GOP05

GROUP SECURITY POLICY

1.0 Policy Statement

1.1 The Royal Wolverhampton NHS Trust and Walsall Healthcare NHS Trust (the Trusts) are committed to providing a safe place of work. This Policy is designed to introduce proactive procedures that will ensure, so far as is reasonably practicable, not only the health and safety of its staff but also welfare in terms of security. The Trusts are also committed to meeting its statutory duties regarding security, as well as NHS Guidance on security and Secretary of State Directives on NHS Security Management measures.

1.2 The aim of the Security policy is to implement local security management procedures and national guidance on how to achieve a secure environment that will protect:

- Patients
- Staff
- Visitors
- The physical assets of the organisation

1.3 Security can be defined as "a state of being where the risks to people and property are minimised from any actions that may lead to personal injury, threat to life or the disruption of the business activity of the Trust."

1.4 Security and Car Parking services at the Trusts are currently delivered by an outsourced service provider.

1.5 This policy applies to all Trust employees including bank staff, agency staff, students, apprentices, volunteers, and people carrying out work experience.

1.6 All contractors and sub-contractors employed either directly, or through agencies, will be bound to apply as far as is reasonably practicable to this policy.

2.0 Definitions

ANPR	Automatic Number Plate Recognition
BWVC	Body Worn Video Cameras
CCTV	Closed Circuit Television
CPSCC	Car Parking and Security Control Centre
HR	Human Recourses
LCFS	Local Counter Fraud Specialist
V and A	Violence and Aggression
Lockdown	Lockdown is the process of controlling the movement and access (both entry and exit) of people around a Trust site in response to an identified risk, threat or hazard that might impact upon the security of patients, staff and assets or, indeed, the capacity of that facility to continue to operate. A lockdown is achieved through a combination of physical security measures and the deployment of security personnel.

LSMS	Local Security Management Specialist
MOVA	Management of Violence and aggression.
Security	Security is defined as the state or feeling of being safe and protected.
Security breach	A security breach is defined as any offence against the Trust, its staff, patients, visitors, or volunteers. Examples of security breaches may include: physical or non-physical assaults, theft, harassment, criminal damage; failure to set alarms or to follow other security procedures; unauthorised access to restricted areas or confidential records etc.
ASBO	Anti-social behaviour order. A civil order issued to a named individual who has caused a disturbance.
Court injunction	A court order requiring a corporation or government entity to stop doing something and refrain from doing in the future.
Fixed penalty notice	A fixed penalty for low level environment crimes, e.g., parking
SIA licence	Nationally recognised, Licence required for all Security staff.

3.0 Accountabilities

3.1 Chief Operating Officer

The Chief Operating Officer has overall responsibility for controlling and co- ordinating security within the Trusts.

3.2 Trust Board

The Trust Board has a responsibility to consider the security strategy on a regular basis and be aware of its responsibilities and liability appertaining to security.

3.3 Divisional Manager, Estates & Facilities

Is responsible for monitoring and ensuring compliance with the directions set out by the Secretary of State on NHS Security Management.

3.4 Security Provider

Is responsible to the appointed Contract Manager for Car Parking and Security Services for the day-to-day operation of the Security Department, car parking systems and the Trust's CCTV system.

3.5 Managers

3.5.1 Trust Managers are responsible for ensuring that they, and their staff, comply with this Policy. They must ensure that their staff undertake any security training identified for their services and staff needs. Managers are to undertake annual security risk assessments of their own respective areas of responsibility. Risk Assessments should be carried out in accordance with Health and Safety Policy (refer section 4.3 and Attachment 1 for information on 'Security within Department' and 'Violence & Aggression' Risk Assessments respectively). Further advice and guidance may also be sought from the Trust Local Security Management Specialist (LSMS) or the Security

Management Team.

3.5.2 It the responsibility of Department managers to identify if there is a risk of V and A or lone working, to complete a Risk assessment and communicate to all staff.

3.5.3 Ensure the dissemination and implementation of the policy within the area of their responsibility by providing support and advice to their managers.

3.5.4 Coordinate security issues with other employers who share the site.

3.5.5 They must ensure that all breaches in security are reported via the Trust's incident reporting systems and inform the Security team of any serious or immediate issues. The security team if necessary, will also inform the Director of Finance and the Local Counter Fraud Specialist (LCFS) immediately if fraud is suspected. Please refer to the Anti-Fraud, Bribery and Corruption Policy.

3.5.6 Ensure that appropriate action is taken in respect of persons who are suspected of committing a criminal offence, misconduct or other breaches of security in contravention of the policies of the Trust.

3.5.7 Ensure that all staff are fully supported when making reports concerning violence, theft and damage or other security related incidents. Please refer to the Management of Violence & Aggression (MOVA) 'Recorded Verbal Warning, Yellow and Red Card Procedures' (Attachment 1).

3.5.8 Ensure that all staff wear their Trust ID badges at all times and return items prior to leaving (along with any keys) in line with Trust Uniform/Dress Policy.

3.5.9 Ensure that digital lock codes are changed on a periodic basis and that all relevant staff and Security Officers are aware of the new codes. Codes must be kept secret.

3.5.10 Provide any safety equipment as deemed necessary by risk assessment controls and mitigating actions.

3.6 Local Security Management Specialist (LSMS)

An LSMS is engaged by the Trusts. They must not undertake responsibility for, or be in any way engaged in, the counter fraud activities of any NHS body. The LSMS role will:

3.6.1 Provide support and guidance to clinical areas, obtaining one to one Patient Watch Security Officers when required. Where patients are deemed a significant clinical risk to themselves or others, staff should refer to the Enhanced Supervision Policy.

3.6.2 Provide advice to managers at all levels on security measures and dealing with violence.

3.6.3 Provide advice, support and guidance to managers implementing risk reduction measures and post-incident management.

3.6.4 Signpost Managers to training course options available for their staff from the Trust.

3.6.5 Report the Security performance and any concerns through to the Health and Safety Committee and Audit Committee.

3.6.6 Provide advice, support and guidance to departments for risk assessments in relation to violence.

3.6.7 Deliver conflict resolution training package to frontline member of staff.

3.6.8 Liaise with police for investigations.

3.6.9 Support staff through the court process.

3.6.10 Undertake appropriate risk assessments regarding the physical security of premises and assets when required.

3.6.11 Liaise with the Health and Safety team on issues relating to security and violence and will work in conjunction with the Head of Emergency Planning on issues relating to emergency planning/incident management.

3.7 Contracted Security and Car Parking Services

3.7.1 The Trusts expect the contractors to assignment instructions that include the following. These will be monitored monthly in the Security contract meeting.

- Protection against criminal activity, other hazards, and the preservation of good order within the Trusts.
- Working towards the protection of staff from physical and/or verbal assault.
- Working towards the prevention of the loss of patients, visitors and Trust property.
- Protection of Trust property against malicious acts, thefts, criminal damage, trespass, etc.
- Detect and report offenders suspected of committing offences against patients, visitors, staff, Trust or private property within Trust premises.
- Reporting of incidents and adverse events within the Trust incident reporting system.
- Maintain the reputation of the Trust.
- Detect and report offenders in line with the Reservations and Delegation of Powers and Standing Financial Instruction Policy and the contract agreed with the Trust.
- Advise and aid with all matters regarding security.
- Assist with crime prevention programmes and campaigns to raise the profile of security and highlight the need for constant vigilance in conjunction with the Police and LSMS.
- Provide a service to escort staff from their offices/departments/wards to other areas of the Trust and their vehicles, when necessary, especially out of office hours.
- Manage the car park and ID access database in accordance with Trust procedure.
- Provide out of hours response and support in any emergency situation e.g. fire.

3.8 Employees

3.8.1 Employees, including volunteers, are required to fully co-operate with this Policy and

to maintain a safe and secure environment. They must also follow any safe working procedures, risk assessments identified within their area to ensure good security at their place of work not only safeguarding their own well-being and property but also that of patients, visitors and all other users of Trust premises

3.8.2 Employees are responsible for always promoting and maintaining security by being involved in crime prevention and security measures, anticipating risks and taking action to remove, reduce or transfer them and receive adequate training on these issues.

3.8.3 Employees must report all incidents of criminal activity, including assaults, theft, fraud, and criminal damage, including those incidents to be of a suspicious nature to their appropriate Line Manager, Security Department or to the Police without delay. This must be reported in line with Trust incident reporting procedures.

3.8.4 All employees have a responsibility for completing mandatory and role specific training.

3.8.5 The Security Management Team will:

- Review the security arrangements for new builds, refurbishments, and upgrades within the Trust
- Develop and implement specific security related policies and guidelines
- Review security incident trends and action targeted improvement and support
- Support the development of Security and V&A risk assessments and oversee action plans for significant risks identified
- Comment on proposed changes to security arrangements across the Trust and receive security reports from the LSMS and report into the Health and safety Group

3.8.6 The Security Management Team will hold monthly Meeting Chaired by the LSMS, Divisional Manager of Estates & Facilities with the contractor providing the Security services to the Trust. The performance of the team will be reported to the Health and Safety Group for oversight and assurance on Trust compliance and for the purposes of consultation of documents, protocols and policies or escalation of issues through the Trust.

4.0 Policy Detail

4.1 NHS Violence Prevention Reduction Standards

4.1.1 The violence prevention and reduction standard provide a risk-based framework that supports a safe and secure working environment for NHS staff, safeguarding them against abuse, aggression, and violence. All NHS commissioners and all providers of NHS-funded services operating under the NHS Standard Contract should have regard to the violence prevention and reduction standard and are required to review their status against it and provide board assurance that they have been met it twice a year.

4.2 Secured by Design

The Trusts are committed to consider security requirements at the initial design and planning stages of projects for either new or refurbished buildings.

4.2.1 All capital and revenue projects involving changes to, or the introduction of, security

devices must be discussed with the Security Management Team prior to installation. The Security Management Team will seek advice from the Police Crime Prevention Design Advisor and/or the LSMS, who is also an accredited Crime Prevention Officer.

4.2.2 The Security Management Team will also advise the Trust on relevant Health Technical Memorandum's (HTMs) or other papers released regarding security in the NHS.

4.3 Security Risks to Premises and Assets (including Security within Department Risk Assessment)

4.3.1 All Risks associated with the physical/environmental "Security within Departments" must be assessed by the relevant Service Manager for their specific area, using the designated Health & Safety Risk Assessment Form – Risk Assessment Profile 2. Refer to MoVA Procedure and Lone Working Procedure below for information on respective risk assessments.

4.3.2 When assessing risks associated with *Security within Departments*, the following **hazards must be considered as a minimum:**

- Inadequate access control to departmental areas/location
- Unauthorised access to vulnerable patients
- Risk of patients leaving the department unnoticed (absconding)
- Tampering with clinical equipment or medications by unauthorised persons
- Theft of medical equipment or medications
- Theft of personal belongings

4.3.3 Control measures identified within the risk assessment must be developed and documented in line with **Group HS01 – Protocol 1 (Understanding the Trust Risk Assessment Process)**. Controls must be authoritative and SMART by describing the action that must be taken and by whom, ensuring they are specific, proportionate, and aimed at eliminating or minimising the risk associated with each identified hazard, in accordance with the hierarchy of risk control as noted in Group HS01 - Protocol 1.

4.3.4 The Service Manager must ensure that the findings of the risk assessment and associated control measures are **communicated to all staff within the service**. Evidence of communication must be retained for **audit and assurance purposes**. Where the residual risk rating (risk rating/level after current controls) remains **above 12** following the implementation of current control measures, the Trust risk management and escalation process must be followed, including consideration for inclusion on the risk register.

4.4 Disciplinary Action

4.4.1 Any act of violence against users of Trust premises and services, theft or misappropriation of Trust property by staff or other persons will be taken seriously. This includes to adhering to the principles of the Anti-Fraud and Bribery Policy. Advice will be sought from the Police, LSMS and/or LCFS as to whether criminal or civil action should be taken by the Trust

4.4.2 Any member of staff suspected or found to be guilty of misappropriating property or

committing security breaches will be subject to the procedures set out in the Disciplinary Policy.

4.5 Building Alarms

4.5.1 Building alarms are linked to Security; the department is manned 24 hours a day. Where a false alarm occurs due to a failure in a work system (i.e., failing to close windows at the end of day) an investigation will be conducted by the department and, if necessary, the appropriate action taken to ensure the same does not recur. The alarms will be reset by the Security Officers/Skanska, although there may be occasions when department managers are called out of hours to reset alarms.

4.6 Access Control, Identification Badges and Safe Hands Cards

4.7.1 All access codes to any part of the Trust external or internal premises must be treated with the utmost confidentiality. This means staff should not share codes to the Trust premises. If a member of staff forgets a specific code, they should contact their relevant Line Manager directly.

4.7.2 All staff, contractors and visitors must always wear Trust-issued identification badges whilst on Trust property.

4.7.3 Any lost ID badges must be reported to the Security Department. When staff leave the Trust's employment, they must return their ID badges which will then be cancelled by the ID card administrator as per Trust Uniform and Dress Policy. Not reporting the loss of an ID Badge may lead to disciplinary action.

4.7.4 All data relating to the Trusts ID card system will remain the property of ADT Fire & Security and Skanska. This data may be used for internal investigations as well as for the prevention and detection of crime.

4.7.5 Managers requiring data relating to the Trust ID card systems must submit their request to their relevant HR Divisional Manager/representative HR Manager copying in a Member of the Security Management Team. Once the request has been approved and the information requested is deemed adequate and relevant for the purposes required then the information will be released.

4.7 Lost and Missing Patients

4.7.1 The Trusts' Women and Children's Units incorporate numerous security systems to manage the risk of security breaches, including CCTV, baby tagging, and door access control arrangements. Exercises and risk assessments will develop a robust system to protect the maternity unit.

4.7.2 In cases of missing adult patients, the Police must be informed where appropriate, i.e., if they are a likely danger to themselves or others. When found, reasonable effort will be made to return the patient to the ward or department (Refer to Restrictive Intervention and Restraint Policy).

4.7.3 Some patients including those who are elderly, frail and confused are particularly vulnerable and will, on occasion, leave ward areas without informing anyone of their plans or expected time of return. These patients may be at risk of harm to themselves or to others and are to be classified as 'missing'. Every effort must be taken to locate these patients; their plans agreed or be assisted back to the ward areas. When a vulnerable / high-risk patient has been identified as "missing", the Trust Security Team must be given the earliest opportunity to become involved in the risk management of

the patient and conduct a systematic search. Those involved in a search for a missing patient should ensure that any systematic search considers high risk areas such as potential ligature points, roof access, plant rooms, fire exits and multistorey car parks.

4.7.4 If the patient is not located, the patient could be considered as having unofficially discharged themselves. The decision as to whether to regard the patient as having self- discharged will be made by the Senior Nurse/Matron in conjunction with the duty Consultant or their deputy. All reasonable efforts will be made to contact the next of kin.

4.7.5 The incident will be recorded in the patient's case notes and the Trust incident reporting system.

4.8 Lost and Found Property

4.8.1 Lost and found property must be handed into Security or the General Office. Information relating to the time and date of when the property was found to also be provided. In cases where money is found staff should sign and provide details of how much was found and where. The Trust will not be held responsible for money lost that was not placed and signed into patients' property as per the Patient Property Policy.

4.9 Access and Egress

4.9.1 Access to, and egress from, hospital buildings will be restricted in accordance with the Trust lock-down procedures. This refers to out of hours lockdown or emergency lockdown. Staff must not force or permanently fix open or modify access-controlled doors/systems at any time

4.10 Property

4.10.1 Trust Property

It is an offence for members of staff to remove any property belonging to the Trust without authority. Failure by anyone to seek the proper authority, usually from their line manager prior to removing Trust property, could result in disciplinary action or criminal proceedings being taken against the person or persons involved. Staff must take reasonable steps to safeguard all Trust property whilst in their care. If any employee is aware that Trust property has been or is being stolen, then they must report this to their line manager and the Car Parking and Security Control Centre (CPSCC) and complete an incident form in line with Trust reporting procedures.

