacity of that facility to continue to operate (please refer to the separate Lockdown Policy on Intranet).

2.9 **Locked door** – this differs from access control systems (i.e. site security) and is the process for managing access and exit because of the increasing need to monitor the patient's movement to and from the ward / unit for their safety either through an assessed risk of harm to self, absconding or vulnerability in relation to inpatient areas, recovery units and certain CAMHS services (please refer to the separate Locked Door Policy on Intranet).

3 Duties and Responsibilities

3.1 The **LSW Board** has ultimate responsibility for ensuring that security policies, procedures and arrangements for monitoring LSW's security performance are implemented.

3.2 The **Chief Executive** not only has overall accountability for the development and maintenance of proactive security throughout LSW, but is also the Security Management Director (SMD) and is responsible for ensuring that any guidance as issued by NHS Protect is complied with.

3.3 The **Director of Finance & Deputy Chief Executive** is responsible for ensuring a sufficient budget for security projects, and for the provision of the Information Governance Strategy and Information Technology Security Policy.

3.4 The **Director of Professional Practice** is responsible for the security of patient healthcare records and data protection requirements.

3.5 **Directors** are responsible for disseminating and ensuring compliance with the Security Management Strategy and this policy within their areas of responsibility, and to ensure that employees are appropriately trained and supported.

3.6 **Locality Managers, Services Managers, Heads of Service, Matrons, Ward, Departmental and Team Managers** – all grades of managers have a specific duty to promote protective security by:

a) Implementing the Security Management Policy and associated guidance throughout their areas of responsibility;
b) Developing local physical security measures (Appendix A), developing local protocols (Appendix B), promoting security awareness through training and listing security risks on local Risk Registers;
c) Ensuring employees, patients and visitors within areas of their remit are aware of their personal responsibilities, local security measures and requirements and are compliant with this policy;
d) Ensuring areas containing items of equipment which is expensive and / or attractive to thieves must be kept locked when not occupied;
e) Ensuring all security related risk assessments are recorded using the Incident Reporting System, Risk Registers & Assets (Safeguard), that appropriate action is taken commensurate with the risk, and that these are regularly monitored to reduce the risk of recurrence;
f) Ensuring all security related incidents are reported using the Incident Reporting System, Risk Registers & Assets (Safeguard), and that these are regularly monitored;
g) Ensuring employees attend security related training appropriate to their appointment, including refresher training;
h) Ensuring employees are provided with any support they require following an actual or potential incident, or ensuring that employees have access to such support.

3.7 The **Local Security Management Specialist (LSMS)** is accountable to the SMD has specific responsibility for implementing the Security Management Policy in line with NHS Protect guidance, and will:
a) Ensure that all security incidents are reported immediately to themselves, the Police, the SMD and/or the Counter Fraud Security Management Specialist (CFSMS);
b) Analyse security incidents in a consistent manner to identify trends, draw conclusions and make recommendations;
c) Regularly review risk registers to ensure that local risks are effectively managed by being accepted, treated or transferred;
d) Develop, in consultation with the SMD, an annual written work plan;
e) Ensure the SMD is kept informed of security management;
f) Apply sanctions by one or more of a combination of civil, criminal, disciplinary and procedural measures. They may include seeking redress through the

criminal and civil justice systems against those who actions lead to the loss of LSW assets and resources;

g) Assess security technology and its application;

h) Prepare and make available to all employees and managers information related to this policy, actively promoting security management issues ensuring a pro-security culture is developed and maintained;

i) Investigate breaches, or suspected breaches, of security, keeping full and accurate records;

j) Attend and report to the Health, Safety & Security Committee, the Audit Committee and annually to the LSW Board;

k) Liaise with the relevant service managers re local security procedures ensuring compliance with this policy;

l) Liaise with NHS Protect, Police Services, Crown Prosecution Service (CPS) and any other relevant external agencies, as appropriate;

m) Develop a continual programme of evaluated formal and informal security awareness training through inductions, briefings, updates and “bespoke” sessions to ensure that all employees, irrespective of status and profession, are aware of the risks;

n) Ensure victims are supported;

o) Support managers to undertake local security risk surveys, assessments and to implement appropriate recommendations.

3.8 **Employees and Contractors** are responsible for:

a) Positively assisting in the implementation of and being responsible for compliance with the Security Management Policy, security procedures and arrangements;

b) Collectively be responsible for the security and the prevention of theft of their personal property, property issued to them by LSW in relation to their employment, and LSW property in general; recognising the need to maintain a high degree of vigilance and not prejudice their own safety, safety of patients, relatives, visitors and the security of property or assets due to acts of negligence or carelessness;

c) Promoting and maintaining security at all times by being involved in crime prevention and security measures, anticipating risks and taking action to remove, reduce or transfer them, and receive training on these issues commensurate with their role(s), including refresher training;

d) Reporting all incidents of criminal activity including assaults, theft, and criminal damage including those incidents to be of a suspicious nature to their appropriate manager and on the LSW’s Incident Reporting System, Risk Registers & Assets (Safeguard), and for co-operating with their manager when incidents are being investigated;

e) Wearing identity badges while in LSW occupied buildings; either the Identification Badge from the company for which they work, or a badge issued by LSW, except where a health and safety evaluation advises against wearing one.

4 Protective Security Arrangements

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

4.2 LSW will build a pro-security culture built on the principles of prevention, deterrence, detection, investigation, sanctions and redress and by taking an inclusive approach with all those involved, as fully detailed in the Security Management Strategy.

4.3 LSW has developed and implemented a number of policies which contribute to the delivery of the organisation's security management strategic aims, as identified in the "Associated Documentation" section of the Reader Information on page 3 of this policy.

4.4 **Risk Management** is a key element to LSW's approach to security. Risk management techniques are concerned with harnessing the information and experience of individuals within LSW (and external expertise as appropriate) and translating that, with their help, into positive action which will reduce risks.

