Security Policy (including The Prevention and Control of Violence & Aggression)

<table>
<thead>
<tr>
<th>CATEGORY:</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLASSIFICATION:</td>
<td>Governance</td>
</tr>
<tr>
<td>PURPOSE</td>
<td>To set out the principles and framework for the management of Security within the Trust, to ensure that all staff understand their roles and responsibilities.</td>
</tr>
<tr>
<td>Controlled Document Number:</td>
<td>146</td>
</tr>
<tr>
<td>Version Number:</td>
<td>6</td>
</tr>
<tr>
<td>Controlled Document Sponsor:</td>
<td>Director of Corporate Affairs</td>
</tr>
<tr>
<td>Controlled Document Lead:</td>
<td>Trust Security Management Specialist</td>
</tr>
<tr>
<td>Approved By:</td>
<td>Board of Directors</td>
</tr>
<tr>
<td>On:</td>
<td>28 July 2016</td>
</tr>
<tr>
<td>Review Date:</td>
<td>July 2019</td>
</tr>
<tr>
<td>Distribution:</td>
<td>• Essential Reading for: All Trust Staff</td>
</tr>
<tr>
<td></td>
<td>• Information for:</td>
</tr>
</tbody>
</table>

## Contents

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>13</td>
</tr>
<tr>
<td>8</td>
<td>13</td>
</tr>
</tbody>
</table>

### Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>15</td>
</tr>
</tbody>
</table>

Policy Statement
Scope
Framework
Duties
Implementation
Monitoring
References
Associated Policy and Procedural Documentation

Monitoring Matrix
1 Policy Statement

1.1 The Trust is committed to providing a safe and secure environment for patients, visitors, staff and all workers engaged within the Trust. In particular, the Trust will not tolerate harassment, violence and/or aggression without lawful justification or excuse.

1.2 The objective of this policy is to ensure that the Trust provides a secure and safe environment which minimises security risks to all patients, staff and visitors alike and also protects the property, assets, service delivery and the reputation of the Trust so that:

1.2.1 There is a safe and secure environment with regards to persons, functionality and physical assets;

1.2.2 There is a unified, structured and proactive approach to the management of security and violence and aggression within the Trust with all due consideration of legislative, regulatory and mandatory obligations; and

1.2.3 All persons are aware of their roles, responsibilities and obligations with regards to security matters;

2 Scope

2.1 For the purposes of security this policy applies to all Trust staff, including Contractors, Agency and Locum workers as well as those undertaking secondments whether they are involved in Trust business whilst on any property owned or controlled by the Trust or off Trust premises. Nominated managers must therefore ensure that any non-employed workers are aware of the requirements of this policy and the associated procedures and how to apply them.

2.2 The policy is applicable in all of the following circumstances:

2.2.1 Violence from staff towards, other staff, patients and visitors/public

2.2.2 Violence from Patients to staff, other patients and visitors/public

2.2.3 Violence from Visitors/public to staff, patients and other visitors/public

2.3 Definitions

Within the context of this policy the following definitions, taken from NHS Protect guidance, are used:

2.3.1 assault is described as `the intentional application of force against the person of another without lawful justification, resulting in physical injury or personal discomfort`; and
2.3.2 Verbal aggression is ‘the use of inappropriate words or behaviour causing distress and/or constituting harassment’.

3 Framework

3.1 This section describes the broad framework for the Security Policy. Detailed instructions are provided in the associated procedural documents.

3.2 The Director of Corporate Affairs shall approve all procedural documents associated with this policy, and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.