4.10.2 Personal Property

If private (personal) property has been stolen then it is the owner's, not the Trust's, responsibility to report the matter to the Police and complete an incident form in line with Trust reporting procedures. Trust staff members must also seek prior approval from the rightful owner prior to removing any personal item/s belonging to another. This can be done via a witnessed verbal agreement or patient signature. Failure to do so may result in an act of theft occurring and may result in criminal or disciplinary proceedings taking place.

4.10.3 The Trust does not accept liability for the loss of, or damage to private property including motor vehicles or other modes of transport. Motor vehicles and other modes of transport are brought onto Trust premises entirely at the owner's risk. The Trust will, however, take all reasonable steps to safeguard vehicles left unattended on its property

4.10.4 Staff, including contractors, sub contactors and agency workers are advised to take adequate precautions to ensure the safety of their personal possessions and not bring valuables to work. Where a locker has been provided for personal use, the person using the locker will be responsible for providing a suitable lock. Any defects of the locker must be reported immediately to the appropriate manager.

4.10.5 Staff must report any loss or damage to their belongings, their lockers or damage to the locker areas, to their line manager and the Car Parking and Security Control Centre (CPSCC) and co-operate in any consequent enquiry into the loss or damage.

4.11 Security Marking of Property

4.11.1 Valuable and/or attractive items of equipment (e.g. IT equipment) will be marked to deter theft, which assists in identification in the event of loss or theft. Items belonging to the Information Technology Department are to be marked by this department.

4.11.2 All marked equipment should have a unique way in which to identify it as Trust Property. The correct visible identification of a marked piece of equipment will help to deter a criminal act occurring, for example a barcode.

4.12 Write-Off

4.12.1 The reporting and investigation of all losses (thefts etc) will be in accordance with the Trust's incident reporting procedures and Standing Orders, reservations and Delegations of Powers and Standing Financial Instructions Policy.

4.13 Key Security

4.12.1 Where specific individual members of staff are provided with keys it is their responsibility to keep them safe and report any loss or theft of these keys to both their line manager and the Security Department.

4.12.2 The following principles provide adequate control over ward and department bunches of keys, and ensures accountability:

- Master keys will not generally be available, keys to specific doors can be issued in accordance with a key issuing protocol, a legible record maintained of the issue and return of keys including names and signatures
- Keys must remain under the control of the department or ward manager (or nominated deputy) and must be accounted for at all times
- Keys held by a ward or department for doors within that area should be held in a lockable key cabinet and a legible record maintained of the issue and return of keys including names and signatures.
- Keys must be held in a lockable key cabinet and a legible record maintained of the issue and return of keys including names and signatures.
- There will be duplicates of all keys held by the Estates Department/Skanska
- All key losses must be reported to the ward/department manager and the relevant Security Service.
- All keys will be cut by the Estates Department/Skanska on receipt of a signed

request form from the ward/department concerned.

- As a rule, labels must not be attached to keys to indicate the lock to which the key.

4.12.3 Computer Security

Policies governing computer and network security are issued by the ICT Department and available via the Intranet.

4.12.4 Lone Workers

The Royal Wolverhampton NHS Trust and Walsall Healthcare NHS Trust recognise that lone working is a significant danger for staff. The Trust is committed to creating a safe working environment for its employees by adopting systems and protocols within the Trust. All forms of aggression displayed towards staff, i.e., verbal abuse (including racial/sexual) and physical assault/threatening behaviour - will not be tolerated and wherever possible action will be taken against persons displaying such behaviour. Steps will be taken in all areas to meet statutory obligations placed upon the Trust (Health & Safety at Work Act Section 2 and the Secretary of State Directions Statutory Instrument 3039, 2002), this will include doing all that is reasonably practicable to identify and control the risk of violence to its staff.

Furthermore, the Trust will strive to maintain compliance with 'Secretary of State Directions' in creating a safer working environment for its staff by the delivery Conflict Resolution Training to staff.

The arrangement for ensuring our staff (if identified as a lone worker) are safe can be found in the lone worker procedure (Attachment 3) The Trusts' overall aim is to:

- Assess and reduce the risk of violence, aggression, or attack on staff
- Take necessary steps to protect against all forms of violence, where possible
- Ensure employees are supported and provided with suitable aftercare or counselling following an incident of violent or aggressive behaviour
- Fulfil legal obligations as outlined in the Health and Safety at Work Act1974
- Ensure the safety of its employees whilst at work
- Ensure lone working arrangements will be developed among each staff group
- Ensure all staff attend Conflict Resolution Training

5.0 Financial Risk Assessment

1	Does the implementation of this policy require any additional Capital resources	**No**
2	Does the implementation of this policy require additional revenue resources	**No**
3	Does the implementation of this policy require additional manpower	**No**
4	Does the implementation of this policy release any manpower costs through a change in practice	**No**

5	Are there additional staff training costs associated with implementing this policy which cannot be delivered through current training programmes or allocated training times for staff.	**No**
	Other comments From a Trust perspective there is a nil resource implication: however, local security risk assessments may identify a resource consequence.	

6.0 Equality Impact Assessment

An Equality Analysis has been undertaken. No adverse effects have been identified for staff, patients or the public as a result of implementing this policy.

7.0 Maintenance

This Policy will be reviewed 3 yearly by the Trusts LSMS who reports to the Chief Operating Officer.

8.0 Communication and Training

Staff will be informed of the policy on local induction. Staff will receive security training relevant to their role in accordance with the Trust Statutory and Mandatory Training policy (Training Needs Analysis) such training will be developed to enable an integrated approach to security management across the Trusts. The policy will be available to all Trust managers and staff via the intranet. The Policy will be shared at Health and Safety Group/Forums and with safety representatives.

9.0 Audit Process

Criterion	Monitoring Method	Frequency	Committee Group	Lead
Requirements to undertake appropriate risk assessments regarding physical security of premises, assets, lone working, violence and aggression	Health & Safety Audit	Annual	H&S Steering Group	Departmental Managers / Health & Safety team
	Self-assessment Return, H&S toolkit	Quarterly		
	Review of H&S Compliance evidence eg risk assessments, SSoW, Training etc.	Quarterly		
Arrangements for ensuring that action is taken as a result of risk assessments including safety of lone workers.	Health & Safety Audit - Review of risk assessments for security / lone working / V&A etc	As required	H&S Steering Group	Departmental Managers / Health & Safety team /LSMS
Incident Monitoring	Review of incident statistics	Weekly / Monthly	LSMS / H&SC	LSMS

Staff Survey Results	Review of Staff Survey results	Annually	H&S Steering Group	LSMS
Monitoring arrangements for compliance and effectiveness of Lockdown arrangements	Following a lockdown event, a report will be provided to the Security monthly meeting. Monitoring of training uptake and drills. Minutes of Emergency Planning meetings. Emergency Preparedness Annual Report	Annually	H&S Steering Group Emergency Preparedness Group	LSMS EPRR Lead
Organisation's expectations in relation to staff training, as identified in the Training Needs Analysis	Refer to Statutory and Mandatory Training policy. Conflict Resolution training.	Refer to Statutory and Mandatory Training policy. 3 yearly.	Refer to Statutory and Mandatory Training policy. H&S Committee	Refer to Statutory and Mandatory Training policy / Department Manager
Review of subject access requests	Monitoring of CCTV and access control data	Monthly (as required) Annual report	IG Steering Group / Divisions / H&SC / Audit Committee	LSMS

10.0 References

- NHS Counter Fraud Authority https://cfa.nhs.uk/
- NHSE Violence Prevention and Reduction Standards Violence Prevention Reduction Standards
- Publication scheme
- Patient Records Policy
- Standing Orders, Reservations and Delegations of Powers and Standing Financial Instructions Policy
- Secretary of State Directions for Security Management
- National Security Strategy
- Health and Safety Policy
- Fire Policy
- Risk Management Policy
- Medicines Policy
- Disciplinary Policy
- Capability Policy
- Communications and Information Security Policy

- Absconding Patient from Walsall Healthcare Trust
- Trust Uniform and Dress Policy
- Statutory and Mandatory training Policy
- Health and Social care Act 2008 (Regulated Activities) Regulations 2014
- Health and safety at work Act
- NHS PAM
- “A Safer place to work”- National Audit Office
- “Tackling Violence against Staff” - CFSMS

Part A – Document Control

Policy number and Policy version: GOP V1.0	**Policy Title:** Group Security Policy	**Status:** Final		**Author:** Security Manager **Director Sponsor:** Managing Directors for RWT and WHT
Version / Amendment History	Version	Date	Author	Reason
	1.0	November 2025	Deputy Head of Security and Car Parking	Implementation of Group Policy – Supersedes RWT's OP26, Security Policy and WHT's WHT-OP980, Security Policy
Intended Recipients: All Trust employees				
Consultation Group / Role Titles and Date: Divisional Management, Health and Safety Committee, Policy Committee, Trust Board				
Name and date of Trust level group where reviewed		WHT Policy Management Core Group – Chair's approval – December 2025 RWT Trust Policy Group – December 2025		
Name and date of final approval committee		WHT Policy Management Core Group – Chair's approval – December 2025 RWT Trust Policy Group – December 2025		
Date of Policy issue		April 2026		
Review Date and Frequency (standard review frequency is 3 yearly unless otherwise indicated – see section 3.8.1 of Attachment 1)		December 2028 – Every 3 years		
Training and Dissemination: Launched by Trust Bulletin, Senior Managers Briefing.				
Publishing Requirements: Can this document be published on the Trust's public page: Yes If yes you must ensure that you have read and have fully considered it meets the requirements outlined in sections 1.9, 3.7 and 3.9 of OP01, Governance of Trust-wide Strategy/Policy/Procedure/Guidelines and Local Procedure and Guidelines, as well as considering any redactions that will be required prior to publication.				
To be read in conjunction with: Health & Safe Policy, Incident Reporting Learning and Management Policy, GDPR (Information Governance) Policy, Lone Working Policy, Fire Policy, Lockdown Policy, Major Incident Plan.				

Initial Equality Impact Assessment (all policies): **Completed Yes Full Equality** **Impact assessment (as required):** **Completed Yes**	
Monitoring arrangements and Committee	Health & Safety Meeting group
Document summary/key issues covered. This Policies covers aspects of Security on Trust premises	
Key words for intranet searching purposes	
High Risk Policy? **Definition:** • Contains information in the public domain that may present additional risk to the public e.g. contains detailed images of means of strangulation. • References to individually identifiable cases. • References to commercially sensitive or confidential systems. If a policy is considered to be high risk it will be the responsibility of the author and chief officer sponsor to ensure it is redacted to the requestee.	**No (delete as appropriate)** If Yes include the following sentence and relevant information in the Intended Recipients section above – In the event that this is policy is made available to the public the following information should be redacted:

Security Policy Attachment 1

Management of Violence & Aggression (MOVA)

A Procedure for Management of Violence & Aggression (MOVA – Recorded Verbal warning, Yellow and Red Card Procedures for persons aged 18 or over)

This Procedure applies to Patient and Visitors

1.0 Procedure Statement

1.1 Walsall Healthcare and The Royal Wolverhampton NHS Trusts have a duty to provide a safe and secure environment for patients, staff and visitors. Violent or abusive behaviour will not be tolerated, and decisive action will be taken to protect staff, patients and visitors.

1.2 The Management of Violence & Aggression (MOVA) will support the Security Policy by setting out the procedure for the management of patients and visitors who are violent or abusive in their behaviour toward staff, other patients or members of the public.

1.3 Those patients who, in the expert judgement of the relevant clinician are not competent to take responsibility for their actions (e.g. an individual who becomes abusive as a result of an illness or injury) or require urgent emergency treatment will not be subject to this procedure. Patients who are under the age of 18, have mental health needs or the impact of cognitive or learning disability or health related delirium are excluded from the MoVA procedure. The required clinical assessments are outlined in section 2.5 below.

1.4 The aim of the procedure is to detail behaviours which are unacceptable. Patients or visitors who are extreme or persistent in their unacceptable behaviour can be issued with a Recorded Verbal Warning, "Yellow" or "Red" Card resulting in extreme cases exclusion from the Trust (this excludes emergency care/treatment).

1.5 This procedure has three stages (Recorded Verbal Warning – stage 1, Yellow Card – stage 2 and Red Card – stage 3) which are normally intended to be followed progressively. However, where the behaviour so warrants, the procedure may be commenced at anyone of these three stages. All three stages should be documented, and relevant records recorded including incident report forms.

1.6 This procedure may also be followed where a patient/visitor is known to present a risk towards staff, other patients or members of the public, irrespective of the source of the information regarding such risks, for example, a patient with a history of violence towards staff at another healthcare provider. In such cases, the procedure may be commenced at any one of the three stages.

1.7 Immediate management of incidents of violence/unacceptable behaviour must be dealt with in accordance with the Security Policy. Incidents must be entered onto to the Trust incident reporting system and consideration should be given to reporting incidents of assault/violence to the police where there is violation of the law.

2.0 Unacceptable Behaviour

2.1 Examples

The following are examples of behaviour that are not acceptable (this is a non-exhaustive list – other behaviours presenting threat or risk to staff will be considered unacceptable):

- Excessive noise, e.g. loud or intrusive conversation or shouting
- Threatening or abusive language involving swearing or offensive remarks
- Derogatory, racial, sexual or remarks of a personal nature
- Malicious / defamatory allegations relating to members of staff, other patients or visitors
- Offensive sexual / racial gestures or behaviour
- Abusing alcohol, drugs or other substances on NHS Premises (however, all medically identified substance abuse problems will be treated appropriately)
- Drug dealing
- Wilful damage to Trust property
- Theft
- Threats or threatening behaviour
- Violent or aggressive behaviour
- Any other behaviour which interferes with any member of staff's effective performance of their duties

2.2 Prevention of Violence & Aggression Risk Assessment

2.2.1 Violence and Aggression is a hazard and must be considered in Risk Assessments. In each department, the level of the Risk should be evaluated by considering:

- The task
- The number of staff present
- The exposure to members of public and patients
- The likely responses of patients
- The work environment
- Previous incidents of violence and aggression

2.2.2 Violence and Aggression risk assessments must be completed by the service manager for their department; the assessment must be carried out using the designated violence and aggression risk-assessment template as prescribed by Group HS01 – Protocol 1. The assessment and any identified control measures must be detailed as required under Group HS01 – Protocol 1.

2.2.3 The detailed current control measures in place to reduce or prevent the risk of violence and aggression should be appropriate and proportionate to the assessed risk (i.e., the risk level in that area). Further controls may be required where current controls are not appropriate or proportionate in reducing the risk; in such instances, they must be

implemented as soon as possible. For guidance on violence and aggression risk-assessments, please refer to a completed example on the Health and Safety Team page on the Intranet or liaise directly with the Health and Safety Team.

2.3 Factors Which Influence Violent Incidents

2.3.1 Environment

Consideration should be given to the following factors particularly in public areas and also considered during redesign or new builds:

- Provision and position of reception / waiting areas
- Layout (e.g., no blind spots)
- Good lighting
- Adequate space
- Aggravating noise
- Passive colour and décor
- Measures to reduce boredom (e.g., magazines)
- Access to public toilets
- Sufficient seating
- Robust and secure fixtures, correct storage of equipment, good housekeeping
- Appropriate segregation between staff and public
- Proper clear signage
- Design of passageways, walkways, car parks, etc., unhindered vision, clear routes
- Layout of rooms, re: escape routes

2.3.2 Security Equipment

Consideration should be given to:

- Locks, keypads, swipe cards
- Intercoms
- View panels in access doors
- Grilles / security glass
- CCTV and monitoring screens
- Flood lighting

- Entry alarms
- Personal alarms
- Panic buttons
- Access to a phone

2.3.3 Work Organisation / Communication

Working practices should encourage a free flow of information between staff, patients and relatives to alleviate frustration. It is essential that information is communicated between staff when potentially violent patients are being treated or transferred within the service (this should also include inter-agency transfers).

Communication of information is particularly important when:

- New staff are employed
- New patients are referred
- There is recognised change in patients' behaviour
- Potentially violent patients present to other departments or are to be referred for a domiciliary visit.