4.5 **Security Risk Assessments** – It will primarily be the responsibility of individual managers to ensure that the risk assessment process is applied to security, violence and the working environment for their areas of responsibility. Specialist and professional advice can be sought from the Risk Management Team to assist with this process. The identification, assessment and management of risks around security will be identified following:

a) Pro-active: site survey, an annual security and data protection audit;
b) Re-active: an incident/occurrence/issue raised by an employee/patient/visitor.

4.5.1 The risk should be recorded on the Incident Reporting System, Risk Registers & Assets (Safeguard) under the Risk module, and in accordance with the Risk Assessment Policy and Procedure. Managers are required to review the assessment periodically, but at least annually to ensure actions are addressed and followed up. Risk assessments will consider:

a) Identification of the employees groups at risk;
b) The working environment;
c) The location;
d) The time of day;
e) Lone working;
f) The suitability, competence, physical capability and experience of the employees;
g) The nature of the work activity (i.e. drug administration, delivery of unwelcome news);
h) The likelihood of an increased risk of violence due to factors (i.e. substance misuse, mental illness, personality disorder, previous history of violence, etc.);

i) The amount and nature of support available to employees.

4.5.2 The LSMS will develop an annual work plan to include the supporting of managers to produce proactive security risk assessment of LSW premises and assets. Each assessment will be summarised in a report which will be shared with the relevant Locality Manager and reported to the Health, Safety & Security Committee.

4.5.3 LSW is responsible for ensuring any new premises or assets that are commissioned be risk assessed prior to operational use of them, in line with this policy.

4.5.4 The Health, Safety and Security Committee meets bi-monthly and its members represent all areas of the LSW's operations and all Union Safety Representatives. The Devon & Cornwall Constabulary provide an officer to advise the Committee on security matters, ensuring a closer working relationship in order to develop and implement local crime and disorder strategies. The Committee monitors security incidents and any actions arising from risk assessments and ensures that appropriate measures are put in place to reduce risks. It also reviews any yellow or red card issued in accordance with the Violence and Aggression Policy.

5 Security Incident Process

5.1 LSW's ability to prevent or investigate crime is dependent to a significant extent on the prompt reporting of security incidents, and "near misses". The reporting mechanism that employees will be required to follow is outlined below:

a) All security incidents must immediately be brought to the attention of the employee's manager, the appropriate Locality Manager or the On-Call Manager / Director;
b) Full details of breaches of security must subsequently be reported to the LSMS using LSW's online the Incident Reporting System, Risk Registers & Assets (Safeguard);
c) Any breach of security that seriously endangers patients, visitors or employees must be reported to the relevant Locality Manager, as per the Serious Incident Requiring Investigation (SIRI) Policy (on Intranet).
d) Sightings of persons acting suspiciously within LSW should immediately be reported to the relevant Service / Ward / Unit manager and then the Police, as necessary.

5.2 In any area where employees feel threatened or believe they are witnessing a criminal activity, they should contact the local Police directly:

a) The contact number is **101** for non-urgent calls.
b) In an **emergency dial 999.**

5.3 The LSMS has direct access to all incidents, including violent and aggression, theft, damage to property / equipment / premises and all other security incidents which may result in prosecution.

5.4 The LSMS will use incident reports and other information to inform the requirement for more detailed security risk assessments, sources of information include:

a) Daily review of incidents.
b) Reviews of Risk Registers.
c) Reviews of lone working device usage reports.
d) Formal surveys, inspections and audits.
e) Investigation into breaches of security.
f) Information and guidance from NHS Protect.
g) National and local legislation and policies affecting security management.

5.5 Action plans derived from reactive risk assessments will be developed and monitored.

5.6 Reports to NHS Protect will be made by the Risk Management Team through the Physical Assaults Records (PARS) system.

5.7 The LSMS will ensure that all incidents of physical and non-physical violence are investigated in line with relevant legislation and as outlined in NHS Protect's guidance and training, including root cause analysis techniques.

5.8 Refer to the Violence and Aggression Management Policy for details regarding investigation of physical and non-physical assault.

5.9 **Police Investigations** - for all security related crime, the Police should be informed (see section 5.2 above for contact numbers) and they will decide whether the case merits a primary investigation by them (the Police log number should be recorded on the incident form). If the Police do initiate an investigation they will require the following information from LSW (refer the Police seeking this information to the Data Protection Service under Section 29(3) of the Data Protection Act):

a) Did the perpetrator have capacity to understand their actions?
b) Is the perpetrator fit to be interviewed?
c) Is the perpetrator fit to plead?

5.9.1 Such information should be sought from the responsible clinician and the LSMS should facilitate the gathering of such information, but where the appropriate clinician is unable to provide this information, the LSMS shall refer the case to LSW's Medical Director, as the organisation's Caldicott Guardian, for further guidance and direction.

5.9.2. Where the Police decline to investigate an incident under these circumstances the LSMS may refer the case to the SMD or NHS Protect for further guidance and direction.

5.9.3 All Police investigations shall be undertaken in line with statutory directions issued through the Police and Criminal Evidence Act (PACE) 1984. The LSMS shall be the nominate LSW contact with the Police during such investigations and shall also provide, where appropriate, support and professional guidance to all employees or persons involved with such investigation.

5.10 For all security related incidents, irrespective of whether the Police may be pursuing sanctions against the offenders, the LSMS will conduct an investigation to establish the causes of the incident and whether any further actions need to be taken. It is essential that where lessons can be learnt that they are fed into revisions of procedures / systems / risk assessments locally to ensure that employees are provided with the best possible protection.

5.11 LSW will consider a range of sanctions that can be taken against individuals (or groups) who abuse employees of LSW, or who steal or inflict damage on its property/assets. These include withdrawal of care to the pursuit of criminal prosecution, anti-social behaviour orders or civil injunctions. The nature of the sanction will be determined by the nature of the security incident. All sanctions must first have the approval of the SMD, and will subsequently be reported to the next meeting of the Risk Moderation & Monitoring Group (RMMG).