3.3 Security – General

In order to achieve a safe and secure environment for all, the Trust shall:

3.3.1 Ensure that risks are properly identified, assessed, and that appropriate mitigation measures are put into place (“Security Risk Assessments”) in accordance with the Security Procedure;

3.3.2 Make available appropriate resources to implement this policy effectively. The Trust’s security service for the main sites is provided by engie who have a dedicated security manager with overall responsibility for engie security staff;

3.3.3 Clearly set out the responsibilities of staff at all levels;

3.3.4 Provide guidance on how to manage security issues and incidents;

3.3.5 Monitor the effectiveness of such measures taken and to make any necessary amendments to policies and procedures;

3.3.6 Provide suitable support, advice and guidance to those involved and exposed to security incidents; and

3.3.7 Sustain positive relationships with other key stakeholders e.g. law enforcement organisations, neighbours, the National Counter Fraud and Security Management Service, the Health and Safety Executive and other regulatory bodies

3.4 Management of Violence and Aggression

For all incidents of violence and aggression the Trust will ensure, where appropriate, that:

3.4.1 potential triggers to violence and aggression are risk assessed as part of the security risk assessments;
3.4.2 reasonable measures to reduce the likelihood of violence and aggression are devised and implemented to address specific risks;

3.4.3 consideration is given to excluding patients/public who present an unacceptable risk in accordance with the Withholding Treatment Procedure;

3.4.4 specialist advice on appropriate control mechanisms will be provided by the Security Management Specialist and/or Health and Safety Adviser;

3.4.5 support is provided to any member of staff involved in an incident of violence or aggression;

3.5 Where staff are either violent and/or verbally aggressive the Trust’s Disciplinary Policy will be followed.

3.6 Where a patient is subject to violence and or verbal aggression from another patient and or a member of the public and it appears that there is a safeguarding risk the Trust’s Safeguarding Processes shall be adhered to.

3.7 All incidents of violence and aggression will be reported to the Trust Security Management Specialist and engie Security who will manage the incident. Police should be informed should a criminal offence be committed and all security involvement will be documented.

3.8 The instructions provided in the associated Security Procedure shall be followed.

3.9 Major Incidents and Serious Threats

3.9.1 The Trust Major Incident Plan may be implemented in the event of a major security incident. In such circumstances, this plan will supersede or enhance the security measures outlined within this policy and associated procedures.

3.9.2 Serious threats, including terrorist threats, to the Trust will be assessed and appropriate measures will be implemented commensurate with the nature and level of risk.

3.9.3 The implementation of general preventative measures will reflect the five national levels of threat, ranging from low (i.e. unlikely attack) to critical (i.e. expected imminent attack) and will include an increase in the frequency of engie Security’s preventative patrols in the event of a rise in the national threat level. The security patrols are to be recorded in the security log.

3.9.4 If the Trust is advised by the County Terrorism Security Advisors of a specific terrorist threat or other serious threat to the Trust or health
bodies generally, the Trust Security Management Specialist will inform engie Security and engie will assess the individual risk and put in place measures to counteract the risk.

3.10 **Lock-down**

A lock down procedure enables an entire building/site or parts of the building/site to be locked down in the event of a serious incident. The TSMS shall, in conjunction with engie Security where appropriate, ensure that a lock down procedure is in place. Lockdown can only be authorised by the Hospital On-Call Manager or the Major Incident Command Control Centre Manager. The Trust’s Lock Down Procedure provides full details of the lock down for each site.

3.11 **Management of Security Incidents**

3.11.1 The Trust will report any security incidents to engie and also report details of the incident on the Trust incident reporting system. The Trust and engie shall respond to all Security Incidents. The Trust shall monitor engie level and nature of response to ensure that it is appropriate to each particular security incident.

3.11.2 The incidents will be documented by engie and TSMS will be informed on a weekly basis or, in the event of a Major Incident, as soon as practicable.

3.12 **Security of Trust Assets**

3.12.1 All Managers are responsible for the safety and security of all Trust assets within their area of responsibility. This responsibility includes carrying out a local risk assessment and putting in place suitable security measures for when the equipment is in storage.

3.12.2 Equipment must not be removed from its intended point of use or safe storage without permission from a suitably authorised person.

3.13 **Identification Badges and Access Control Cards**

All Trust staff must display authorised Trust identity badges at all times when on duty. Routine stop-checks will be undertaken by engie security. All staff must comply with a request from security to show the officer identify badge.
3.14 **Key Management**

All Wards and Departments are responsible for implementing a safe and secure system for the management of keys that are issued for their use as part of local security procedures. engie will put in place a secure, robust and fully auditable system for the management and distribution of keys used by security, including master sets.