In regard to the assessment and communication of specific patient needs where the patient is under 18, has mental health needs, the impact of cognitive or learning disability, delirium or the acuity of their illness, reference must be made to the Enhanced supervision Policy (CP66).

2.3.4 Staffing

Staff may become more vulnerable to attack or threat if they are:

- Fatigued
- Over stretched
- Lone working
- Under qualified or inexperienced
- Not trained to respond to violent incidents

2.4 MOVA Process for Adult Patients (18 or over)

- **Patients**

PRIOR TO ANY STAGE OF MOVA

A clinical review of the patient's condition must be made by the most senior member of the individual's clinical team to ascertain whether the behaviour is excused by the patient's mental state at the time, considering their medical condition and their medication. If the behaviour is excused on medical grounds, this must be documented

fully in the patient's healthcare records and managed under the appropriate policy for enhanced care supervision.

Where following the clinical review, it has been established that there is no clinical justification, cause or excuse for the patient's behaviour, the following process must be applied.

In the event of unacceptable behaviour by a patient (outlined in Section 2.1), the Departmental Manager or Nurse in charge of the relevant area must explain to the patient that his/her behaviour is unacceptable and of the expected standards that must be observed in future and advised on any failure to comply. Where possible this explanation must be carried out in front of a witness and must be documented in the patient's healthcare records with the details of the incident that triggered the MOVA process Recorded Verbal Warning. An incident report form MUST be completed using the Trusts incident reporting system. The patient must be advised that he/she is receiving a Recorded Verbal Warning; the patient's Consultant must be informed of the warning that has been issued.

NB. For patients under the age of 18, mental health presentations, the impact of cognitive or learning disability, delirium or the acuity of their illness please refer to the Enhanced Supervision Policy (Refer CP66/TBC).

- **Sanctioned Visitors (anyone who is not a patient or staff member)**

  Any staff member can challenge visitors who display any of the behaviours listed in Section 2.1 will be asked to stop and offered the opportunity to explain their actions.

  Continued failure to comply with the required standard of behaviour will result in security staff being contacted and the offending individual will be asked to leave Trust property. Should the persons not leave the premises of their own free will, then the Police will be contacted for removal. Should details of the individual be available or shared then the MOVA process can be followed if no details shared then removal on verbal warnings given.

  The behaviour of visitors will not affect the treatment of the patient that they were visiting. If excluded the individual may subsequently request a review of the exclusion and this must be in writing to the relevant senior member of the Trust management team who issued the sanction.

- **MOVA Overview**

  Following any V&A incident deemed to be appropriately severe or a repeated threat, and subsequent to a clinical review of the patient's medical condition and mental state; the appropriate senior manager (as listed below) can decide to issue a **Stage 1- Recorded Verbal Warning** and explain to the patient (or visitor) that his / her behaviour is unacceptable and explain the expected standards that must be observed in the future.

  If the behaviour continues, the responsible manager or clinician will issue a **Stage 2- Yellow Card** detailing the possible consequences of any further repetition. Failure to comply with the MOVA, at the request of staff can result in escalation to exclusion from the Trust (**a Stage 3 - Red Card**).

  Such exclusion will usually last one year, subject to alternative care arrangements being made; the provision of such arrangements will be pursued with vigour by the relevant clinician. In the event of an excluded individual presenting at the Trust's Urgent and Emergency Care Centre for emergency treatment, that individual will be treated and

stabilised with, if necessary, security staff in attendance. Where possible, they would then be transferred immediately. However, if admission is unavoidable, security staff will, if necessary, remain in attendance. The need for security attendance will be determined by an appropriate member of staff.

Any patient behaving unlawfully should be reported to the police and the Trust may seek the application of the maximum penalties available in law.

The Trust will potentially seek a Court Injunction preventing the individual coming onto site or coming within a defined distance of the site / or named employee.

A relevant divisional manager / senior nurse / clinician may as part of the sanction decide to continue to exclude any individual removed from the premises or restrict their visiting only to specific times and, if necessary, under escort from security staff arranged by relevant staff from the department.

When patients trigger for the MOVa policy to be implemented this can in certain situations be done during the patients stay within the hospitals however some situations will warrant the process being followed the incident.

At all times it is best practice to seek guidance and support from the Security Management Team on this so that assistance can be given and additional security measures put in place while the process is implemented (this can be additional security patrols, and one to one care should the behaviour warrant such action). The process of MOVa can take place post incident as on many occasions the individual will have left the care of the hospitals in this scenario the process is still the same with the warnings and communications being posted out or the individual being notified of the process on their return to the site with support from security should the need arise.

The standard 1 year exclusion period could be extended where the terms are not complied with and/or there are repeat incidents. The LSMS/Security team will provide advice to local management to assess each MoVA sanction as it approaches expiry for a decision on removal or extension of the sanction.

The Electronic Patient Record will provide an alerting platform for staff to be notified of risks of Violence and Aggression from patients. The LSMS/Security will be responsible for entering MoVA sanctions into the alerts section of the Electronic Patient record system; and for reviewing and maintaining accurate records of live and expired MoVA sanctions.

The Incident Reporting system will provide the platform for recording Violence and Aggression incidents from patients and non-patients (in the case of non patients it will be the main data source along with intelligence from the Security staff).

A detailed outline of the MOVA procedure steps is provided below

Stage 1 – Recorded Verbal Warning to be Added Onto Patients Record

A Recorded Verbal Warning must be decided and implemented by an appropriate senior member of the Trust management team. These include:

- Site Manager / Out of Hours Practitioner
- Clinical Director / Consultant
- Divisional Management Team

- Directorate / Care Group Management Team
- Local Security Management Specialist (LSMS)
- On Call Manager / On Call Director
- Senior Nurse / Ward Manager
- Matron

Individuals (patients and visitors) will be informed that they are being issued with a Recorded Verbal Warning and their behaviour will not be tolerated and where unacceptable behaviour continues further sanctions may be sought to prevent them attending Trust property by use of legal means. Patients and visitors are subject to all three stages of this procedure where the criteria is met.

When a patient warrants a Recorded Verbal Warning, the status will remain in effect for a 12 - month period. If the patient has not had any further episodes of unacceptable behaviour, the Recorded Verbal Warning status will be removed unless there is indication of continued unacceptable behaviour. The LSMS and Security Management Team will consider any continued or repeated behaviours to inform local management decisions to remove, extend or escalate the MoVA sanction.

When a decision has been made to implement a Recorded Verbal Warning, it is the responsibility of the person issuing the card to undertake the following:

- Document staff member's concerns
- Decide whether action under this procedure is required after confirming the clinical review. Further consultation with the patient's medical team may be appropriate.
- Ensure that the correct procedure has been followed in the issuing of the Stage 1- Recorded Verbal Warning
- Ensure the incident Reporting System records are completed (including a copy of the formal letter issued)
- Provide a file copy of Recorded Verbal Warning letter to the patient notes and to the LSMS and Trust Security team who will record the MoVA sanction in the alerts section of the electronic Patient record system.

If a patient (or visitor) complies with the terms of the MOVA he / she can expect the following:

- That (for patients) their clinical care will not be affected in anyway
- That where substance abuse has been identified, appropriate assistance will be provided
- That the Trust Security team, Local Security Management Specialist (LSMS) is informed
- That the Walsall Healthcare and The Royal Wolverhampton NHS Trust will fully investigate all valid concerns raised by the patients, through the normal PALS process
- That the MOVA will expire after one year where the requirements of the sanction

are complied with and there are no repeat incidents or threats to safety

- To be informed in writing of any extension to the MoVA sanction and the reasons for this decision

Staff must report all incidents and Recorded Verbal warning onto the relevant Trust incident reporting system (attach/upload the formal warning letter to the incident), and in the case of patients, staff must add the Recorded Verbal warning to the patient's care record and attach a copy of the formal letter issued to the patient, a brief summary of behaviour exhibited by the individual, the risk/impact on staff and circumstances of the decision taken for the sanction issued.

A copy of the Stage 1 Recorded Verbal Warning letter issued to the patient must be sent to the Security team and LSMS enabling Security Management to actively monitor Recorded Verbal Warnings on site and to enter the MoVA sanction as an alert on the Electronic Patient Record.

Stage 2 – Issue of Yellow Card

Continued unacceptable behaviour will result in progression of MOVA process and the application of a Yellow Card.

A Yellow Card must be decided and implemented by an appropriate senior member of the Trust management team. These include:

- Site Manager / Out of Hours Practitioner
- Clinical Director / Consultant
- Divisional Management Team
- Directorate / Care Group Management Team
- Local Security Management Specialist (LSMS)
- On Call Manager / On Call Director
- Senior Nurse / Ward Manager
- Matron

The patient will be advised by staff that any further incident of unacceptable behaviour within a 12-month period may result in escalation to Red Card Status, i.e. their exclusion from (non-emergency) treatment within the Trust.

When a patient warrants a yellow card, the status will remain in effect for a 12- month period. If the patient has not had any further episodes of unacceptable behaviour, the yellow card status will be removed unless there is indication of continued unacceptable behaviour. The LSMS and Security Management Team will consider any continued or repeated behaviours to inform decisions to remove, extend or escalate the MoVA sanction.

If a patient (or visitor) complies with the terms of the MOVA he / she can expect the following:

- That (for patients) their clinical care will not be affected in anyway
- That where substance abuse has been identified, appropriate assistance will be provide
- That the Trust Security team, Local Security Management Specialist (LSMS) and

their GP is informed

- That the Walsall Healthcare and The Royal Wolverhampton NHS Trust will fully investigate all valid concerns raised by the patients, through the normal PALS process
- That the MOVA will expire after one year where the requirements of the sanction are complied with and there are no repeat incidents or threats to safety
- To be informed in writing of any extension to the MoVA sanction and the reasons for this decision

The LSMS/Security will be responsible for entering MoVA sanctions into the alerts section of the Patient record system; and reviewing and maintaining accurate records of live and expired MoVA sanctions.

Stage 3 – Issue of Red Card

The final decision to issue a Red card must be approved by the Chief Executive Officer before it is issued to the patient and implemented. Local recommendation for issuing a Red card will be formed by appropriate senior members of the Trust management team listed below.

The Red Card Status maybe issued, where the patient or visitor has failed to comply with the terms of the procedure during a Recorded Verbal Warning, Yellow Card status and/or in situations where the patient's behaviour has been of an extreme or serious nature.

The issue of a red card and subsequent exclusion from treatment within the Trust will be implemented (following CEO approval) by an appropriate senior member of the Trust Management Team, who must be different to the staff member who issued the Yellow Card. These include:

- Site Manager / Out of Hours Practitioner
- Clinical Director / Consultant
- Divisional Management Team
- Directorate / Care Group Management Team
- Local Security Management Specialist (LSMS)
- On Call Manager / On Call Director
- Senior Nurse / Ward Manager
- Matron

The case for implementation of a Red Card must be presented to the Chief Executive, before any formal action is taken. The Chief Executive will discuss the case and either endorse or deny the Red Card implementation.

When a decision has been made to implement a Red Card, it is the responsibility of the person issuing the card to undertake the following:

- Document staff member's concerns
- Decide whether action under this procedure is required after confirming the clinical review. Further consultation with the patient's medical team may be appropriate

- Ensure all necessary alternative care arrangements are made promptly
- Ensure that the correct procedure has been followed in the issuing of the Stage 3 – Red Card
- Ensure the incident Reporting System records are completed (including a copy of the formal letter issued)
- Provide a copy of the Patient letter and GP letter to the CEO for final approval and signature
- Provide a file copy of Red card letter to the patient notes and to the LSMS and Trust Security team who will actively monitor compliance with the Red Card and record the MoVA sanction in the alerts section of the electronic Patient record system

A checklist for implementation of Red Card Status (appendix 1b and 4a) must also be completed to ensure that all stages of the Red Card process have been completed correctly. The completed checklist must be sent with the patient Red card letter and the GP letter to the CEO for sign off prior to the Red card being issued to the patient or implemented.

Such exclusion will usually last one year, subject to alternative care arrangements being made; the provision of such arrangements will be pursued with vigour by the relevant clinician, information on care arrangements must be documented in the patient record and in the Patient Record system.

The patient will be sent a letter from the Chief Executive informing them of the implementation of the Red Card. (Appendix 4b).

When a patient warrants a Red card, the status will remain in effect for a 12- month period. If the patient has had no further episodes of unacceptable behaviour, the Red card status will be removed unless there is indication of continued unacceptable behaviour. The LSMS and Security Management Team will consider any continued or repeated behaviours and make proposal to the local management and to CEO to inform decisions to remove or extend the MoVA sanction. Where decisions are made to extend the sanction, the appropriate responsible clinician must arrange extended/ongoing alternative care arrangements and to formally notify the patient's GP and the patient in writing. Records of the decision to extend and rationale must be made in the patient's care record (by responsible clinical staff), the patient record alerts system (by the LSMS/Security team) and in the incident reporting system with formal letters attached (by the incident reporter and/or LSMS/Security team).

The LSMS/Security will be responsible for entering MoVA sanctions into the alerts section of the Patient record system; and reviewing and maintaining accurate records of live and expired MoVA sanctions.

Implication of a Red Card

If a patient (or visitor) complies with the terms of the MOVA Red Card sanction, the patient can expect the following:

- The patient will be excluded from the clinical care at the relevant Trust, except when presenting at the Emergency Department for emergency care and treatment
- An alternative location and arrangements for any ongoing care needs will be made by an appropriate clinician and their GP will be informed
- The Trust will fully investigate all valid concerns about the process raised by the patient

- The Red Card sanction will expire after one year where the requirements of the sanction are complied with and there are no repeat incidents or threats to safety

- To be informed in writing of any extension to the MoVA sanction and the reasons for this decision

- That the Trust Security team, Local Security Management Specialist (LSMS) and their GP is informed

- That the Walsall Healthcare and The Royal Wolverhampton NHS Trust will fully investigate all valid concerns raised by the patients, through the normal PALS, complaints process

- Where substance abuse has been identified, appropriate assistance where available may be offered via GP services

Exclusion from Treatment / Alternative Care Arrangements

A patient who has received a Red Card must be advised that they can appeal to the Trust against any decision to exclude them from treatment through the Trust PALs process. Such exclusion will usually last for a period of 12 months, subject to alternative care arrangements being made. The Consultant responsible for the patients care (on behalf of the Trust) will discuss such arrangements with the patient's general Practitioner (Appendix 4c) and the relevant Commissioning body to ensure appropriate alternative arrangements are commissioned.

In the event of an excluded individual presenting at the Trust's Urgent and Emergency Care Centre, that individual will be identified by the electronic Patient Record system upon booking in. They will be treated and stabilised with, if necessary, security staff in attendance. Where possible they must be transferred immediately. However, if admission is unavoidable, security staff will, if necessary, remain in attendance. The need for security attendance will be determined by an appropriate member of staff for example ward manager, senior nurse or matron.

Return onto Trust Premises

If an excluded individual returns to the Trust in circumstances other than a medical emergency, security staff should be called immediately. If necessary, the police will be asked to attend. The Trust may subsequently seek a Court Injunction preventing the individual coming onto site or coming within a defined distance of the site/ or named employee.

Appeals Against Recorded Verbal Warning / Yellow / Red Card Status

Should the patient wish to challenge the decision, they may do so by requesting a review of the Sanction/exclusion and this must be in writing to the PALs service.

MoVA Within Primary Care

Primary Care services have a slightly different procedure for managing yellow and red cards in the community (see appendix 6); this flow chart is to be followed for primary care patients and there is also a requirement for any sanctions for primary care patients to also be added onto the Patient Record system so that information can be shared as patients may present at the Trust.

MoVA Arrangements Within Community Services

Community services are still covered by the MoVA procedure but how the procedure will be implemented will differ from service to service and depend on the level of care required. It's recognised that some services are unable to be removed from the community settings as this would have a detrimental effect on patient care. Community services will have their

own procedure in place to follow in line with MoVA which should be made available to all staff which will also align with the departments risk assessments.

Security management team will work closely with all community departments to help reduce the risk and offer advice and guidance on the risk assessments in place and any local producers that are created to help reduce the risk to staff working in the community settings.