5.12 Incidents involving assaults on employees, theft of, or damage to LSW occupied property/ assets have a direct impact on both the human and financial resources of LSW. This policy will enable LSW to identify resources lost as a direct result of a security incident, providing the necessary information and evidence to attempt to recover that loss, whether through the criminal courts, by way of compensation, or seeking redress through the civil courts.

6 Security Planning

6.1 Security planning is reliant on general principles, involving:

a) Analysis of security risk assessment;
b) Cost effective deployment of protective security measures and sensible recommendations;
c) Early consultation in refurbishment projects to determine physical security measures;
d) Pro-active security management, including personal security (refer to the Lone Working and Violence & Aggression policies).

6.2 **Access Control Systems** – this differs from managed access and exit in relation to assessed patient safety. Where access control systems are utilised on LSW occupied premises, it shall be the responsibility of the designated manager of the ward, unit or department to ensure that local procedures are in place to ensure correct procedures and working practices are adopted for the use and management of such systems. The following information shall provide guidance, direction and best practice to be adopted by employees where access control systems are utilised:

a) Doors that are designated access control points (i.e. air lock door entry into restricted area) should be kept closed at all times and should never, for any reason, be propped open.
b) Keys or access control proximity/swipe cards that have been allocated to an individual employee should never be lent to, or used by another person.
c) Employees should always be aware of, and safeguard against potential unauthorised access into restricted areas and not allow unauthorised persons attempting to tailgate through access control points into such areas.
d) Premises and individual departments vacated for any length of time must be secured to restrict any form of unauthorised entry.
e) Combinations for key pad control locks should never be given to unauthorised persons and should be changed at least twice a year.
f) All access control points should be checked on a regular basis to ensure that they are working correctly and are properly secure.

6.3 **Control of Keys/Access Fobs** - where keys/fobs are utilised by employees to control access into restricted areas the following guidance shall be applied:

a) The issuing, recovery, recording and security of keys/fobs is the responsibility of ward/unit/departmental managers;
b) Employees should be aware of all local procedures relating to their area of work for the issue, security and use of keys/fobs;
c) Duplicate keys must be available in a designated secure place for use in the event of an emergency; registered / signed in and out accordingly;
d) Keys should not be able to be identified easily and should not be tagged with the name of ward/department/unit to which they belong (i.e. colour coding is a secure method of identification providing the explanatory chart is stored separately from the keys themselves);
e) Managers should keep a list of keys/fobs issued to employees and should ensure that they are returned prior to employees leaving; leaving employees to be advised by their manager that they will be charged a replacement key fee for failure to return their key;
f) Managers need to consider whether to replace locks if keys are not returned; the fee for this will be from local budgets;
g) Managers to ensure that fobs are deactivated when an employee leaves LSW;
h) Where keys/fobs are issued to contractors for access, a record should be kept. This should include details of the company, the individual, the date and time of issue and return;
i) Key boxes should be kept locked at all times when not in use and the issue and return of keys must be recorded;
j) An initial issue of keys will be made for locks on the acquisition of new premises to cover employee requirements. New keys will only be supplied by the Estates Department when locks are found to be defective or exchanged; other replacements will have to be funded by the ward/department if payment not secured from the employee leaving;

6.4 Employee and Visitor Identification

6.4.1 **Employee Identification**:

a) Whilst on LSW occupied premises, all employees will have available on their person, at all times, a valid LSW identification badge;
b) Identification badges will bear the organisation's name, the individual's name and designation and photographic likeness of the employee;
c) Lost or damaged cards must be reported to the employee's line manager immediately and a replacement sought without delay;
d) Identification badges must be surrendered to the employee's line manager on leaving the employment of LSW;
e) Individual managers who employ or allow temporary workers, volunteers or contractors on their premises shall ensure that these persons are bona-fide and if these persons are working within the area for a considerable period of time consideration should be given to issuing them with a LSW identification badge.

6.4.2 **Visitor Identification**:

a) Where appropriate, individual wards/departments/units shall be encouraged to operate a visitor recording system that requires all visitors to LSW occupied premises to sign in and out of such premises;

b) Visitor recording systems may vary between sites and areas but all should record similar information that will include the visitor's name, the date and time, the purpose of their visit and the registration of any vehicle parked on the premises;

c) Visitor recording systems will include reference to essential safety information that must be brought to the attention of the visitor on their arrival, (i.e. action to be taken in event of fire or other emergency).

7 Security of LSW Occupied Premises

7.1 Damage to and the loss of property owned by or occupied by LSW can have serious financial and operational consequences. All employees will make every effort to protect all property. All criminally damaged property will be reported to the Police and reported using LSW's Incident Reporting System, Risk Registers & Assets (Safeguard) on Intranet.

7.2 **Work area security** - a security survey / risk assessments should be completed for each service / unit / ward / work area. The LSMS will assist with undertaking any such security survey and risk assessments.

7.2.1 Whilst all employees are responsible for security of the building when leaving a work area unoccupied at any time of the day. If an investigation can prove that a breach of security has occurred as a result of this principle not being followed, disciplinary procedures may be a consequence, therefore, teams shall apply the principle of "last one out; check" in respect of:

a) Closing curtains and blinds;
b) Closing / locking windows and doors;
c) Switching off electrical appliances at the socket and unplugging, as appropriate;
d) Ensuring personal belongings are secure;
e) Locking away all patient records and portable equipment such as laptop, ThinkPad computers and calculators;
f) Ensure alarms are set and external doors are locked if applicable to the building;
g) Checking external lighting and reporting any lights that are not working to the Estates Department and service / ward / unit manager.

8 Alarms

8.1 **Security Alarm Systems** (burglar alarms) – security alarm systems that are properly selected, correctly installed and properly monitored can help to prevent losses of property through criminal activity and provide better personal protection for employees and patients. It should, however, be recognised that an alarm system can only monitor areas for breaches in security and will not protect premises, objects or personnel by themselves. To offer protection, an effective response to the alarm activation is essential.