3.15 **Termination of Employment**

Upon termination of employment, Line Managers shall ensure that the individual returns all Trust assets which will include: all equipment, uniforms, ID badges, Access/Smartcards, keys and car parking permits. engie security office must be informed to ensure that all access control permissions are removed.

3.16 **Lone Working**

Nominated Managers shall be responsible for identifying any staff who are subject to lone working and completing a risk assessment. They will develop and agree suitable working practices, in accordance with the Trust Lone Worker guidelines including the consideration to the issue of `Reliance` lone worker alarms.

3.17 **Intellectual Property and Security of Information**

3.17.1 Staff are required to respect confidentiality of information and must adhere to the Trust’s Information Governance Policy.

3.17.2 It is the responsibility of all staff to ensure that information is kept secure.

3.17.3 Staff are required to comply with the Trust Information Security Processes.

3.18 **Security of Trust Vehicles**

3.18.1 All vehicles owned or leased by the Trust must only be used by authorised personnel and doors and windows locked when left unattended. Keys must be in the possession of the driver at all times.

3.18.2 All items contained within a vehicle must be appropriately stored and concealed from public view, so far as is reasonably practicable.

3.19 **Car Parking**

3.19.1 All vehicles parked on Trust property shall be at the owner’s risk and the Trust will not be held liable for any damage, however caused.
3.19.2 All drivers are required to abide by the terms and conditions that are contained within the Trust’s Traffic Management Policy

3.20 Waste and Hazardous Items

All waste including potentially hazardous items must be segregated, handled, contained, secured and stored in accordance with the Trust’s Waste Policy and its associated procedure.

3.21 Training

The Trust will ensure security and violence and aggression awareness training, including conflict resolution training, is provided in accordance with the Trust’s Training Catalogue (Training Needs Analysis).

4 Duties

4.1 Executive Director for Security Management

4.1.1 In accordance with the requirements of the Secretary of State for Health, The Director of Corporate Affairs has been appointed as the Trust’s Security Management Director (SMD). The post holder shall act on behalf of the Board of Directors as the named Director with overall responsibility for Security Management arrangements within the Trust.

4.1.2 They shall provide assurance to the Board of Directors on compliance with this policy and report any material failures of compliance or other security concerns including violence and aggression.

4.2 Deputy Director for Corporate Affairs

The Deputy Director of Corporate Affairs shall have responsibility for the planning and delivery of security management arrangements.

4.3 Trust Security Management Specialist

The Trust’s Security Management Specialist (TSMS) will be responsible for co-ordinating and delivering a professional operational security management service. In so doing, the post holder shall:

4.3.1 ensure that engie has completed a security risk assessment for all Trust sites;

4.3.2 ensure engie carry out the site security risk assessments;

4.3.3 Provide specialist support, advice and assistance in relation to all security and violence and aggression matters;
4.3.4 Develop and implement appropriate Trust-wide security policies and procedures;

4.3.5 Monitor and support the development of localised operational security procedures within all areas of the Trust;

4.3.6 Act as the main point of contact with the National Counter Fraud & Security Management Service, law enforcement agencies and other such organisations;

4.3.7 Monitor security equipment to ensure that it is functional and appropriately maintained;

4.3.8 Liaise with the Police where necessary and to provide information on identified perpetrators of violence and other crime;

4.3.9 Collate and analyse reported security incidents, identifying trends in the interventions required of security staff in respect to all security incidents including violent incidents; and

4.3.10 Advise on the availability and use of ‘Reliance’ lone worker alarms.

4.4 **Senior Divisional and Corporate Directors/Managers (Including Directors of Operations and Associate Directors of Nursing)**

Senior Divisional & Corporate Directors/Managers will be responsible for ensuring that this policy and associated practices, as well as local security procedures are developed, implemented and effectively managed within each of their areas of responsibility. They will ensure that each department under their control undertake a security risk assessment, including the potential for violence and aggression, implement controls where risks are identified and monitor these for effectiveness.