All new referrals will be screened for background information which may indicate a potential risk. All referrals will be checked against the Trust's PAS/ Clinical Web portal for alerts/warnings. Where there is a history of violence concerning the patient or site location that is deemed a high risk, staff must work in pairs. Where possible, the visit should take place at a neutral location or within a secure environment, for example, health centre/GP practice. Alteration to staff uniforms will be permitted where there is a perceived or known risk (e.g. wearing polo t-shirts in place of tunics).

Due consideration needs to be given to time of visit and seasonal variations. Risk assessments (individual patient and generic) should be undertaken and locally held.

Staff considerations - All staff should undertake a "10 Second" assessment prior to putting themselves in a potential risk situation. Consider the following signs/triggers:

- Negative body language
- Signs of agitation
- Negative / aggressive verbal behaviour
- Evidence / suspicion of intoxication of any substance
- Imposing groups
- Premises: seclusion/poor lighting / damage / unexpected open doors N.B. This is in addition to staff following:
    - Buddying procedures (when not starting from or returning to base)
    - Sky Guard use
    - "Red/Purple folder" code word (Adult Community only)
    - Personal alarm use
    - Frequent calls to base or "buddy"

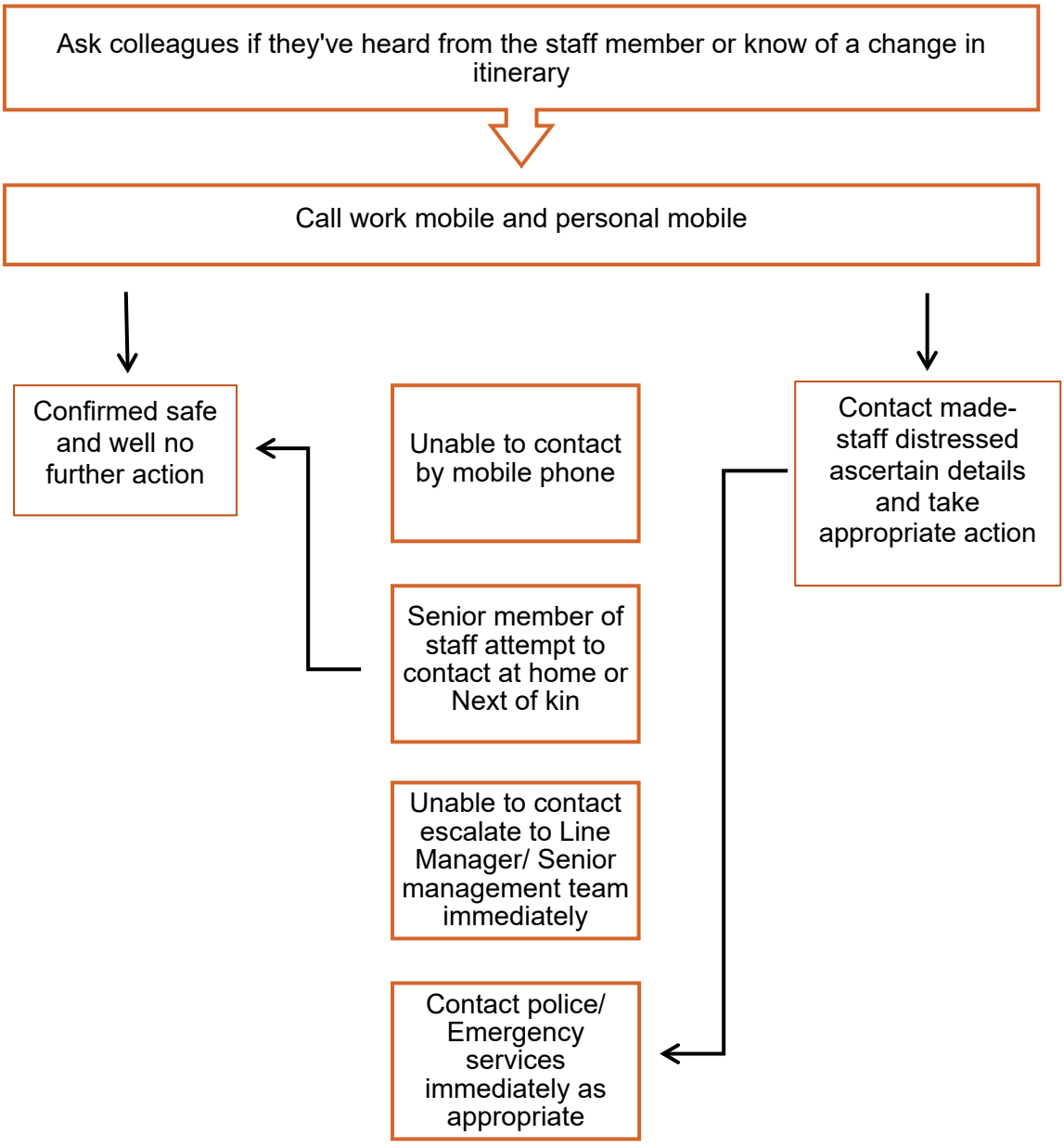
In the event of identifying a risk, staff should contact office/colleague and arrange a 5-minute call back. This will provide the opportunity to leave the situation without causing suspicion. In a clinic environment the member of staff should activate any panic alarm facility available or use either the landline or mobile telephone to make a discreet call to a colleague/reception staff. If no panic alarm facility exists follow advice below.

Managers should ensure a list of staff members along with car details (registration/make/model) should be kept in a secure location but accessible to designated leads. This would enable a formal vehicle search to be undertaken should concerns for a lone worker arise. Managers should ensure emergency contact sheet is kept up to date for each member of staff and consider holding a photograph of each staff member on their personal file. This should be reviewed annually for any update in appearance where a new photograph may be required. IMEI numbers for Trust mobile phone and iPad SIM cards should be held on individual personal files, as these can be GPS tracked in the event of an emergency.

Staff members should ensure use of E-community (for RWT staff) and Community portal (for WHT staff) as this acts as a live allocation.

For Community settings Recorded verbal warning, Yellow and Red card sanctions will follow the trust processes with warnings applied to the Patient information system and risk assessments completed at the location of care being provided. See Flowchart below.

Staff Member Does Not Return to Base or Fails to Confirm Whereabouts



- **MoVA Oversight by the Security Management Team**

  The Security Management Team will receive copies of MOVA correspondence from Service areas/management and will monitor all stages of MoVA sanctions throughout the applicable period; and as they approach expiry.

  Along with local intelligence, the Security team will liaise with the service areas/management to consider whether the requirements of the sanction have been complied with to allow for the closure of the sanction on expiry. The Security team advise to support local management on this decision and will update the Patient record system with the local management decision i.e. whether the sanction is to be closed on expiry or if it is to be extended. The appropriate service management must communicate to the person or patient in writing (and their GP in the case of red/yellow carded patients) and upload the further documentation to the patient records and the incident reporting system.

  The MoVA sanction will automatically expire after 12 months where no extension has been updated in the patient record system by the LSMS/Security team.

  MoVA alerts will be recorded within the Electronic Patient Record system and the incident reporting system. Where system developments permit, the Security team will be aided in their oversight/monitoring responsibilities by automated notifications and system reports that trigger review and update of MoVA alerts.

3.0 Audit / Monitoring

This procedure will be available on the Trust intranet and implementation of this procedure will be monitored by the relevant divisional management team.

Divisions, Directorates, Care Groups and Department will ensure that all breaches of this procedure, by patients and visitors, are reported in line with Trust Incident and Risk Management Policy.

The oversight and enacting of active Recorded Verbal Warnings, Yellow and Red cards will be monitored by the Security Management team.

The Security Management Team will review the process for issuing of all Recorded Verbal Warnings/Yellow/Red cards and report within their routine reporting to Trust groups and an annual report. The LSMS and Security team will monitor all active MoVA sanctions in light of local intelligence held in considering whether a sanction should be extended; ensuring the appropriate systems are updated and communications made with all appropriate stakeholders.

The Security Management Team will monitor V&A incident trends and themes for targeted redress action.

The Security Management Team will produce reports on MoVA activity for the Trust Health and Safety meeting.

4.0 Equality and Diversity

This procedure has been assessed as not affecting the equality and diversity of any one particular group of stakeholder.

Appendix 1a

Management of Violence & Aggression

(MOVA) Guidance

Implementation Guidance – "Recorded Verbal Warning, Yellow and Red Card Procedures"

In the event of inappropriate behaviour by a person and in the case of a patient, following the clinical review by the individual's clinical team to ensure the MoVA procedure applies, the Management of Violence & Aggression (MOVA) "Recorded verbal warning, Yellow and Red Card Procedures" (hereafter referred to as the (MOVA) can be instigated.

Staff should advise their immediate manager who would contact a suitably senior member of staff e.g. the Divisional Manager/senior nurse/service manager or on call manager (out of hours).

It is the responsibility of that senior staff member (e.g. Divisional Manager/senior nurse/on call manager etc) to undertake the following:

1.0 Take full details of the incident and the staff member's concerns, wherever possible, get witnesses to the event to sign the record as true and accurate. Ensure staff record the incident within the incident reporting system.

2.0 Ensure a clinical review has occurred and check the requirements of the MoVA procedure to decide whether MOVA is required. Refer section 2.5 of the MoVA procedure for the required clinical assessment review and relevant criteria e.g. age, clinical condition etc.

3.0 If MOVA is required (Recorded Verbal warning, Yellow and Red Card):

- Inform and seek advice from the patient's consultant or senior member of the medical team (on-call team out of hours) or their GP if necessary. Where the individual is not a patient obtain as much information as possible for documentation.

- Inform the patient (or person) of the staff concerns and fully explain the MOVA procedure, ensuring that there is no confusion as to the standard of behaviour required or the possible consequences of failure to comply.

- Ensure that the correct MoVA approval and documentation sign off occurs - For the issue of stage 1 Recorded verbal warning and stage 2 Yellow Card, final sign off is undertaken by suitably senior members of staff as listed in section 2.4.3 of the procedure and in each standard patient letter (Appendix 2, 3b, 4b). For issue of stage 3 Red Cards final sign off must be obtained from the Chief Executive Officer. (Refer flowchart).

- Check the documentation and ensure that the MOVA process has been applied appropriately (complete the MoVA checklist in appendix 1b and in appendix 4b for Red Cards)

- Prepare a copy of the standard patient letter (either Appendix 2, 3b or 4b) for approval and sign off by a suitably senior members of staff as listed in section 2.4.3 of the procedure and in each standard patient letter (Appendix 2, 3b, 4b). (IMPORTANT NOTE – For the issue of Red cards, the patient letter and the GP letter must be signed by the CEO and alternative care arrangements agreed before the Red card is implemented and letter issued to the patient and the GP).

- In the case of stage 1 Recorded verbal warning, ask the patient or person to sign the Confirmation of MOVA document (Appendix 2). Ensure that a suitable member of

staff (any doctor or registered nurse) witnesses the explanation to the patient and signs the Confirmation of MOVA (Appendix 2). If the patient refuses to sign, this should be documented in the patient's notes, and it should be explained to the patient that the document will be valid with or without the patient's agreement.

- Give the patient/person a copy of the signed letter (either Appendix 2, 3b, 4b) and a copy of the MoVA procedure itself.

- Prepare a copy of the standard GP letter (either in Appendix 3a – for Yellow card or Appendix 4c – for Red card) for approval and sign off by a suitably senior members of staff as listed in section 2.4.3 of the procedure and in each standard patient letter (Appendix 2, 3b, 4b). (IMPORTANT NOTE – For the issue of Red cards, the patient letter and the GP letter must be signed by the CEO and alternative care arrangements agreed before the Red card is implemented and letter issued to the patient and the GP). A copy of the MoVA Policy must be sent to the patient GP.

- Copies of the signed patient/person letters for all stages of MOVA sanction must be sent to the Local Security Management Specialist for recording on the electronic patient record system (as an alert).

- Copies of documentation for all stage 2 and stage 3 MOVA sanction (Red and Yellow card only) must be sent to the Chief Executive Office and Security for file.

- A copy of the patient letter and GP letter must be kept in the patient's medical records

- The full process must be recorded in the patient's medical and nursing documentation and within the incident reporting system

Appendix 1b

Management of Violence & Aggression (MOVA)

Implementation Checklist – "Recorded Verbal Warning, Yellow and Red Card"

If Management of Violence & Aggression (MOVA) is required:

- Ensure the appropriate medical review is conducted and the person/patient does not meet any of the exemption criteria (Refer to section 2.5) and the MoVA procedure is correctly applied. ☐
- Inform the patient's consultant or senior manager of the medical team (on call team out of hours). ☐
- Ensure that the incident that triggered the MoVA procedure is fully documented in the patient's health record and reported in the incident reporting system. ☐
- Inform the patient of the staff's concerns and fully explain the Management of Violence & Aggression procedure (MOVA), ensuring that there is no confusion as to the standard of behaviour required or the possible consequences of failure to comply. ☐
- In the case of Stage 1 Recorded Verbal Warning - ask the patient to sign the Confirmation of MOVA document (Appendix 2). If the patient refuses to sign, this has been documented in the patient's notes and explained to the patient that the document will be valid with or without the patient's agreement. ☐
- Ensure that a suitable member of staff (any doctor or registered nurse) witnesses the explanation to the patient and signs the stage 1 Confirmation of MOVA letter. ☐
- In all cases provide the person or patient with a signed copy of the MoVA letter (either Appendix 2, 3b or 4b) and a copy of the MoVA procedure. (IMPORTANT NOTE – For the issue of Red cards, the patient letter and GP letter must be signed by the CEO and alternative care arrangements agreed before the Red card is implemented and letter issued to the patient and the GP) ☐
- In the case of Stage 2 Yellow card – a GP letter is completed and approved by the appropriate staff. ☐
- In the case of Stage 3 Red card – a GP letter is prepared and approved by CEO with alternative care arrangements agreed before the Red card is implemented and letter issued to the GP. ☐
- **Prior to the issue of Red Card for approval and to the patient please refer** to Appendix 4a Red Card Exclusion Procedure checklist. ☐

Appendix 2

Stage 1 Recorded Verbal Warning – Confirmation of MoVA

Surname		Forename	
NHS Number		Phone Number(s)	
Home Address			
GP Name		GP Phone Number	
GP Address			

This is to formally confirm that due to your unacceptable behaviour on (date).....

at (location)……,you have been issued with Recorded Verbal warning and are now subject to the conditions outlined in the Management of Violence & Aggression (MOVA).

The consequences of failure to comply with MoVA Procedures have been fully explained to you and you are advised of the expected standards of behaviour moving forward.

A copy of the Trust Policy for the Management of Violence & Aggression (MOVA) has been provided to you with this letter.

If you wish to appeal the decision, you can request a review of the sanction in writing to the relevant senior member of the Trust management team who issued the sanction or via the PALs service.

Patient Statement

I agree to comply with the expected behaviours set out in the Trust MoVa procedure, under which care will be provided at *The Royal Wolverhampton NHS Trust/Walsall Healthcare NHS Trust ** delete as appropriate*.

Patient Signed		Date	

If patient refuses to sign, this document is still valid.

Reason for refusal……...

Trust Initiator of the Stage 1 Procedure

I confirm I have explained the expected behaviours set out in the Management of Violence & Aggression (MOVA) procedure and the consequences of a failure to comply with the Procedures requirements.

Staff Name		(See appropriate staff listed below)	
Staff Signature		Date	

Examples of appropriate members of staff able to initiate the Procedure:- **Delete once selected*

- Site Manager / Out of Hours Practitioner
- Clinical Director / Consultant
- Divisional Manager
- Local Security Management Specialist (LSMS)
- On Call Manager

- Senior Nurse / Matron

Please note this verbal warning has been recorded in your patient record. This helps ensure the safety of both you and staff and ensures that actions taken are documented accurately and securely.

Note: A copy of the Management of Violence & Aggression (MOVA) Procedure must be attached to this letter.

Witnesses for the Trust Initiator of Stage 1 Recorded Verbal Warning Procedure

I confirm I was present when the explanation was given and this form completed.