8.1.2 Where security alarm systems are utilised on LSW occupied premises is shall be the responsibility of the designated Manager of the unit / ward / department to ensure that local protocols are in place to ensure correct procedures and working practices are adopted for the use and management of such systems.

8.1.3 All employees who are required to use these systems during the course of their work should be given the relevant training and guidance to ensure that they are utilised in the correct manner.

8.2 **Panic Alarm Systems**

a) In all high risk inpatient areas, employees will have the use of an effective panic alarm system. The requirement for a system will be made following a suitable risk assessment of the area by service manager;
b) In line with The Provision and Use of Work Equipment Regulations 1992, it will be suitably and sufficient maintained;
c) It is recommended that, as a minimum, weekly panic alarm checks are made to ensure the continuous efficiency of the system;
d) All managers must ensure that all employees receives an appropriate level of training in its use which is documented and regularly updated;
e) It is true to say that the use of a panic alarm system is only as good as the procedure which backs it up. On this basis, managers must ensure that robust local procedures exist in terms of action to be taken in the event of activation and individual roles and responsibility;
f) A system for monitoring the effectiveness of the procedure must be included in any local procedure;

g) A post-incident analysis following alarm activation or failure to activate can provide valuable information in order that lessons can be learnt to improve procedures.

8.3 **Personal Alarms** – in areas not covered by integral panel alarm systems, employees may feel access to a personal attack alarm is beneficial. Lone working risk assessments undertaken by service managers will highlight if and where a personal alarm should be issued to employees. LSW are currently employing MySOS devices from Skyguard (please refer to the Lone Working Policy on Intranet).

9 Safety of LSW Employees and their Personal Effects

9.1 **If any employee feels threatened by any person and/or experiences a state of fear, they must raise the alarm and summon assistance immediately, as determined by local policy or procedure.**

9.2 **Employees** have a legal **obligation** to cooperate with management to achieve the aims of this policy, to familiarise themselves with:

a) Any special security arrangements relating to their place of work or work practice, which may include any one or more of the following:

- Fixed panic/emergency alarms within bespoke LSW occupied buildings.
- Employment of bespoken security assistance from Securi-Guard.
- Mobile telephone.
- Lone working devices.
- Training in Conflict Resolution and Breakaway.
- Secure entry system and signing in/out system.
- CCTV.
- Employee support system.
- Working in pairs.

b) Taking the appropriate action in the event of a security related incident, or near miss, in order to comply with this policy, which include but are not limited to:

- Violence and aggression.
- Threats of violence and aggression.
- Absconding.
- Theft.
- Damage to property.
- Suspicious persons on-site.
- Unsecure areas.
- Physical assault; clinical or non-clinical.

c) Local arrangements to protect and safe keep their private property. Any loss of private property must be reported on the Incident Reporting System, Risk Registers

& Assets (Safeguard) as an incident; if it has been stolen, it is the responsibility of the employee to inform the Police, although LSW will support the employee affected and request that whenever the Police have been contacted the appropriate manager is informed as soon as is practicable;

d) Safeguarding themselves, colleagues, visitors, patients so far as is reasonably practicable and ensure that neither equipment nor property are put in jeopardy by their actions, either by instruction, example or behaviour;

e) The use of **identification badges** (ID) (see section 6 above), including any security equipment issued such as ID badges, keys, access cards and personal alarms, lone working devices are safely stored, appropriately used and reserved specifically for their use only.

9.3 **Use of Securi-Guard** – LSW has a contract with Securi-Guard where there is the potential for a breach in security or employee safety, when a planned outpatient client appointment has been made on LSW occupied premises, the service manager is encouraged to discuss security concerns with the LSMS with at least 24 hours' notice, in order to ascertain whether the presence of Securi-Guard ought to be employed to provide an accompanied patient service. Once agreed, booking of Securi-Guard is through the LSMS (via the Risk Management office).

9.4 **Lone Working** – great emphasis is placed on the importance of the cooperation of all employees in observing security and combating crime and ensuring their own and colleagues' safety, in accordance with the Lone Working Policy (on Intranet), as it applies to them. It is crucial, therefore, that appropriate risk assessments are undertaken for those employees who work in potentially high risk areas, i.e. community mental health and learning disability teams, and appropriately communicated to those regarding the controls around identified risks.

9.5 **Hostage Incidents** (refer to the Lockdown Policy on Intranet) - whilst it is accepted that a hostage situation would, in normal circumstances, be easy to identify in a location where a number of employees routinely work (i.e. inpatient settings), it would be difficult to identify that a hostage situation has arisen during a home visit or in premises where employees are working alone. For this reason, it is the responsibility of all managers to ensure that robust local lone working procedures are in place that identify the whereabouts of employees, and that it is included within local security protocols. If any employee (especially lone workers) has been identified as being "missing" during the course of their work and concerns have been raised about their safety then this fact should also be reported to the Police.

9.6 **Firearms and Weapons** (refer to the Lockdown Policy on Intranet) - whilst it is rare, incidents involving firearms or offensive weapons may occur in both the community or in LSW occupied buildings, therefore, employees should be aware of the risks of becoming involved in such an incident. It should be recognised that each incident has the potential to cause alarm, distress or fear and be extremely serious. Such incidents are more likely to occur in the community due to lone working arrangements.

9.7 **Violence and Aggression** – LSW recognises the problem of violence and aggression to employees as a major priority. LSW is committed to reducing incidences of this nature and supports the prosecution of persons who commit acts of violence and/or aggression against employees or other persons delivering services on behalf of the organisation. This will include criminal prosecution, private criminal prosecution and civil prosecution. Where prosecution is not appropriate, other sanctions will be considered. Procedures as to risk assessment and for dealing with incidents of this nature can be found in the Violence & Aggression Management Policy (on Intranet);

9.8 Dangerous Animals - if LSW employees are exposed to dangerous or uncontrolled animals in the course of their duties the same approach will be taken as that to physical and non-physical assault. LSW considers it to be the responsibility of the patient or the patient's family or carers to remove all risks to employees arising from their animals. The risk from animals should be assessed during the pre-visit assessment (refer to Appendix A of Violence & Aggression Management Policy on Intranet re the Workplace Violence Assessment Checklist).