4.5 **Heads of Departments, Group Managers and Matrons and Nominated Managers**

All Heads of Departments, Group Managers and Matrons and Nominated Managers are responsible for:

4.5.1 ensuring local security procedures are in place;

4.5.2 undertaking a comprehensive departmental risk assessment and creating an environment and climate where violence is less likely;

4.5.3 ensuring that the Policy, the associated Procedures, guidelines and are made known and available to all their staff;

4.5.4 supporting any member of staff who has been involved in any security incident including violence and aggression;
4.5.5 ensuring that an online Datix Incident Report Form is completed for every security incident including violence and/or aggression and the Trust Security Management Specialist together with the Health and Safety team is informed; and

4.5.6 Prevention, control measures and monitoring arrangements are implemented;

4.5.7 All staff are made aware of their obligations and receive appropriate education, training and development.; and

4.6 **Ward/Departmental Managers and Supervisors**

Ward/Departmental Managers and Supervisors will be responsible for ensuring that Security policies, practices and procedures are complied with, which shall include:

4.6.1 Ensuring that local security procedures are adhered to and that all actual or potential breaches, acts of assault, violence or aggression are reported using the Trust incident reporting system and action plans devised as required;

4.6.2 ensuring that all security equipment is fully functional and reporting any faults to engie helpdesk;

4.6.3 Ensuring that all Trust assets, property and information are not left unattended and are correctly and securely stored at all times;

4.6.4 Ensuring that the department is kept secure and locked when unattended;

4.6.5 Ensure that all patients are made aware of the risks associated with bringing in large amounts of money or valuables into the Trust and where this responsibility is delegated to staff that the patient property guidelines are followed.

4.7 **All staff**

All staff are responsible for assisting and supporting in the provision of a secure and safe environment and to this aim they must:

4.7.1 Comply with this policy and associated procedures, including local security arrangements;

4.7.2 Maintain a high degree of vigilance and not undertake any actions that may compromise their own personal safety, or that of colleagues, patients or visitors;
4.7.3 Routinely assess potential and actual security risks and report any concerns to their Line Manager;

4.7.4 Attend relevant security training and awareness sessions;

4.7.5 Report any malfunctioning of security equipment at the earliest possible opportunity, using the engie helpdesk;

4.7.6 Not interfere with or misuse any security equipment, property or the environment as a whole;

4.7.7 Ensure that they wear an authorised Trust ID badge, in a visible position at all times;

4.7.8 Challenge any persons not known to them and not wearing an authorised Trust ID badge;

4.7.9 Ensure that Trust assets are not removed from their intended location without appropriate authorisation;

4.7.10 Ensure that their personal property is kept secure at all times;

4.7.11 Try to de-fuse violent/aggressive situations if they feel safe to do so and immediately summon assistance when aware of a potential or actual violent incident;

4.7.12 If involved in an incident either as a victim or when going to someone’s assistance, use the minimum of force necessary to control the violent person(s) bearing in mind the legal/medical constraints and personal responsibility to act within the law; and

4.7.13 Complete an online Datix Incident Report Form immediately following such an event or as soon as possible thereafter.

4.7.14 Compliance with this policy and associated procedures is mandatory and failure by any member of staff to comply with such requirements will result in consideration of the use of disciplinary action.

4.8 Trust Health, Safety and Environment Committee

The Trust Health Safety and Environment Committee regularly assesses and reviews security activity, trends, risks and issues across the Organisation as a whole. The Committee recommends the development of action plans by the TSMS with a view to mitigating or eradicating such risks. The Chair of the Committee reports to the Trust Board.
4.9 Divisional and Corporate Consultative Committees

4.9.1 The Divisional & Corporate Consultative Committees act as a local forum for reviewing local security activity, trends, risks and issues.

4.9.2 The Chair of each Committee report to the Trust Health, Safety and Environment Committee through the Directors of Operations and the Trust’s Security Management Specialist.