Name		**Name**	
Designation		**Designation**	
Signed		**Signed**	
Date		**Date**	

Examples of appropriate members of staff to witness the Procedure: *Delete once selected

- Any Doctor or Registered Nurse

Appendix 3a

Management of Violence & Aggression (MoVA)

Stage 2 Yellow Card – Letter to GP

GP"s name and address

Date

Dear Dr

Re: Patient's name

Patient's address

Patient's date of birth

Patient's NHS number

The above individual is currently an in-patient on …… ward at The Royal Wolverhampton NHS Trust/Walsall Healthcare NHS Trust.

In order to protect the healthcare environment for other patients and members of staff, it has been necessary to instigate a Management of Violence & Aggression (MOVA) Procedure which has resulted in the issue of a stage 2 Yellow Card to the above patient (see enclosed letter).

If you have any queries, please do not hesitate to contact:

……. (Name and telephone number of patient's consultant)

and / or

……. (Name and telephone number of Divisional Manager or Head of Nursing)

A copy of the procedure Management of Violence & Aggression (MOVA) Procedure is enclosed for your information.

Your sincerely

*Sign and delete as appropriate

- Site Manager / Out of Hours Practitioner
- Clinical Director / Consultant
- Divisional Management Team
- Directorate / Care Group Management Team
- Local Security Management Specialist (LSMS)
- On Call Manager / On Call Director
- Senior Nurse / Ward Manager
- Matron

Enc

Enc Note: A copy of the Management of Violence & Aggression (MOVA) Procedure must be attached to this letter.

Appendix 3b

Management of Violence & Aggression (MoVA)
Stage 2 – Yellow Card – Letter to Patient

Ref:

Date:

Name: ……..

Address: ……..

……

……

NHS Number: ……..

Dear …….

This is to formally confirm that due to your unacceptable behaviour on (date).....

at (location)……,you are now subject to the conditions outlined in the

Management of Violence & Aggression (MoVA) Procedure. The Second stage of the procedure which is a Yellow card has been applied to you and you will have received an explanation as to why you are subject to this procedure. Your GP will also be informed.

You will also have been given a copy of the Trust's Procedure entitled Management of Violence & Aggression (MOVA) Procedure for "Recorded Verbal Warning, Yellow and Red Card."

Should you, on any occasion in the future, fail to comply with the expected standards of behaviour explained to you by…… and outlined in the MoVA Procedure, you may become subject to the next stage of the procedure (Red card), which may involve your immediate exclusion from the Trust premises by our security staff / police. Such an exclusion from Trust premises would mean that you will only receive emergency care and treatment at the Trust and your responsible clinician would make alternative arrangements for you to receive non-emergency care and treatment.

The duration of this sanction is 12 months and will expire after 12 months where there is compliance with the expected standards of behaviour outlined in the MoVA procedure.

If you wish to challenge the decision, you can request a review of the sanction in writing to the relevant senior member of the Trust management team who issued the sanction or via the PALs service.

Yours sincerely

Please note this yellow card warning has been recorded in your patient record. This helps ensure the safety of both you and staff and ensures that actions taken are documented accurately and securely.

*Sign and delete as appropriate

- Site Manager / Out of Hours Practitioner
- Clinical Director / Consultant
- Divisional Management Team
- Directorate / Care Group Management Team
- Local Security Management Specialist (LSMS)
- On Call Manager / On Call Director
- Senior Nurse / Ward Manager
- Matron

Enc Note: A copy of the Management of Violence & Aggression (MOVA) Procedure must be attached to this letter.

Appendix 4a

"Red Card" / Exclusion Procedure Checklist

1.0 Confirm the Red Card criteria and MoVA procedure has been applied correctly (Refer to section 2.7 of MoVA procedure outline)

2.0 The decision to exclude can only be taken by Chief Executive Officer on the recommendation of appropriate senior members of the Trust Management Team (as below) and once alternate care arrangements have been made. This does not preclude the relevant clinician discharging a patient who no longer requires in-patient care in the normal manner. Senior members of the Trust Management Team include:

- Site Manager / Out of Hours Practitioner
- Clinical Director / Consultant
- Divisional Manager
- Local Security Management Specialist (LSMS)
- On Call Manager
- Senior Nurse
- Matron

3.0 The Chief Executive Officer must be informed and is required to approve the letter to the patient and the letter to the GP. The relevant Department and responsible lead must also inform the Security Manager (LSMS), site managers and ED Manager.

4.0 The relevant Department and responsible lead must also inform the responsible consultant must be informed and write to the patient's GP detailing the exclusion and the reasons for it (See appendix 4c).

5.0 The patient must be informed that they may challenge exclusion via the established Patient Advice and Liaison Service (PALs).

6.0 A detailed record of the rationale for exclusion and of the alternative arrangements for care should be kept in the patient's health records including all relevant paperwork attached to this procedure.

7.0 If an excluded individual returns in any circumstances other than a medical emergency, security staff should be called immediately. The Trust will subsequently seek legal redress to prevent the individual from returning to the Trust property.

8.0 On expiry of the exclusion period of 12 months the "red card" will be removed from the Patients records unless there are grounds to consider an extension where there is continued non-compliance with the expected behaviours in the MoVA procedure.

Appendix 4b

Management of Violence & Aggression (MoVA)
Stage 3 – Red Card – Letter to Patient

Ref:
Date:
Patient's Name: …….
Patient's Address: …….
…….
NHS Number: …….
Dear …….
This is to formally confirm that due to your unacceptable behaviour on (date).....
At (location)……you are now subject to the conditions outlined in the Management of Violence & Aggression (MOVA) Procedure.

The third stage of the Procedure which is a Red Card has now been applied to you and you will have received an explanation as to why you are subject to this. Your GP will also be informed.

You will also have been given a copy of the Trust's Procedure entitled Management of Violence & Aggression (MOVA) Procedure for "Recorded Verbal Warning, Yellow and Red Card".

As you have failed to comply with the expected standards of behaviour explained to you by …….. and outlined in the Management of Violence & Aggression (MOVA) Procedure, you are now subject to the next stage of the procedure, which involves your immediate exclusion from the Trust premises by our security staff / police. Such an exclusion from Trust premises would mean that you will only receive emergency care and treatment at the Trust and your responsible clinician would make alternative arrangements for you to receive non-emergency care and treatment. The duration of this sanction is 12 months and will expire after 12 months where there is compliance with the expected standards of behaviour outlined in the MoVA procedure.

If you wish to challenge the decision, you can request a review of the sanction in writing to myself or via the PALs service.

Yours sincerely

Chief Executive

Please note this red card has been recorded in your patient record. This helps ensure the safety of both you and staff and ensures that actions taken are documented accurately and securely.

Appendix 4c

Management of Violence & Aggression (MoVA)
Stage 3 – Red Card – Letter to GP

GP name and address
Date

Dear Dr

Re: Patient name
Patient address
Patient's date of birth
Patient NHS number

The above individual was an inpatient on……. Ward at The Royal Wolverhampton NHS Trust/Walsall Healthcare NHS Trust.

In order to protect the healthcare environment for other patients and members of staff, it has been necessary to instigate a Management of Violence & Aggression (MOVA) Procedure which has resulted in the issue of a stage 3 Red Card to the above patient (see enclosed letter).

Such an exclusion from Trust premises would mean that the patient will only receive emergency care and treatment at the Trust and their responsible clinician would make alternative arrangements for them to receive non-emergency care and treatment. The arrangement made in this case are stated below:

•

The duration of this sanction is 12 months and will expire after 12 months where there is compliance with the expected standards of behaviour outlined in the MoVA procedure.

If you have any queries, please do not hesitate to contact:

……. [Name and telephone number of patient's consultant]

and / or

……. [Name and telephone number of Divisional Manager or Head of Nursing]

A copy of the Trusts procedure Management of Violence & Aggression (MOVA) Procedure is enclosed for your information.

Yours sincerely

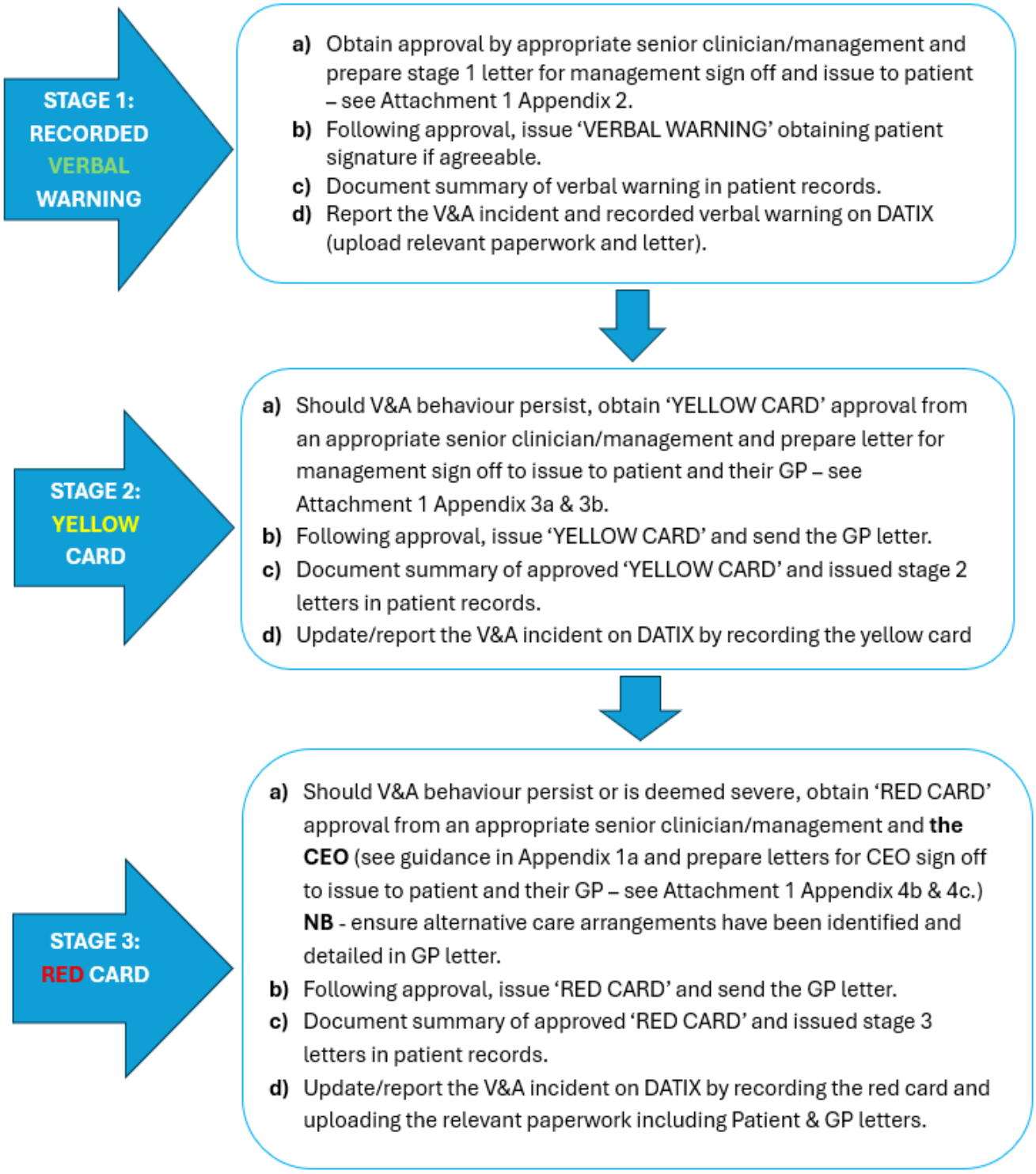
Chief Executive

Note: A copy of the Management of Violence & Aggression (MOVA) Procedure must be attached to this letter.

Appendix 5a: MoVA Flowchart - PATIENT RELATED VIOLENCE & AGGRESSION EVENT

IMPORTANT INFORMATION PLEASE NOTE – In implementing any stage of this flowchart, confirm age and clinical review criteria is met:

- If 'Yes' proceed as required.
- If 'No' and involving a **patient**, refer to Enhanced Supervision Policy.

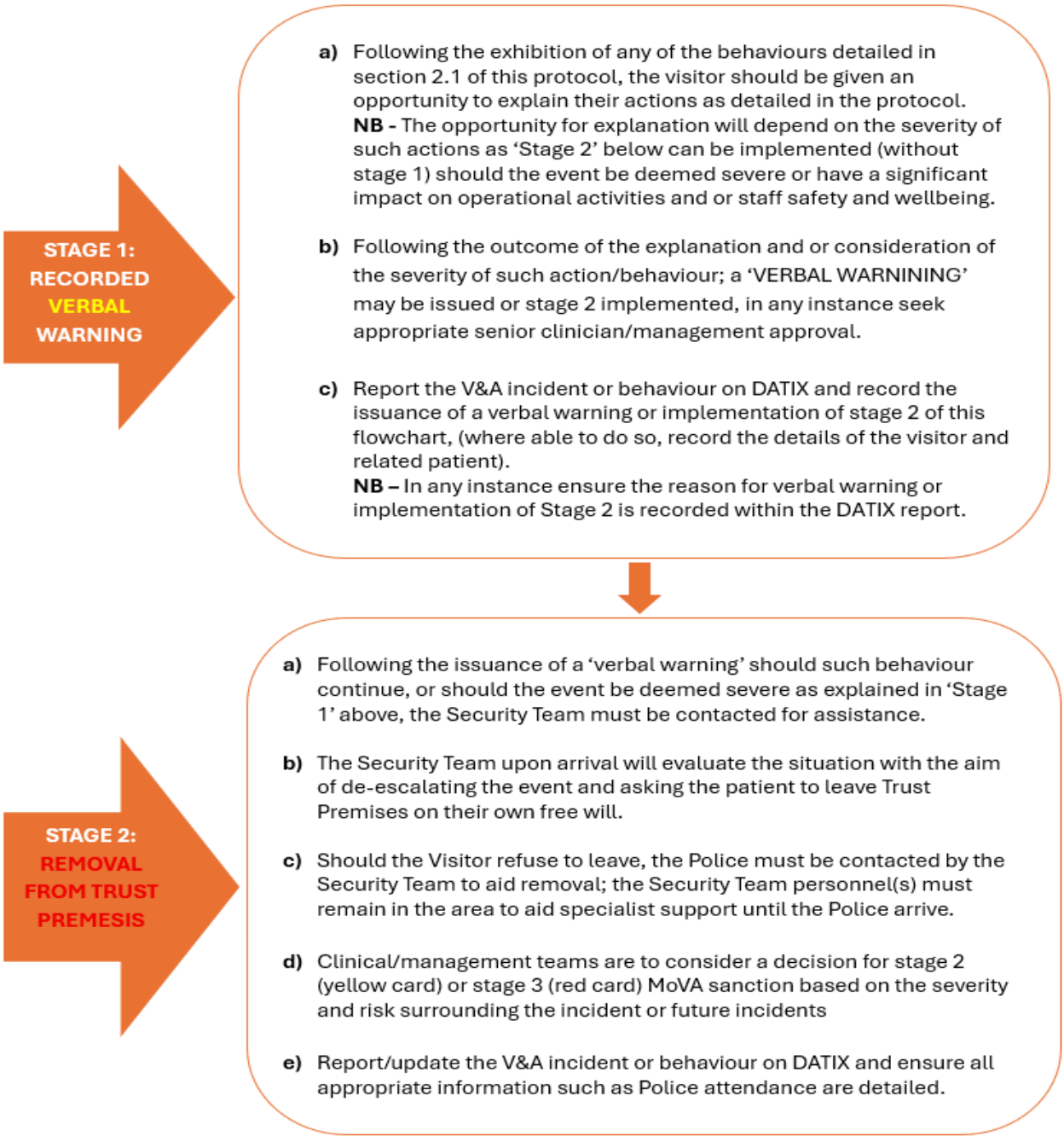


IMPORTANT - Copies of the signed MoVA letters for all stages of MOVA sanction must be sent preferably by email to the Local Security Management Specialist for recording on the electronic patient record system as an alert. Email to: paul.smith8@nhs.net, richard.jones26@nhs.net, thomas.bishop3@nhs.net OR by post to Security & Car Parking Management, Ground Floor Building 12, New Cross Hospital.