9.9 **Suspicious Objects, Packages or Bomb Threats** - refer to the Major Incident Plan (on Intranet); Annex O – Responding to Suspect Packages, and Annex P – Responding to Bomb Threats.

9.10 **Prevent and The Channel Process** - Prevent is part of the Government's counter-terrorism strategy CONTEST, which is led by the Home Office. The health sector has a non-enforcement approach to Prevent and focuses on support for vulnerable individuals and healthcare organisations in helping stop them becoming terrorists or supporting terrorism – refer to Section 7 of the Risk Management Strategy or to the Major Incident Plan (Intranet) for more details regarding possible terrorist threats.

10 Locked Doors - refer to the Locked Door Policy (on Intranet).

11 Lockdown Procedures - refer to the Lockdown Policy (on Intranet).

12 Children Security

12.1 The provision of a safe and secure environment is recognised by LSW as a statutory requirement of health and safety legislation and in compliance with NHS Protect guidance. Services are responsible for carrying out suitable and sufficient risk assessments and, where required, develop local policies, protocols and procedures bringing them to the attention of all stakeholders (please refer to the separate AWOL & Missing Person Policy on Intranet).

13 Drugs and Medicine Security

13.1 LSW has established practices to ensure that FP10 prescription pads, medicines and drugs are handled appropriately (see the Safe and Security Handling of

Medicines Policy on Intranet). It is the responsibility of the Pharmacy Manager and managers of clinical teams to ensure that appropriate and proportionate investigations are undertaken.

14 Finance Control

14.1 A pro-active approach is taken by LSW, with an internal audit programme generated by the Internal Audit Committee. The programme directs internal and external audit to ensure compliance with financial regulations and the effective operation of control systems.

14.2 **Cash Handling & Fraud** – procedures for the movement and transfer of cash are specific in the Cash and Cheques Handling Procedure on Intranet). Alleged or suspected irregular financial transactions and fraud will be reported to the Local Counter Fraud Specialist through the Director of Finance (see the Counter Fraud Policy & Guidance on Intranet).

14.3 **Asset Management** - (refer to the Medical Devices and Equipment Management Policy on Intranet) collectively, terms "property" and "assets" are used interchangeably to describe LSW-owned items. For the purposes of this guidance, we have chosen to focus our work on the following classes of goods:

- medical and non-medical equipment
- consumables
- supplies
- LSW employee personal issue equipment
- fixtures and fittings

14.4 **Patient Monies and Property** - the loss of a patient's monies and personal property can be particularly stressful, can affect treatment and may damage the reputation of individuals, wards and the LSW. Every effort will be made to safeguard patient monies and property, particularly that belonging to people who are vulnerable and lack of capacity. All lost property incidents should be reported in line with the Incident Reporting Policy (Safeguard) and investigated at ward/unit/department level (please refer to the Patients' Monies and Property Policy on Intranet). Loss of or damage to patient property is likely to be investigated.

15 Security of Information

15.1 **Human Resources and Health Records** – measures must be in place to ensure that the security, transmission and disposal of information meets current national and LSW data protection requirements (see Health and Corporate Record Management & Record Keeping Policy on Intranet).

15.2 **Information Security** – LSW has in place measures to ensure the security of information in line with Data Protection principles and the requirements of NHS Information Governance Toolkit (see Information Governance Strategy on Intranet).

16 Security of Transport

16.1 Drivers of LSW vehicles will take effective measures to prevent theft of and damage by locking the vehicle when not in use and ensuring that property is not left in view and a temptation of theft. Private vehicles on LSW occupied premises or in spaces leased to the organisation are parked at the owner's risk.

17 Employee Support

17.1 Immediate support for employees after any stressful incident has occurred is crucial; they may have been traumatised by the event both professionally and personally.

17.2 A manager will undertake this role and ensure that arrangements for any employees who may be injured are sent to an A&E Department at the nearest hospital, or to the Minor Injuries Unit, or to their GP immediately following the incident. Employees may also be referred to Staff Health & Wellbeing themselves or via their manager for further support / counselling. In all situations, the employee should be given the opportunity to withdraw from the vicinity and permitted to take reasonable time out.

17.3 As soon as practicable, a meeting should be organised, for the employees involved who may wish to be accompanied and their manager to discuss the incident freely and to ascertain what further support may be needed. If the incident involved a patient, at this meeting the risk assessment should be reviewed and an action plan implemented.

17.4 Within seven days, a formal debrief should take place (refer to Appendix B of Violence & Aggression Management Policy on Intranet re Debriefing Employees Checklist). Debrief should be an opportunity for all employees to reflect upon thoughts and feelings evoked by the incident, the teams current working practice, and whether any changes are necessary; risk assessments require reviewing to reflect learning.

17.5 This meeting will be conducted in a culture of non-blame and will be respectful of everyone's opinions and feelings. Throughout this process, management, team, union representative and peer support should always be offered.

17.6 In most cases line management supervision will meet an individual's needs, however all LSW employees have access to counselling services via referral to Staff Health and Wellbeing.

17.7 Managers are responsible for ensuring that security related risk assessments are updated and communicated to those who need to know; appropriate feedback to their teams is required.

17.8 Support can also be requested from the Training and Development Advisors for Conflict Resolution within the Professional Training and Development Team.

18 Training

18.1 Training required by employees will vary from site-to-site and will be provided through the local induction programme and, where appropriate, site specific training will be arranged by service managers (i.e. use of local panic alert systems).

18.2 Conflict Resolution training is mandatory and available to non-clinical employees in high risk areas on a bi-annual basis and to clinical employees on an annual basis; Breakaway should be considered as "essential" training for other groups of employees, with an annual refresher.