4.10 Security and Estates Management

Security and Estates Management is provided by engie The Manager of engie will ensure that:

4.10.1 All site security risk assessments are completed in accordance with their contract with the Trust;

4.10.2 A secure, robust and fully auditable system is established for the management and distribution of keys used by security, including master sets;

4.10.3 engie undertake lock and unlock procedures for designated Trust premises. This includes promptly attending and assessing premises where a breach of security has been reported;

4.10.4 A method statement outlining engie service provision is produced annually

4.10.5 Ensure that all security equipment is fully functional

4.10.6 Respond and assist with potential and actual security incidents, including acts of assault, violence and aggression;

4.10.7 provide continuous surveillance of security monitoring systems and undertake regular patrols (as defined within engie method statements) of Trust premises and grounds with a view to identifying potential risks and resolving any actual breaches of security; and

4.10.8 Investigate any breaches of security and report the finding to the Trust Security Management Specialist (TSMS)

5 Implementation

5.1 This policy will be implemented by all levels of management in the Trust and made available to all staff via the Trust intranet.

5.2 In addition, information on security issues will be provided to wards and departments by the TSMS to encourage a pro-security culture among staff.
5.3 The TSMS will provide advice, assistance and support on various security related matters

5.4 Security awareness will be included as part of Trust induction with additional training sessions made available to staff as required.

6 Monitoring

The standards to be achieved and the monitoring arrangements to ensure compliance are detailed at appendix A.

7 References


7.2 Health and Safety at work Act 1974

7.3 The Management of Health and Safety at Work Regulations 1999

7.4 The Corporate Manslaughter and Corporate Homicide Act 2007

7.5 The Civil Contingencies Act 2004

7.6 NHS Litigation Authority

7.7 The Management of Health and Safety at Work Regulations Working Alone in Safety (HSE) Publication

7.8 Data Protection Act 1998 (CCTV)

8 Associated Policy and Procedural Documentation

8.1 Withholding Treatment Procedure for Aggressive Patients

8.2 Lone Worker Guidelines

8.3 Security Procedure

8.4 Disciplinary Policy

8.5 Information Governance Policy

8.6 Traffic Management Policy

8.7 Major Incident Plan

8.8 Lock Down Procedure.
8.9 Trust Waste Policy

8.10 Training Catalogue (Training Needs Analysis)
## MONITORING OF IMPLEMENTATION

<table>
<thead>
<tr>
<th>Monitoring of secure environment</th>
<th>Monitoring Lead</th>
<th>Reported To Person/Group</th>
<th>Monitoring Process</th>
<th>Monitoring Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a) Duties</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Trust Security Management Specialist (TSMS)</strong> will ensure that:</td>
<td>TSMS</td>
<td>By exception to TSMD</td>
<td>TSMS</td>
<td></td>
</tr>
<tr>
<td>• engie has completed security risk assessments</td>
<td></td>
<td></td>
<td>• Monthly Audit of engie risk assessments (all risk assessments saved in evidence folder)</td>
<td>Weekly, monthly or annually (see monitoring process)</td>
</tr>
<tr>
<td>• Police is informed of identified perpetrators of crime</td>
<td></td>
<td></td>
<td>• Monthly meetings of TSMS with the police to discuss any security incidents (any necessary actions are followed up by email - email evidence available upon request)</td>
<td></td>
</tr>
<tr>
<td>• Security incident trends are detected</td>
<td></td>
<td></td>
<td>• Weekly meetings of TSMS with engie staff to discuss any security incidents (any necessary actions are followed up by email - email evidence available upon request)</td>
<td></td>
</tr>
<tr>
<td>• Departments (Nominated Managers) have completed their risk assessments and have local security procedures in place</td>
<td></td>
<td></td>
<td>• Annual check of departmental risk assessments and local procedures. Any updates are then fed into the central database</td>
<td></td>
</tr>
<tr>
<td><strong>Trust Health, Safety and Environment Committee</strong></td>
<td></td>
<td></td>
<td></td>
<td>Every quarter</td>
</tr>
<tr>
<td>• assesses and reviews security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>activity, trends, risks and issues across the Trust every quarter</strong></td>
<td></td>
<td>(quarterly)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>b) Risk assessments of physical security or premises and assets</strong></td>
<td><strong>engie carry out yearly risk assessments of premises</strong></td>
<td><strong>engie</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Departmental security risk assessment of assets</strong></td>
<td><strong>engie</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Risk assessment</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>engie</strong></td>
<td><strong>TSMS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Departments</strong></td>
<td><strong>TSMS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Yearly audits of engie, risk assessments of premises by TSMS saved electronically.</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>TSMS collates all departmental risk assessments of assets and feeds information into a Trust wide database (saved in evidence folder)</strong></td>
<td><strong>Annually</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>c) and d) Development and Following up of Actions Plans</strong></td>
<td><strong>TSMS develops and follows up any actions by email as immediate response is required. Datix is updated as and when required.</strong></td>
<td><strong>TSMS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>TSMS</strong></td>
<td><strong>TSMS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>TSMS reviews any outstanding actions on a weekly basis (email evidence available upon request).</strong></td>
<td><strong>Weekly</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>e) Overall compliance monitoring</strong></td>
<td>Monitoring of the Security service provided by engie</td>
<td><strong>TSMS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>PFI Performance Manager</strong></td>
<td><strong>PFI Performance Manager</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>engie send monthly reports containing security responses to incident reports to the TSMS. The TSMS then ensures compliance with the PFI security contract. Any event failures are reported to the PFI Performance Manager via email as an immediate response is required.</td>
<td><strong>Monthly</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring of Trust security incidents</td>
<td>TSMS</td>
<td>Trust Health, Safety and Environment Committee</td>
<td>The Trust Health, Safety and Environment Committee assesses and reviews security activity, trends, risks and issues across the Trust every quarter. These meetings are minuted.</td>
<td>Every quarter</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------</td>
<td>-----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Monitoring of all Trust security issues</td>
<td>TSMS</td>
<td>NHS Protect</td>
<td>TSMS reports all Trust security issues to NHS Protect.</td>
<td>Annually</td>
</tr>
</tbody>
</table>