Appendix 5b: MoVA Flowchart - VISITOR RELATED VIOLENCE & AGGRESSION EVENT

IMPORTANT INFORMATION PLEASE NOTE:

- In implementing any stage of this flowchart, where able to do so obtain the name, age, and gender of the visitor as well as any related patient information or reason for being on Trust premises
- Where relevant, the behaviour of a visitor must not affect the treatment of the patient they are visiting.



IMPORTANT - Copies of the signed MoVA letters for all stages of MOVA sanction must be sent preferably by email to the Local Security Management Specialist for recording on the electronic patient record system as an alert. Email to: paul.smith8@nhs.net, richard.jones26@nhs.net, thomas.bishop3@nhs.net OR by post to Security & Car Parking Management, Ground Floor Building 12, New Cross Hospital.

Appendix 5c: MoVA - VIOLENCE & AGGRESSION INCIDENT INVESTIGATION FORM (for Incidents Involving Patients and Visitors and **Graded 'Low Harm or Above'**)

Section A – General Details

Datix Number:	**Date of Incident:**
Location (Ward/Dept/Areas):	**Time of Incident:**

Section B – Person(s) Involved

Victim (**Please Specify**): **Staff ☐ |Patient ☐ |Visitor ☐**	Victim's Name:
Perpetrator (**Please Specify**): **Patient ☐ | Visitor ☐**	Perpetrator's Name:

Section C – Existing Information

Was the perpetrator already on a sanction (recorded verbal warning / Red card / Yellow card) under the Management of Violence & Aggression (MOVA) Protocol?	**Response Yes ☐ | No ☐**	If **'Yes'** please specify: Recorded Verbal Warning ☐ **|** Yellow Card Issued ☐ **|** Red Card Issued ☐
If the perpetrator was not on a sanction prior to the incident; was a verbal warning, yellow card, or red card implemented post the incident?	**Response Yes ☐ | No ☐ | Already on a Sanction ☐**	If **'Yes or already on a sanction'** please specify: Recorded Verbal Warning ☐ **|** Yellow Card Issued ☐ **|** Red Card Issued ☐

Section D – Clinical Factors (if Patient Involved)

Was the patient's diagnosis, capacity, or medication a contributory factor to the incident?	**Response:** Yes ☐ | No ☐	Please specify:
Was a Verbal Handover given by the Nurse/staff from the transferring Ward to the receiving Ward?	**Response:** Yes ☐ | No ☐	Comments:
Where required, was there an accompanying '**Situation Behaviour Assessment Recommendation – SBART'** form sent with the Patient that had been completed in full?	**Response:** Yes ☐ | No ☐	Comments:
Where required, was the 'Enhanced Care Score' form completed in full?	**Response:** Yes ☐ | No ☐	Comments:
Where required, was there a Safety Huddle completed on the Ward for all Staff?	**Response:** Yes ☐ | No ☐	Comments:
Did the affected Staff Member attend the Safety Huddle on the Ward?	**Response:** Yes ☐ | No ☐	Comments:
Where required, was there a Hand Over completed on the Bay?	**Response:** Yes ☐ | No ☐	Comments:
Where was the Patient Bed allocated?	**Response:** Yes ☐ | No ☐	Comments:

Section E – Investigation Findings and Recommendation

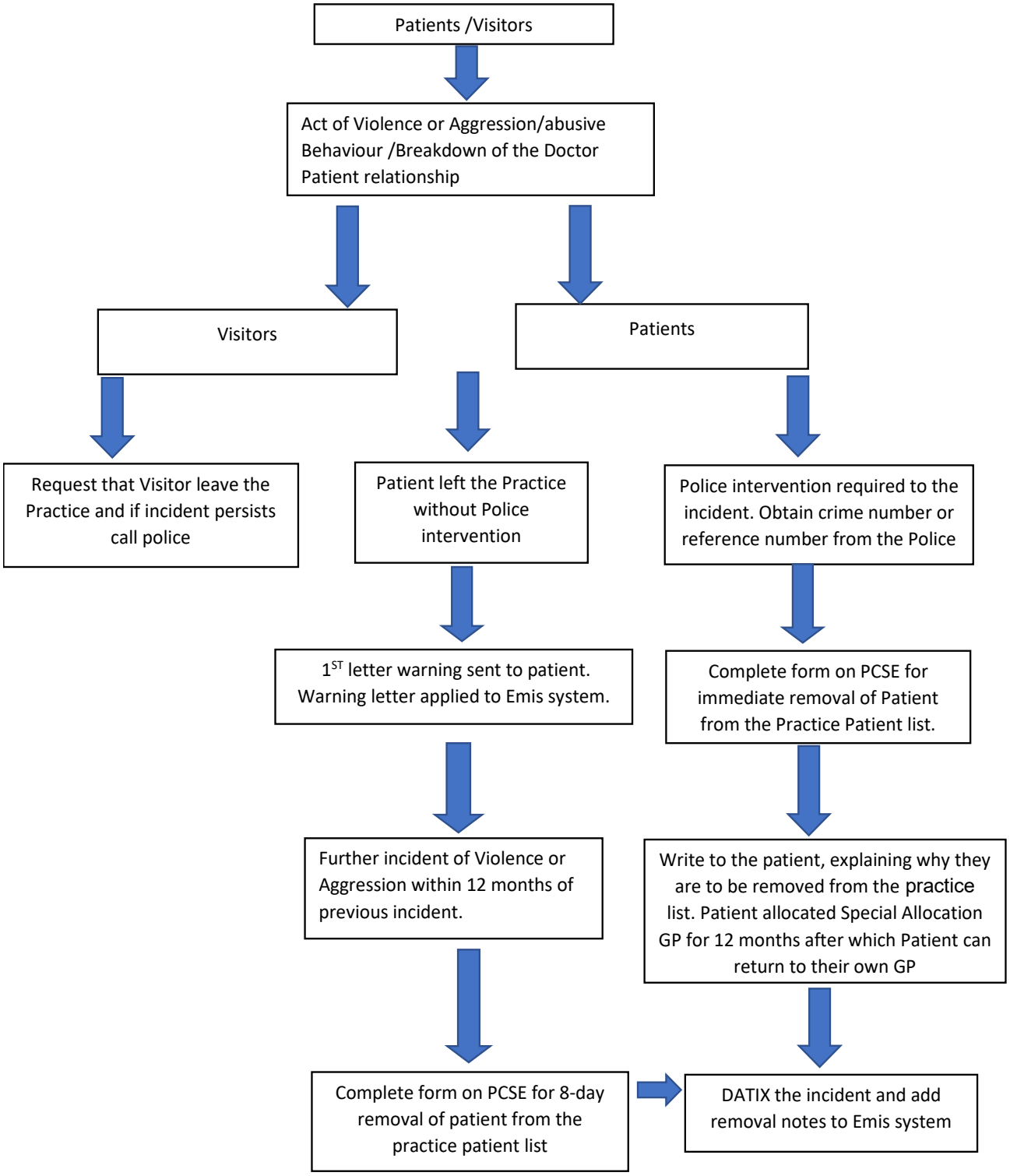
Findings:	**Recommendation:**

Section F – Investigator Details

Name & Role:	**Date Completed:**

Appendix 6

Primary care Act of Violence or Aggression against staff or other patients



Policy Reference: Security Policy

Title: Lone Working Procedure

Author: Local Security Management Specialist (LSMS)

1.0 Introduction

The Royal Wolverhampton NHS Trust and Walsall Healthcare NHS Trust recognise that lone working is a significant danger for staff. The Trusts are committed to creating a safe working environment for its employees by adopting systems and protocols within the Trust. All forms of aggression displayed towards staff, i.e. verbal abuse (including racial/sexual) and physical assault/threatening behaviour - will not be tolerated and wherever possible action will be taken against persons displaying such behaviour. Steps will be taken in all areas to meet statutory obligations placed upon the Trust (Health & Safety at Work Act Section 2), this will include doing all that is reasonably practicable to identify and control the risk of violence to its staff.

Furthermore, the Trust will strive to maintain compliance with Secretary of State Directions in creating a safer working environment for its staff by the delivery of de- escalation skills - Conflict Resolution Training.

The Trusts' overall aim is to:

- Assess and reduce the risk of violence, aggression or attack on staff.
- Take necessary steps to protect against all forms of violence, where possible
- Ensure employees are supported and provided with suitable aftercare or counselling following an incident of violent or aggressive behaviour.
- Fulfil legal obligations as outlined in the Health and Safety at Work Act
- Ensure the safety of its employees whilst at work.
- Lone Working arrangements will be developed among each staff group
- Ensure all staff receives Conflict Resolution Training

2.0 Purpose

To highlight the associated risks around concerns identified with lone working, not only in a community setting but all general working throughout the Trusts. The aim of this document is to highlight safety measures and precautions that can be taken by staff whilst carrying out Trust business.

3.0 Objectives

To raise awareness of lone working issues, the following are some of the risks that may result from lone working and to advise staff of precautions to be taken in some of the situations listed below.

The aim of this Procedure is to offer guidance and practical advice to staff that travel around the borough on Trust business – both in a clinical or non-clinical capacity, and to heighten staff awareness to some of precautions they should take whilst going about their

daily routine.

- Violence & Personal Safety – the nature of some work that some staff carry out may increase the risk of physical and verbal abuse. Some staff have also experienced contact with dangerous animals
- Incidents involving car related theft, carjacking, or a crash
- Lifting & Handling – attempting to move and handling tasks when alone may result in injury
- Fire – isolated workers may have difficulty evacuating buildings when the alarms are activated

Some of the high-risk activities undertaken by staff may include:

- Undertaking work in isolated areas
- Undertaking work within known high-risk areas
- Working alone at base
- Working with people with known risk factors, i.e., violence and/or aggression
- Staff carrying medication, equipment, or valuables
- Staff travelling between site/homes/offices
- Staff handling cash and/or banking

4.0 Duties

4.1 Duties Within the Organisation

Chief Executive

Chief Executive Officer (CEO), Chief Operating Officer (COO) leads the work with the Trusts' Local Security Management Specialist (LSMS) to tackle violence, aggression, and security issues within the Trust.

4.2 Specific Responsibilities

All Directors

Directors are responsible for ensuring that appropriate procedures and suitable precautions, including appropriate training, are in place to safeguard the health, safety, and welfare of lone workers.

4.3 Responsibilities of Other Staff Lone Working Arrangements

Managers

Professional judgement should be exercised regarding who should be required to work alone, this may include:

- Health professionals on home visits

- Ancillary/security staff working in buildings/offices/receptions/wards on their own
- Staff who work from home
- Staff working out of hours or returning to the site when on call
- Staff working separately from others
- Students in training
- Newly qualified staff
- Volunteers, etc.

Managers are responsible for:

- Raising awareness of this guidance throughout their departments and assessing the need to work alone
- Carrying out and reviewing suitable and sufficient risk assessments of all lone worker activities which have a potential to cause harm to employee/s
- Supporting those employees who have been involved in an incident and investigating such incidents and making recommendations to prevent recurrence
- Developing, implementing and ensuring the awareness of appropriate procedures and suitable precautions to account for, and trace the whereabouts of, lone workers and regularly checking that these procedures are followed
- Ensuring that systems are in place so that all information about patients referred from other departments/agencies is passed on, particularly if there is a known risk or previous history of violence or aggression
- The roll-out of appropriate information and training, to safeguard the health, safety and welfare of lone workers

Managers must take account of individual capabilities when allocating tasks to staff. However, work placement or other visitors to the trust should not be required to work alone. Irrespective of the working location of a member of staff classified as a lone worker, managers must ensure that the worker has the necessary capabilities, disposition, and training for working alone.

In addition, managers of staff who are working alone in the community must manage risks identified and associated with lone working, these include:

1. Provide mobile phones/replacement phones and personal attack alarms were deemed appropriate for use.
2. Ensure that there is a documented „safe system of work" in place for lone workers and that this is communicated to and understood by those involved.
3. Ensure that staff adopt a “Buddy” system, and that staff work together to establish their own individual whereabouts with colleagues/base.

4. Managers must also ensure that the departmental operational policy for their own specific team is updated to incorporate Lone Working protocol and procedure and also ensure that all staff are fully aware of the content of that policy.

5. Decide what supervision is required for lone workers and to what extent. This depends on the risks involved and the proficiency and the experience of the employee to identify and handle safety issues. Employees new to the job, and undergoing training whilst doing a job, which presents special risks, or dealing with new situations, may need to be accompanied and supported at first. Safety supervision may take the form of periodic visits to the lone worker.

All Staff

Where staff are considered to be 'lone workers' they must comply with risk assessments and safe systems of work and apply the following minimal standards:

Lone Working Risk Assessment

Lone working presents significant risks, particularly in environments where staff may face accidents, health emergencies, or aggression without immediate support. The absence of colleagues and systems can delay emergency assistance, increasing the severity of injuries or medical incidents. Employees working alone, especially in high-risk areas or during unsociable hours, may also be more vulnerable to verbal or physical abuse. Limited communication or supervision with lone workers can lead to heightened stress and mental health concerns. Without proper communication systems and risk controls, lone workers face an increased likelihood of harm, making proactive safety control measures essential.

Where applicable to a department or team, the Service Managers must ensure that the risks associated with Lone Working has been assessed using the appropriate designated form – Risk Assessment Profile 2. Identified control measures must be detailed in line with Group HS01 – Protocol 1 (Understanding the Trust Risk Assessment Process). All risk assessment must be shared with all staff.

Lone Working in the Community

1. Ensure that the mobile phone provided, or other security items, remain in working order and are always carried, ensure familiarity with the methods of use and in the event of failure/defect, advise the line manager immediately.

2. Follow the safe system of work for lone working, for the relative department, at all times, and ensure that any concerns relating to working alone are brought to the attention of the line manager or supervisor.

3. Work in conjunction with colleagues and management to identify, evaluate and reduce lone working risks (by using the risk assessment approach).

Lone Working on Trust Premises

- Review the work to be carried out, i.e. can the work be carried out at a different time, in an area where there are other workers

- Assess if the work does have to be done on Trust property and whether it be completed at home if possible.

- Obtain the authorisation of the line manager before working out of hours and, where practicable, let a colleague/someone at home know what the intentions are and give an instruction to contact the police if there is any concern

Community and Domiciliary Visits

Measures that should be taken to enable staff to work effectively without feeling threatened by isolation include:

Before undertaking community / domiciliary visits:

1. Undertake a risk assessment, that must be documented and made available to staff required to work with client or client group.

2. Patients and relatives must be contacted to agree an appointment time in accordance with patient's charter standards and given sufficient information about the reason for the visit/treatment. Ideally, a first visit should be carried out in two's, if possible, but not during hours of darkness.

3. Where possible, contact must be made with other health professionals or social workers to ascertain the patient's home environment and any prehistory before undertaking a home visit for a new patient, e.g. clinical history of disturbed behaviour, aggressive relatives, vicious animals, and investigation of complaints.

4. Where there is knowledge of a potential risk, if practicable, two health workers should visit together, e.g. Dietician and Health Visitor, District Nurse & Colleague etc. This is particularly important for an initial visit during which time a risk assessment for future visits must be made.

5. Itineraries containing information regarding the patient's addresses and times of visits must be left with a nominated person.

6. Suitable clothing should be worn, be aware that, it is recognised that the wearing of uniforms can sometimes bring unwanted attention, if needs be, cover the uniform by the wearing of a long coat. Trust Photo-ID badges must always be always carried and be available for inspection.

7. For their own safety, staff must ensure that their car is in good working order and have sufficient petrol for the return journey.

8. Providing information on the risks presented to staff by specific patients/relatives and on 'high risk' geographical areas, especially to new or deputising staff.

9. Adopting extra security procedures for visiting 'high risk' patients, and/or High risk' areas, especially on night visits and/or where female members of staff are involved.

Note – where there is doubt about the safety of a particular visit (geographical location, patient's condition, previous history of violence etc.) it may be more advisable to arrange for interviews/treatments to be carried out on NHS property or any appropriately agreed venue.