18.3 In mental health and learning disability services, service users may exhibit more challenging behaviour directed at employees or other services users. Physical Intervention training for these high risk areas will be mandatory for clinical employees and provided three-yearly, with an annual refresher. The training will enable employees to develop the skills they need to ensure the safety of themselves and service users. This includes the recognition of triggers; de-escalation techniques where situations do arise and the appropriate response to incidents of violence and aggression in the workplace.

18.4 In accordance with the Appraisal and Management Supervision Policy on Intranet, managers are required to forward a copy of the training needs analysis to the Professional Training & Development Department. It is recommended, although optional, that a local record of all training, formal and informal, be held (i.e. training matrix) in addition to the electronic staff record (ESR).

19 Maintaining Services to Patients (Business Continuity)

19.1 If the perpetrator of a violent incident is a patient or associate of a patient requiring further care from LSW employees, arrangements must be made by the responsible Locality/Service Manager to provide this without any further risk to employees. This action will include:

a) Informing all parties of the Security Management Policy;
b) Ensuring that other LSW employees who may come into contact with the perpetrator of a security-related incident are made aware of the possibility of further incidents and of the steps being taken to prevent this;
c) Making arrangements for employees to be protected; this may include visits being made by employees working in pairs, clinic appointments at specific times of the day, clinic appointments in the presence of a security officer or other such steps.

20 Monitoring and Review

20.1 LSW will monitor and review this policy in partnership to ensure that we are achieving the aims of the policy. We will do this with trade unions / professional organisations and safety representatives. The review processes will include:

a) Service / unit / ward managers collecting and monitoring all reported incidents.
b) The Health, Safety and Security Committee conducting quarterly reviews of local incident statistics and safety improvement measures which have been introduced.
c) The Health, Safety and Security Committee reviewing LSW's incident statistics and Red / Yellow Card Issues every three months.
d) The Health, Safety & Security Committee reporting to the Safety & Quality & Performance Committee quarterly on how the organisation is following the policy, the outcomes of risk assessment and details of training provided.
e) Annual reporting to LSW Board to highlight progress in reducing risk and incidents and making recommendations for the forthcoming year.

20.2 Local statistics and incident reports are reviewed regularly by Service Managers at Locality Meetings, the Health, Safety and Security Committee and the more high risk incidents and associated risk assessments are reviewed by the Risk Moderation & Monitoring Group (RMMG) and Safety & Quality & Performance Committee / LSW Board as appropriate, thus ensuring appropriate monitoring of the effectiveness of this policy and associated local protocols.

All policies are required to be electronically signed by the Lead Director. Proof of the electronic signature is stored in the policies database.

The Lead Director approves this document and any attached appendices. For operational policies this will be the Locality Manager.

The Executive signature is subject to the understanding that the policy owner has followed the organisation process for policy Ratification.

Signed: Director of Professional Practice Safety & Quality

Date: 27 April 2015

Security Risk Assessment / Profile

Premises Address	
Assessor	
Date	
Review Date	

Policies	✓	✗	N/A	Comments/Actions
Are employees aware of:				
Security Management Strategy				
Security Management Policy				
Lone Working Policy				
Violence & Aggression Management Policy				
Incident Reporting & Investigation Policy and Procedure				
Locked Door Policy				
Lockdown Policy				
AWOL & Missing Person Policy				
Use of Personal & LSW Vehicles for Work Purposes Policy				
Are employees briefed on the above policies and local procedures? If so, how often and how evidenced?				
Are employees aware of local procedures for:				
Securing and opening LSW occupied premises				
Security of LSW property				
Are employees aware of the procedure to follow when an actual or potential incident occurs				

(including whom to call for help?)				
Have all employees been trained to report incidents online?				
If panic alarms are in place, either fixed or personal, are employees aware of actions to take when the alarm sounds?				
Does local practice ensure that people known to be violent / aggressive are identified? Is this covered by a local procedure?				
Where appropriate following any incident, are amendments made to a risk assessment on the local Risk Register?				
Is there a local procedure in place for the handling of cash / valuables to ensure the minimum requirement to do so?				
If handling money / valuables is carried out regularly, is there a local system to ensure the security and propriety of the system?				
Are employees aware of the requirement to wear ID badges at all times whilst at work (where appropriate)?				
Employee Safety – Security and Support				
Have all employees attended Conflict Resolution Training?				
Have employees received Breakaway Training?				
Are all employees involved in any security related incident provided with appropriate and timely feedback?				
Are managers referring victims of violent / aggressive incidents to Staff Health & Wellbeing to support / counselling?				

Site Security Profile - perimeter	✓	✗	N/A	Comments/Actions
General description of location, plus access points				
Area in square feet				
Site characteristics – number of buildings on-site and whether it is a multi-occupancy site?				
General description of the site (landscape), shape and slope				
Does the site have a perimeter fence with gates / barrier?				
What type of fencing and state of repair is it in?				
Does the fencing prevent unauthorised access?				
Are the gates / barrier used to control access to the site during normal working hours?				
Are the gates secured at night?				
Is the site secure out-of-hours?				
Is there signage around the site warning against illegal access to the site?				
Description of types of roads and number of them on-site				
Description of bus routes, frequencies and their route(s) onto site?				
Direction and movement of traffic on-site?				
Describe neighbouring land usage (i.e. residential, industrial, farming, energy supplies)?				
Number of car parking facilities, where they are situated and how they are controlled:				
Number of buildings and how are they spread on-site?				
Identify the access and egress points (mark on site plan)				
Do employees have access to on-site parking?				
Is the car park maintained, secure and patrolled if on-site?				