**Monitoring of violence and aggression (including lone workers)**

#### a) Duties

**TSMS** will:
- Advise on availability and use of ‘Reliance’ Lone worker alarms.
- Monitor any trends in violence and aggression compared to other Trusts.

**Trust Health, Safety and Environment Committee** will:
- Consider completed security risk assessments (including violence and aggression) and agree action plans and appropriate control measures

**TSMS**
- Reports from Reliance to TSMS
- Violence and Aggression statistics submitted to NHS Protect by TSMS

**Trust Health, Safety and Environment Committee**
Minutes/Reports of meetings (quarterly)
to reduce risks to the lowest possible level.

| b) and c) Risk assessment for prevention and management of violence and aggression, including timescales |
|---|---|---|---|
| Risk assessments for the prevention and management of violence and aggression, including lone workers | Departments (Nominated Managers) | TSMS | TSMS collates all departmental risk assessments (including violence and aggression and lone workers) and feeds information into a Trust wide database (saved in evidence folder). |
| | | | Monthly |

| d) and e) Development and Following up of Action Plans |
|---|---|---|---|
| See above – duties – Trust Health, Safety and Environment Committee | | Mins of Trust Health, Safety and Environment Committee | Quarterly |
| Staff involved in incidents of violence will be provided with both psychological and practical support as required. | Occupational Health and Safety Department | Head of Health and Safety Department. | Records held by Health and Safety. |
| | | | Ad hoc |

| f) Arrangements for lone workers |
|---|---|---|---|
| The Trust ensures the safety of lone workers by giving them access to a bespoke alarm system | Reliance | TSMS | The TSMS receives a report from Reliance on the availability and use of lone workers alarms (see duties above) |
| | | | Monthly |

| g) Training |
|---|---|---|---|
| Training is delivered by the TSMS (in accordance with the TNA) | TSMS | Executive Director of Delivery | Compliance with training is monitored via the dashboard which provides live data. The TSMS will check the dashboard data on a monthly basis to check overall compliance by |
| | | | Monthly |
### h) Overall compliance

| TSMS will monitor any trends in violence and aggression compared to other Trusts (see duties). | TSMS | NHS Protect | TSMS will submit Violence and Aggression statistics to NHS Protect | Annually |