If this is not possible, consideration must be given to requesting that the police accompany staff for the visit. If the police are not prepared to accompany staff, or if the general view is that it is not beneficial to the health worker, i.e. for fear of reprisals later, then the visit is not carried out. This must be then documented and discussed with the line manager and if appropriate at a more senior level for decision regarding the future care of the client.

The decision to exclude a client can only be taken by a senior medic responsible for the patients care, in conjunction with relevant Trust Policy Security Policy/Management of Violence and Aggression Procedure (MoVA).

Whilst Working in the Community

1. Staff should not enter the premises of patients if they feel it is unsafe to enter, e.g. where there are vicious animals, unsafe buildings, etc., but should inform their supervisor or line manager or, if out of hours, the deputising manager or manager.

2. Drugs / valuable equipment must not be carried unless it is essential to the visit, but if carried must be left on view.

3. Where staff are working alone in an isolated clinic, another person should always be accessible, this will be via mobile phone, as well as there being an appropriate system for raising the alarm.

4. Staff must contact their base or nominated colleague at least once every two hours, to inform them that they are on duty in the community and if a lone worker fails to call in after two hours, the nominated colleague or line manager must make a welfare call to the worker's mobile phone.

5. If the lone worker fails to respond to the welfare call, the nominated colleague/line manager will attempt to contact the last person on the lone worker's appointment schedule. If it is not possible to trace the lone worker, the colleague will work back through the lone worker's appointment schedule to make contact/gather relevant information. The colleague may then ring the lone worker at home. If it is the end of the day, the lone worker's home telephone number should be tried prior to working back through the appointment schedule.

6. If the lone worker cannot be traced, the nominated colleague must inform the worker's line manager. If there is cause for concern, the police must be contacted and requested to visit the patients' homes. An incident report form must be completed and forwarded to the designated manager.

Staff Working in Isolated Areas

Staff working alone and/or in isolated areas of Trust property will encounter similar issues as those working in the community or carrying out domiciliary visits.

Staff are to be encouraged to ensure that locations are secure and that a locking up/opening procedure is followed to secure the building/area in which they are required to work. Other measures taken because of a risk assessment might include:

1. A review of work carried out by the member of staff, i.e. can the work be carried out at a different time, in an area where there are other workers.

2. If the work must be carried out in the location, it is possible to move another worker into the location both to provide company and greater sense of security.

3. Fitting a security alarm that can be activated by the member of staff.

4. Initiating a regular reporting system, for example initiate a “Buddy System” with colleagues in other areas.

Control of Contractors

The local management should always be aware of the location of contractors. Outside

Contractors should be issued with visitors I.D. badges whilst working on Trust property.

HIGH RISK VISITS

Where there is a history of violence, concerning the patient or site location that is deemed a high risk, the lone worker **must** be accompanied by a colleague. Where it is possible, the visit should take place at a neutral location or within a secure environment.

Lone workers should mentally carry out a “10 second” risk assessment when they first arrive at a patient's address and the front door is opened. If they feel there will be a risk to themselves, they should have a readymade excuse available so that they do not have to enter the property and tell the patient that an alternative appointment will be made.

4.4 Responsibilities of Specialist Staff

Local Security Management Specialist (LSMS)

The LSMS is responsible for:

- Liaising with the local police in the event of a physical or nonphysical assault to assist with any investigation
- Undertaking an investigation, feedback to the victim on the progress of any police or LSMS investigation into physical or nonphysical assault
- Providing security advice
- Assisting managers to carry out risk assessments of selected sites where lone workers are based
- Sending letters to offenders of physical and nonphysical occurrences towards staff, copy of letter to be sent to the line manager for their records

4.5 Responsibilities of Key Committee and Boards

Trust Board

The LSMS produces an annual Security report for the attention of the Board. This document highlights the number of reported incidents of physical and nonphysical occurrences to staff. It also documents and advises the Board of any improvements that have been made to enhance the safety of lone working staff (devices/protocols). This report is also shared with the NHS Security Management Service and the Health & Safety Executive (HSE).

Health & Safety Group

Will regularly receive Security performance and assurance reports from LSMS including progress on action plans developed from risk assessments and to reduce incidents of physical/non-physical abuse.

Through Security reports provided to the Health and Safety Group, the LSMS/Security team disseminate relevant information concerning lone working down to Divisions and well as direct liaison with their local Directorates/Care Groups.

5.0 Definitions

5.1 What is Lone Working

A worker is defined as a member of staff whose terms and conditions of employment require him or her to work alone, or who has been authorised by their manager to work alone, as an exception to their normal duties lone workers may be working away from their base within the community, e.g. district nurses, health visitors etc. Alternatively, lone working may take place on trust premises e.g. certain on call staff or, an office worker working late/during a weekend to meet a deadline in exceptional circumstances, and maintenance staff working on call, late at night.

It is recognised that, in accordance with the Trust's duties under the Health & Safety at Work Act 1974, establishing safe working arrangements for lone workers is no different from managing the safety of other employees. Employees duties under the Health & Safety at Work Act of 1974 state that the employee has a duty to take reasonable care of themselves and other people affected by their work. They are to co-operate with their employer with respect to any procedures or systems that are put into place to protect lone workers.

The Trusts recognise that lone working is potentially more hazardous than working with others. The practise of lone working should be questioned by managers, and if it is essential, it must be subject to risk assessment in accordance with the Management of Health and Safety at Work Regulations 1999 and measures put in place to minimise the associated risks. Staff working alone may be particularly at risk from violence and aggression.

Supporting Legislation

Secretary of State Directions

NHS healthcare organisations have responsibilities to manage security, which includes the protection of lone workers in accordance with the Directions to health bodies on measures to deal with violence against NHS staff and Directions to health bodies on security management measures, 2003 and 2004 respectively and as amended 2006.

Health and Safety at Work Act 1974

NHS healthcare organisations have responsibilities under the Health and Safety at Work Act 1974, particularly in relation to employers ensuring, as far as is reasonably practicable, the health, safety and welfare of employees at work.

Employers should have written policies setting out their arrangements for managing health and safety risks. These policies should be publicised and easily accessible to staff.

The Management of Health and Safety at Work Regulations 1999

These regulations require employers to assess risks to employees and non- employees and make arrangements for effective planning, organisation, control, monitoring and review of health and safety risks.

Where appropriate, employers must assess the risks of violence to employees and, if necessary, put in place control measures to protect them.

Safety Representatives and Safety Committees Regulations 1977(a) and the Health and Safety (Consultation with Employees) Regulations 1996(b)

Employers must inform, and consult with, employees in good time on matters relating to their health and safety. Employee representatives, either appointed by recognised trade unions under (a), or elected under (b), may make representations to their employer on matters affecting the health and safety of those they represent.

The Corporate Manslaughter and Corporate Homicide Act 2007

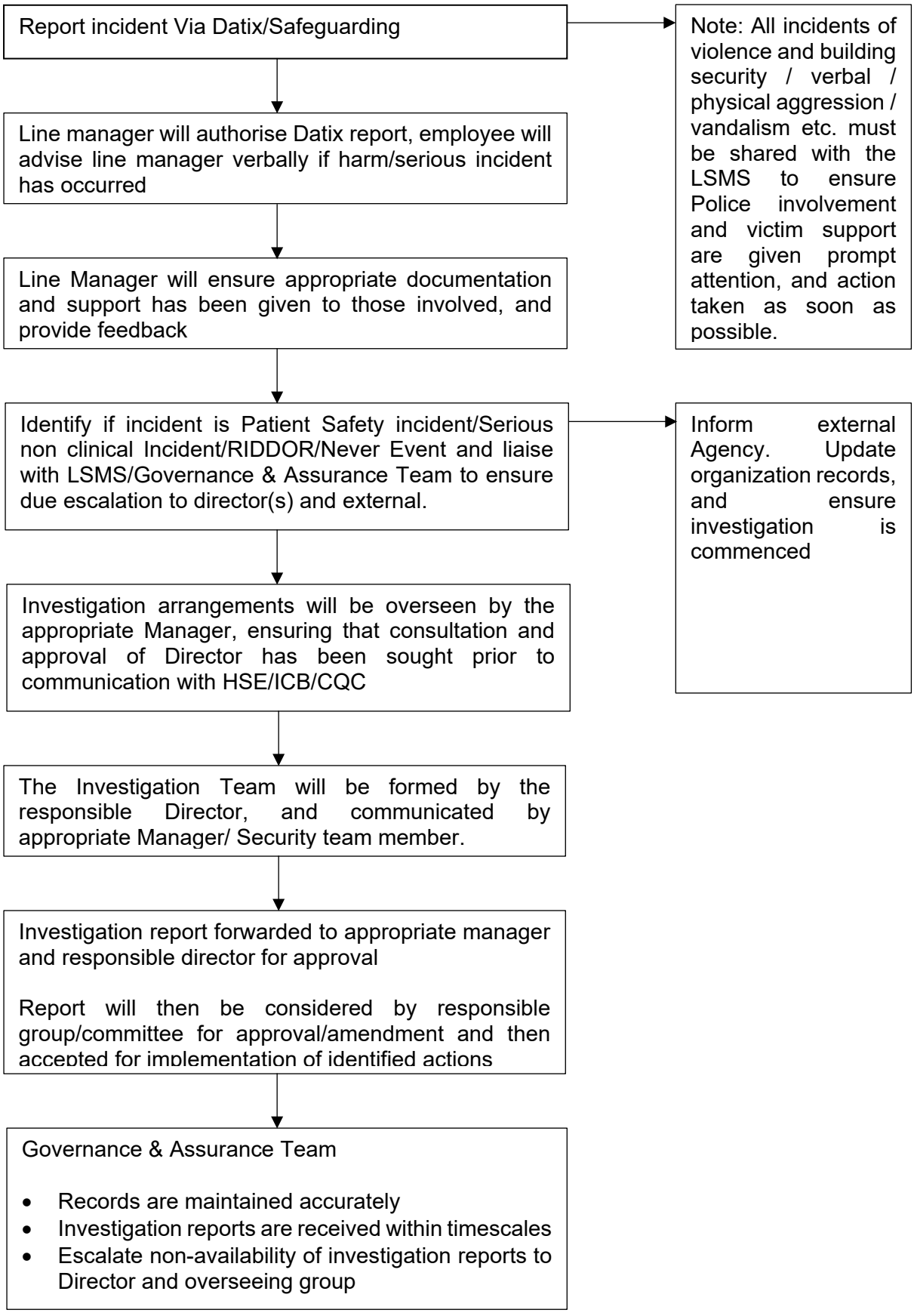
Under this legislation which came into force in April 2008 an organisation (rather than any individual) can be prosecuted and face an unlimited fine, particularly if an organisation is in gross breach of health and safety standards and the duty of care owed to the deceased.

5.2 Consultation

This document will be distributed for initial consideration/comment to the Health & Safety Group; the Health & Safety Group will be responsible for approval and ratification of the policy. Following ratification at Policy Group, final approval will be sought from the Trust Board.

5.3 Incidents of Violence and Aggression – The Process

Action to be taken: Employees / Visitors / Services / Contractors



6.0 Lone Working Arrangements

Safe Systems of Work

A Safe System of work is a defined method for doing a job in a safe way. It takes account of all foreseeable hazards to health and safety and seeks to eliminate or minimise these. Safe Systems of Work are normally formal and documented, e.g. In written operating procedures but in some cases they may be verbal.

It is the responsibility of the directors, line managers, locality managers and supervisors to ensure that its operations are assessed to determine where safe systems of work need to be developed/implemented.

Safe Systems of Work must be properly documented, communicated to staff and wherever possible they should be incorporated into normal process operating procedures. Records should be kept of the documentation so that amendments or updates can be made when a revision of the Safe System of Work is due.

7.0 Risk Associated with Lone Working

The following are some of the risks that may result from lone working:

- Violence and personal safety – the nature of some work that staff carry out may increase the risk of physical and verbal abuse. Some staff have also experienced contact with dangerous animals
- Incidents involving car related theft, carjacking or a crash
- Lifting and handling – attempting to move and handling tasks when alone may result in injury
- Fire – isolated workers may have difficulty evacuating buildings when the alarms are activated

Some of the high-risk activities undertaken by staff may include:

- Undertaking work in isolated areas
- Undertaking work within known high-risk areas
- Working / visiting patients in their own home
- Working alone at base
- Working with people with known risk factors, i.e. violence and/or aggression
- Staff carrying medication, equipment or valuables
- Travelling between site/ homes/ offices
- Staff handling cash and/or banking

8.0 Development Plan

This policy was initially designed to reflect good practice which is in use throughout the NHS and other organisations to help protect staff that work alone and do not always have access to immediate support from colleagues or others when they are faced with difficult or hostile situations.

This Policy has been developed in line with guidance from the NHS Security Management Service also with constructive comments from Health & Safety Committee.

9.0 Performance Management

The LSMS monitors incidents of a physical or verbal nature to Staff daily.

NHS Security Management Service receives on an annual basis a
Violence Assault Statistics (VAS) report. This report is for National Statistical purposes and contains information concerning physical and non-physical reported incidents within the Trust.

Other stakeholders who monitor performance in tackling physical/verbal incidents towards staff are the Health and Safety Executive and the NHS Litigation Authority.

Appendices

Appendix A

Guidelines for Staff Working Alone Within an Office During Working Hours

Wherever possible this situation should be avoided; where it is unavoidable, staff must:

- Ensure that they are near a telephone to call for help if needed
- Make sure their working areas are safe; be particularly careful in layout of furniture and equipment; ensure no potential weapons are lying around
- Ensure their manager/colleagues know they are working alone and know where they are working alone
- Secure valuables in an appropriate place
- Ensure that keys are secured and not accessible to visitors
- If they become anxious regarding their safety, call security (where appropriate) or emergency services for help
- Avoid meeting people if they are alone in the workplace
- If they are meeting someone, let other people know who they are meeting, when, where and telephoning them to let them know that X has arrived and that they will get back to them at a certain time
- Do not let visitors place themselves in front of the exit point
- Do not tell any potential visitors/external persons that they are alone in the workplace
- Report any incidents or near-misses to the relevant manager as soon as practical after any events
- Ensure that all windows and doors are secured to prevent unauthorised access, so that the working environment is as safe as possible
- Do not open doors to any strangers no matter what identification they have; if they are meant to be there, they will either have keys or another means of access
- Never give security codes or keys to any stranger; again, there are channels they can use to gather information if they are legitimate and are meant to have access Make sure fire escape routes are available and not locked (they might be locked outside normal working hours).
- Do not use lifts at these times, as they may become trapped inside and unable to gain assistance or attention
- If the fire alarm activates whilst inside the office alone, leave the building immediately by the nearest fire exit; go to the front of the building, a safe distance away and wait for the

emergency services to arrive

- Do not attempt to repair or tamper with the controls if any problems with equipment are discovered whilst alone in the office; if it is not serious, report it to the manager the following working day
- On leaving a department, ensure that all windows are closed and doors locked
- Ensure access to a phone in case of need to call the emergency services
- Park as close to the building as possible, in a well-lit area to minimise the risks if leaving the building alone
- If an incident or near-miss occurs, follow the Trust's Incident Reporting Procedures

NEVER ASSUME IT WILL NOT HAPPEN TO YOU – PLAN TO STAY SAFE

Appendix B

Guidelines for Staff Working Alone Within a Department Outside Office Hours

From time to time, staff may need to carry out their office-based work outside of normal office hours, such as weekends and evenings. The following precautions, aside from those described in Appendix A for those working alone in an office within office hours, must be taken to ensure that health and safety of staff continues to be protected outside office hours:

- Where applicable, let main reception, or your “Buddy” know that you are staying behind in an office at the end of the normal working day, so that they will know to check on you before they leave

- If you are working at weekends or very late at night/early in the morning let a friend or relative know your whereabouts and the time that you are expected back. Contact them at regular intervals to verify that you are okay. If your plans change, let your contact know immediately

- Where applicable, liaise with other staff on site, who in turn should liaise with anyone else in the building about estimated exit times, their whereabouts during extended hours and when they plan to leave the building

- Where applicable, when there are only two members of staff left working and when one is ready to leave the other will also be required to cease working so that they can exit the building together

NEVER ASSUME IT WILL NOT HAPPEN TO YOU – PLAN TO STAY SAFE

Appendix C

Guidelines for Lone Working Off Site

When making lone worker visits it is important to communicate with others about your intentions during the delivery of your services within the Trust.