Site Security Profile - External Lighting	✓	✘	N/A	Comments/Actions
Is there security lighting installed around the site – grounds and buildings)?				
Does the security lighting support CCTV – grounds and buildings?				
Is the level of security / street lighting adequate for the site?				
Are there any unit areas which cause concern?				
Are any of the security lights obstructed or damaged?				
Are movement sensors / PIR security lights fitted? If yes, for what purpose and where?				
How is security lighting date activated?				
How is security lighting controlled?				
Site Security Profile – General External Security	**✓**	**✘**	**N/A**	**Comments/Actions**
Is there any evidence of unauthorised use of the site (i.e. antisocial behaviour, graffiti, alcohol / drug abuse)?				
Is there a grounds maintenance programme in place for gardens, shrubs, trees, hedges, etc.?				
Building Security	**✓**	**✘**	**N/A**	**Comments/Actions**
Does the building have any areas which are not covered by security lights / CCTV that may be used for antisocial behaviour?				
Is the building fitted with a security alarm?				
If yes, is the alarm monitored by an approved alarm monitoring centre?				
Does the alarm company provide a key holder response to all alarm activation?				
How is the security alarm controlled? How is it activated?				
What is the building used for? Is it multi-occupancy? Is it an un-zoned area (i.e. restricted movement within the building)?				

What shape is the building and the size of it?				
How many levels does the building have (including basement) and advise what each level and area of the building is used for?				
What is the general description of the building?				
Is there a nominated person responsible for security and key holding, with a deputy in the event of alarm activation?				
Does the building have signage directing visitors of the main reception and/or public access points?				
Are all external doors fitted correctly, and do they open and shut as required (i.e. are they fit for purpose)?				
Are all doors fitted with appropriate locks which meet the minimum requires of being at least a 5-lever mortise or similar hook lock, fitted top and bottom?				
If the building is fitted with either a digital or electronic key pad as its main means of access, is there a back-up system in place in case of failure?				
In the case of key pads, are the codes changed on a regular basis? If yes, how often?				
Are doors which are not used as primary access and egress kept locked and alarmed?				
Are all windows securable and do they meet minimum security standards?				
Where appropriate, are window opening restrictors / limiters fitted to prevent access?				
Does the building have any flat roofs?				
Does the building have fire escapes to upper floors?				
Are there measures in place to restrict access to fire escapes from ground level?				

Is there a system to ensure that facilities that are broken / out of order are reported and attended to promptly (i.e. an Estates Log)?				
How many corridors does the building have? Do they interconnect and where do they lead?				
What is the number of access and egress points in each building and their location?				
Does air conditioning exist in all or part of the site / building? If so, where is it controlled (may be from more than one point)?				
Who is responsible for maintaining the air conditioning?				
How quickly can the air conditioning be turned off?				
Where is the power supply located and how is it supplied?				
Is the power supply secure from tampering? Is uninterrupted power supply available?				
Who owns the property? Is it NHS Property Services or private property that LSW occupy?				
If it is private property, can it be locked down?				
CCTV - Security	✓	✘	N/A	**Comments/Actions**
Is the perimeter / access points covered by CCTV?				
Where are the cameras located? Is there a map of their locations?				
Does the CCTV face any residential property?				
What are the CCTVs trained on?				
Is CCTV signage displayed around the site?				
Does the system provide external coverage?				
Does the system provide internal coverage?				
Are images recorded?				
Is CCTV monitored?				
Is there a maintenance contract in place for the system?				

Is the system registered with the Information Commissioner’s Office, and does it comply with the Data Protection Act?				
Access - Security	**✓**	**✘**	**N/A**	**Comments/Actions**
Is visitor access to the building / premises managed?				
Does the building have a manned reception?				
Is the receptionist a lone worker?				
If yes, does the receptionist have access to a panic button or a personal attack alarm?				
Is access to the building via an intercom?				
Does the intercom have a camera?				
Are visitors escorted to and from reception or access point?				
Are visitors required to book in, and are they issued with a security badge?				
Is reception / access point covered by CCTV?				
Additional comments:				

Appendix B

Local Security Protocol

Please complete the information below for each location where LSW services are provided. The information should be made available to all employees operating from this location.

Address:			
Responsibilities			
Manager: (NB: This should be the Locality / Service Manager; this person may be based elsewhere)			
Name:		Contact No:	
The above Manager shall be responsible for: • Producing robust local protocols in respect of security of the above premises, which should cover building security (site specific), personal and property security; see “Policies and Protocols” section below; • Security incident reporting.			
Deputy: (NB: This should be a manager, team leader, etc., who is based on-site at this location)			
Name:		Contact No:	
The above Deputy shall be responsible for ensuring: • All employees are aware of, and comply with, the protocols which relate to their work place; • Every security-related incident is appropriately reported and investigated in line with policy; • Risk assessments are carried out as appropriate.			
Employee Responsibilities			
Security is the responsibility of **all** employees, irrespective of their role within LSW, and they shall: • Understand their roles and responsibilities in respect of security of both the premises and their personal safety / property whilst at their place of work - “Policies and Protocols” section below; • Report all security-related incidents, no matter how minor: ➢ To their manager; ➢ On the online incident reporting system (Safeguard) via Intranet; ➢ To the LSW’s Local Security Management Specialist (via the Risk Management Team) and/or the Police, as appropriate.			
Policies and Protocols			
• Building and Premises Security (site specific) • Locking and unlocking premises and alarming (where appropriate) • Key holding responsibilities and the management of access control systems (i.e. fobs) • Visitors to premises • Security of LSW property and information • Monitoring and maintenance of CCTV systems (if applicable) (NB: the above procedures should be expanded to provide guidance to be adopted under each heading)			
Personal Safety and Security of Property			
• Lone working • Violence and aggression • Security of property ➢ LSW (i.e. laptop, ThinkPads, iPads, mobile telephones) ➢ Patient ➢ Personal (i.e. wallet, handbag and/or contents, car keys, etc.) (NB: the above procedures should be expanded to provide guidance to be adopted under each heading)			

NB: Local procedures / protocols should be produced in accordance with LSW’s Security Management Strategy / policies, and in consultation with LSW’s LSMS, where necessary. Local procedures do not require the approval of the Policy Ratification Group; simply an annual review.

Appendix C

Firearms & Weapons Guidance

Whilst it is rare, incidents involving firearms or offensive weapons may occur in both the community or in LSW occupied buildings. It is the overriding priority of LSW to ensure the safety and security of its employees and others. To this end, it is stressed from the outset that, where there are any concerns about the safety or security of any individual, the Police should be called immediately.

An “offensive weapon” is “any article which is made or adapted for use for causing injury to a person” i.e. knives, knuckledusters, rice flails, etc. Other household objects or tools may be classed as weapons depending on their design and the intent of the person carrying them, i.e. hammer, Stanley knife, washing up liquid bottle filled with acid. Firearms and gas sprays are termed ‘prohibited weapons’. Possession of a canister of CS gas, pepper spray or a stun gun is an offence under the Firearms Act. Employees should always assume firearms are loaded and functioning; contact the Police on every occasion.

The issue of searching individuals is dealt with at length in LSW’s Searching of Property or Person Policy on Intranet. Please contact your manager or the LSMS or for further advice on this issue.

The issue of the use and carrying of firearms and weapons is of national public concern. This guidance contains information relevant to all employees working in the community or inpatient settings and should be included in the local security procedures developed for each premises, and should be followed by LSW employees should they find themselves under threat from firearms or weapons:

Prevention & Deterrence

The best way to protect employees, patients and visitors is to deter individuals from attending LSW occupied premises with weapons. The organisation should also consider producing warning notices for display within premises:

Offensive Weapons

- Weapons of any kind are prohibited on LSW premises
- Any weapons found will be confiscated and will not be returned
- All weapons will be handed to the Police for disposal
- If you are suspected of possessing a weapon, you will be asked to surrender the item
- If you refuse to do so, you may be refused treatment and asked to leave
- If you are in possession of a weapon and refuse to surrender it, you may be refused treatment and will be asked to leave
- The Police will be called and given your personal details

Confiscation & Disposal

If anyone attends LSW occupied premises in possession of a weapon, NHS Protect advise confiscation. The individual should be advised of LSW's stance on security/weapons, shown any warning notices and advised that the Police will be contacted.
Where weapons are surrendered, they should be handled as little as possible before being passed to the Police for disposal. Any items should be placed in a bag or suitable container and locked away until the Police arrive.

Wherever possible, the Police will collect any item from the premises. If they are unable to attend, employees should contact the Police and advise them that an employee will transport the item to the local Police station. A written record of this journey should be made. Employees must also obtain a receipt from the Police once the item is in their possession. If the individual wishes for the return of their item, they should be advised to contact the Police. The Police are responsible for disposing of all offensive weapons.

Personal Safety

Your safety and the safety of others in the vicinity are a matter of priority and, where possible:

- Where the possession/use of a firearm is known or suspected the Police, Local Security Management Specialist (LSMS) and the immediate line managers should be informed without delay
- If the individual is actively threatening others, employees should consider evacuating the area until the person is calmer and it is safe for employees, or the Police, to approach. In an inpatient setting, ensure all appropriate steps are taken to treat the person if they require clinical assistance.
- Discreetly active any lone working device you have been issued with.
- Call the Police without putting yourself at risk.
- If you are unable to contact the Police yourself, as discreetly as possible attempt to raise the alarm to others in the vicinity.

Contacting the Police

- All incidents involving firearms or weapons are a matter for the Police and should be reported to them immediately by dialling 999 or 101 for non-urgent calls.
- The employee who calls the Police should give as much relevant information about the situation as possible, including:
  - ➢ The nature of firearm or weapon (i.e. rifle, knife, gas spray, etc.)
  - ➢ Who has (if name known) possession of the firearm or weapon
  - ➢ Description (if name not known) of the person who has possession of the firearm / weapon
  - ➢ Exact location of the incident and where the offender physically is within the vicinity
  - ➢ Whether any shots have been fired or weapons used
  - ➢ Any injured persons or potential imminent risk to personal safety or life

Before the Police Arrive

Whilst it is accepted that this may be extremely difficult or potentially dangerous, the following information will give employees guidance on how to deal with the situation:

- Make an immediate escape if safe to do so, but do not attempt it if it would compromise your safety;
- Stay as calm and composed as you can, engaging with the individual if appropriate.
- Do not say or do anything that is likely to escalate or enflame the situation
- Do not use force or attempt to disarm a person unless life or personal safety is in immediate danger
- If the incident is on LSW premises the Lockdown Procedure should be invoked
- A phased evacuation of the immediate and subsequent areas should be implemented where safe to do so, in line with the Lockdown Procedure on Intranet

Following Police Arrival at the Scene

On arrival, the Police will assume full command and control of the incident **without exception**. The following LSW employees should be on hand to assist the Police as appropriate:

• Relevant manager or On-Call Manager out-of-hours	• LSMS
• LSW Communications Manager	• Witness(es) to the incident

Record Keeping

Where a service user or ex-service user is involved in any incident relating to an offensive weapon employees shall:

- Record the incident via the online incident reporting system **or** complete Appendix A from the Serious Incident Requiring Investigation (SIRI), depending on severity – recording the Police Crime Number accordingly. In all circumstances, a written record of the events and actions taken, along with relevant details of those involved, should be made as soon as possible after an incident. This should be retained and given to the LSMS and, where appropriate, to the Police.
- Log a “Special Note” (formerly called “warning” on Epex) on SystmOne (contact SystmOne re any queries)
- Update Clinical Risk Assessment
- Update Clinical Risk History
- Update Clinical Care Plan

Confidentiality & Data Protection

LSW has a duty under the Crime & Disorder Act 1998 to consider the implications of crime and disorder when carrying out its statutory functions and to work together with responsible and co-operating bodies listed in the act. Reporting to the Police will inevitably mean a breach of confidentiality, particularly if patient personal details are involved. NHS Protect consider such a breach to be justified as being in the public interest, in accordance with the provisions of the Data Protection Act 1998 and the Human Rights Act 1998.