You must inform a colleague of:

- The location of the visit or meeting where you are attending
- A contact telephone number, if possible
- The time of the appointment
- The likely or estimated length of the meeting or visit
- The time when you are expected to return to the office, base or call in
- If not returning to the office, the time and location of your next visit or the time when you are due to arrive home
- If driving, car make, registration and model
- Colleagues may be aware of issues that you are not, and vice versa; you should always provide and ascertain as much information as possible about an appointment, use the list below as a reference
- Do you need physical support from another colleague during the visit?
- Is it necessary to carry a personal attack alarm with you?
- Is your mobile phone fully charged and does it have satellite coverage and signal reception?
- Do you have any credits on your phone or spare change or a phone card in case of emergency?
- Can you park your car (if using one) close to the visit address without putting yourself at risk, i.e., in a darkened road or cul-de-sac?
- Is it necessary to have an exit strategy in the event of an emergency arising?
- Do you require directions/a map of the area? Know your route and avoid the need to ask strangers for directions
- Do not take short cuts when driving – stick to main roads where possible
- Accessibility of the off-site place of work and whether there is public transport within easy walking distance
- Take additional precautions in inclement weather – ensure warm, waterproof clothing is in the car plus a snack and a drink and consider whether your journey can be re-scheduled

NEVER ASSUME IT WILL NOT HAPPEN TO YOU – PLAN TO STAY SAFE

Appendix D

Guidelines for Visiting Patients in Their Own Homes / Premises

In addition to the precautions described above (lone working off site), visits to a patient's home represent a series of risks which a lone worker and the Trust should aim to minimise. Visits to a patient's home must only take place when it is impossible for them to come to Trust premises for attention, this may be due to their physical or mental state Before making a home visit alone, the member of staff should assess the risks and ascertain whether it is safe enough to attend alone. The assessment must be fully documented where there is a residual risk which cannot be controlled; this should be agreed and discussed with the Department Manager, shared with all relevant staff and always available to them. If there are any concerns regarding the safety of a particular home visit, either a colleague should accompany them, or the visit should be rearranged to a time when the risks can be minimised.

This guidance is designed for all staff who visits patients within their own homes. Prior to a home visit taking place, staff must:

- Obtain as much information as possible about the patient, their families and location to be visited; this can be done via the Violent Persons Data Base (Community Staff) – if you do not have access to this, get your Manager to check for you
- Review the last documented risk assessment, or if this is unavailable, contact the referrer to ascertain whether there are any relevant risk factors present and/or whether there is any reason why it would be unadvisable to visit the client alone; It is best practice to design referral forms to your department so that they automatically capture such information
- Double check the address and telephone number
- In the even of a call-out, check the authenticity of the call
- In the event that no records or information is available, reschedule for another time, when you have been able to gather all relevant information

If it is decided that a home visit is required, staff must:

- Consider whether visiting the patient presents potential high risk
- Consider whether it would be appropriate to arrange to have a second staff member present for the duration of the visit
- Always ensure that fellow workers know where you are; details should include expected time of return, names and addresses of the patients being visited and time of appointments when visiting alone, mode of contact (i.e., mobile phone number, patient's phone numbers), by completing the log sheet at Appendix B of this policy
- Make sure that you carry appropriate personal identification, i.e., name badge, ID card, to verify your authenticity
- Dress appropriately for the area or patient to be visited, particularly when the patient's culture demands that women are covered; do not wear expensive- looking jewellery items and consider wearing shoes and clothes that do not hinder movement or the ability to run in case of an emergency

- Ensure that the means of communication and any personal attack alarms are working and accessible, i.e., keep mobile phone in pocket of clothing worn as opposed to at the bottom of a bag; programme the work base number and any emergency numbers into mobile phones so that they can be speed dialled

In any home situation there is the potential for violence or aggression, whether from a patient or a patient's family or friends. Such risks can be higher where:

- There is a previous history of violence and aggression
- Drug and alcohol are involved
- Disputes or stressors exist within the home setting
- The nature of the home visit may cause perceived threat or anger
- Disputes exist between the patient/family and member of staff, or any other statutory body
- There are unpredictable elements, i.e., confusion or disorders of perception

En route to the home visit, ensure:

- Ensure the vehicle is well maintained and has sufficient fuel and that you are covered by a suitable breakdown service
- Bags, drugs and equipment are concealed and cannot be seen when the vehicle is parked or on route
- You only carry to individual appointments equipment that is needed

Consider:

- The time, the location and the route; take particular care in high rises, noting exit routes
- Locking the car whilst driving and waiting
- If you are you being followed or feel uneasy, remain with or return to your vehicle and drive away for a short while to a place of safety
- If you are away from your vehicle, cross the street and make your way to your vehicle or towards shops or other place of safety, whichever is closer
- If suspicions are confirmed, use your personal attack alarm and contact the police

TRUST YOUR INSTINCTS – YOUR PERSONAL SAFETY IS PARAMOUNT

On arrival:

- Be alert, aware and look confident. Know where you are going, walk tall and keep your head up
- Park with care – as near to the address as possible in a lit area away from subways and waste ground, in a position prepared to drive away quickly in an emergency, i.e., not facing into a cul-de-sac

- Always lock your car, when leaving it
- Keep your car keys about your person so that they are accessible in an emergency
- Do not leave nursing equipment/valuables in your car on show
- Assess the situation on approach and be prepared to abandon or postpone the visit if there is a concern for safety
- Have identity badges available on request
- If the person answering the door makes you feel uneasy about entering, then an excuse should be made not to enter. For instance, when the patient or relatives are aggressive, drunk or 'high' on non- prescribed drugs
- You should follow the occupants in when entering and not take the lead
- Remain alert while in the house – look for anything that may present a problem
- When taking a seat within the property, ensure you are near an exit route and be aware of entrance/exit points
- Be aware of any obstacles that may prevent you from exiting the premises quickly
- Be aware of any potential weapons lying around and ensure that your own equipment is not within any potential aggressor's reach, if it has the potential to be used as a weapon, i.e., scissors, scalpels
- Consider other people present during the visit and what introduction is necessary
- If it is possible that a rapid exit may be necessary, avoid spreading equipment out
- If the situation deteriorates during a visit, consider terminating the visit, perhaps by making an excuse, and leave – trust your instincts - your personal safety is paramount
- If useful, consider phoning your base on a pretext, explaining your whereabouts, so the patient recognises that you are in contact and your whereabouts are known
- Have a recognised departmental password to inform colleagues covertly if you are in danger
- If an animal is causing concern, speak to the owner to enlist their co-operation. If co-operation is not forthcoming, consider terminating the visit and leaving

If in doubt:

- Do not enter premises
- Plan your action

IF VIOLENCE IS THREATENED - LEAVE IMMEDIATELY

Personal Safety

- Park in well-lit areas
- Do not take short cuts off main, well-lit pavements
- Walk facing oncoming traffic
- Avoid rowdy groups of people
- Carry a torch in the dark
- Have a personal attack alarm readily at hand

On return to the car:

- Have your keys ready
- Check the exterior/interior before getting in
- Lock the doors as soon as you get in
- Do not waste time by putting things in the boot – you can do this once you have left the area, and it is a safer environment
- Check back with the team following a home visit
- If, for whatever reason, you find you will not be back at the expected time you must ring and let colleagues know of any alterations
- If you have to make a first visit at the end of a shift, ensure that you have a mobile phone, and report back to base or to another designated person – use the “buddy” system
- Review any risk assessment carried out; record any perceived risks and discuss with your manager and colleagues; review care plans accordingly

Known High Risk Home Visits

- If any visit is deemed to be a potential high risk, it may be necessary to visit in pairs and/or request a police escort. The need for such additional support should be discussed with your manager so that appropriate arrangements can be made
- For such visits, it is recognised as good practice for staff at base to contact the employee mid-visit (instituting emergency procedures if contact cannot be made or a covert password) and for the employee to report back to their work base to confirm that the visit has ended and that they have safely left the patient. A record must be made of the times entering and leaving the patient’s home

Warden Controlled

If visiting a patient, known to be potentially verbal or aggressive in their behaviour towards Trust staff, and they reside in a Warden Controlled Scheme, it may be advisable to approach the Warden to establish if they would escort you on the visit, if working in twos is not possible.

If possible, arrange any further visits to the patient with the Warden in attendance, if they are

not able to do this, ensure that the Warden knows of your visit, and roughly how long you intend to be with the patient – give a positive time scale so that they can attend should you fail to inform them of your leaving after the agreed time.

Appendix E

Dealing With Animals

- If a lone worker is confronted by an aggressive animal on a first visit to a patient's home address, they should cancel the visit and inform their line manager of the problem – this should also be treated as an incident and the appropriate incident form must be filled in.

- If the problem with animals is known, the patient should be contacted prior to the visit, and asked politely, if they would remove or secure the pet before arrival – Clinical procedures can provoke a hostile/protective reaction from animals if they think their owner is being harmed.

- If the lone worker is not happy with animals being present when a visit is taking place, the above protocol should be followed.

- All possible efforts should be made when dealing with these situations so that by asking for the removal of a pet it does not provoke a negative reaction with the patient.

- All efforts should be made to ensure that the situation is managed and de- escalated should any hostilities become evident.

- If this is not possible, an alternative arrangement must be made – rescheduling perhaps so a fellow colleague (who is at ease with animals) can accompany the lone worker on the visit.

Appendix F

Interviewing / Treating Patients in the Office / Clinic

In addition to advice already given earlier in this document, when interviewing/treating in the office/clinic, consider the following:

- Use interview/treatment rooms with panic buttons where possible
- Make sure your working areas are safe; be particularly careful in layout of furniture and equipment ensure no potential weapons are lying around; ensure that your own equipment is not within any potential aggressors reach, if it has the potential to be used as a weapon, i.e., scissors, scalpels
- Sit nearest the exit
- Ensure that you are aware of locks, bolts on doors, exits, etc., and observe how they work
- Ensure that colleagues are aware that an interview/treatment is taking place
- If there is ever a need to take a patient/visitor through a coded security door, ensure that they do not see the code or knock on the door to allow main security to let you through

Appendix G

Travelling on Foot

- You have a better chance of escape from a potential attacker by wearing clothes that you can easily move in and shoes that are comfortable
- Keep your valuables in an inside pocket or concealed on your person – bum bag for example – this enables you to keep both hands free
- If possible, women should carry their handbags with the strap slung across the body, and if further possible, concealed under outer clothing
- Always ensure you know where you are going – plan your route before you leave base (RAC Route Planner is available on the intranet and is free to use)
- If someone attempts to steal from you, relinquish your property immediately, without challenge
- Consider keeping your mobile phone, house keys, wallet/purse away from your bag - a good trick is to carry an old wallet/purse in your bag with a few coins in, an old phone along with expired credit cards, this gives the robber the impression they have been successful in the robbery
- When walking, you should stay in the centre of the footpath, facing oncoming traffic
- Avoid at all costs any waste ground, isolated pathways and subways – particularly at night
- When you have reached your destination let your „Buddy" know you have arrived and are safe

Appendix H

Lone Working and Taxis

- Wherever possible, the taxi should be booked in advance from a reputable company
- If a taxi has not been booked, the lone worker should go to a recognised taxi rank to hail a taxi
- NEVER use a mini cab, unless it is licensed, or it is a registered hackney carriage
- Sit in the back, behind the front passenger seat
- DO NOT give personal information about you to the driver, either by conversation with the driver, or if you are using your mobile phone
- Be aware of child locks and central locking mechanisms – most black cabs will lock the doors whilst in transit
- When you have reached your destination let your “Buddy" know you have arrived and are safe

Appendix I

Lone Working and Public Transport

- Always wait for transport at a busy stop or station that is well lit
- Check timetables before you leave
- Try and sit as close to the public vehicle driver as is possible, preferably in an aisle seat
- Avoid empty upper decks on buses, or empty train compartments – also avoid these areas if there is only one other passenger
- If threatened by other passenger(s) inform the driver or guard
- When you have reached your destination let your “Buddy“ know you have arrived and are safe

Appendix J

Transporting Patients in Your Own Vehicle

The Trust operates a patient transport service which includes the use of non-emergency ambulance, or taxi.

This provision should be the first consideration at all times, rather that staff transporting patients in their own vehicles.

Please see Non-Emergency Patient Transport Services Policy available on the Trust Intranet page.

Before a decision is taken to convey a patient/service user, a full risk assessment should take place. This should consider the safeguards that need to be in place before and during the escorting process.

Consideration should be given to the physical and mental state of the patient when planning to drive, and to whether they are capable of being transported, and it is safe for you to do so.

The level of staff experience and their qualifications, and the number of staff needed to manage the patient during the transfer should be considered.

Lone workers should not escort a patient by car if there are any doubts about their safety in doing so and alternative arrangements should be made. Lone workers should not agree to transport a patient's animals.

If there is a need for a lone worker to convey a patient in their own vehicle, they should always seat the patient behind the front passenger seat and ensure that their seat belt is fastened. This will enable the lone worker to operate the vehicle safely. There have been reported incidents of patients seated as front-seat passengers grabbing at handbrakes and steering wheels while being transported.

If a conflict arises (or a patient becomes aggressive), the lone worker should pull over into a safe place and exit the vehicle – if possible, ensuring that the keys are removed. They should follow local procedures, which may involve calling the police, their manager, a colleague or their buddy.

Appropriate planning and provision should be made for the safe return of a lone worker to a familiar place, once the patient has been dropped off. This is particularly important if the lone worker has to return from an unfamiliar place late at night and travel to their place of work alone.

Appendix K

Staff Whereabouts Procedure

All buildings and departments must have a means of recording staff whereabouts whether this is simply to indicate whether at work that day, absent or attending a meeting/visit away from their usual place of work. All departments should question whether a visit is necessary and if so are adequate controls in place to safeguard the staff conducting the visit. There are a number of ways in which this can be achieved and a sample procedure would consist of the following information:

1. Where and when to access the booking in and out record (record book held at reception, phone call to Team Leader, text message etc.).

2. The type of information that is required (name, location of visit, time out, time of return, emergency contact).

3. Special requests/requirements (including check call, use of code word, planned interruption).

4. Failure to Return to Base Details (who will check if someone hasn't returned when they had indicated).

5. Sickness/Holiday Cover (who will buddy or cover for a point of contact when they take leave).

6. The procedure should be communicated to all staff and suitability/effectiveness reviewed at regular intervals.

7. Regular progress reports and discussions should be held at local Risk Action Groups and incident statistics reviewed to take account of safe systems of work and incident management.

Appendix L

When a Colleague Does Not Return as Expected

If one of your colleagues has not returned to the office or rung in to confirm their whereabouts, then the first and most important thing is to remember not to panic! It may be that they have genuinely forgotten to let you know of changes to their plans or have been delayed.

- Ask your colleagues whether they have heard from them or have been properly informed of changes to their plans
- If not, ring their mobile phone number and check to see that they are safe – remember your code word
- If you receive no answer, or if they answer but sound distressed (in this latter instance call the police before taking any further steps), then you should notify their manager immediately. If they are not available, notify the most senior person on the premises
- If it has not been possible to obtain an answer from their mobile, the Manager should then try to contact them at home or through their next of kin before contacting the police
- In cases where the person answers but appears to be in distress, the police should be called immediately
- A password for recognising a potentially dangerous situation needs to be discussed throughout individual teams. It needs to be something that will not arouse suspicion, i.e. “I am picking Mothers flowers up later” or “it is in the blue folder”.

Appendix M

Lone Working in Adult Community and Primary Care Settings

Standard Operating Procedure

1. Objectives

- To ensure staff are adopting safe working practices in line with the Trust Lone Worker Policy (Security policy – Attachment 3) and any additional service specific guidelines.
- To highlight the associated risks around concerns identified with lone working including (but not limited to) the following high risk activities:
  - Undertaking work in isolated areas.
  - Undertaking work within high-risk areas.
  - Working/visiting patients in their own home.
  - Working alone at base.
  - Working with people with known risk factors i.e. violence and/or aggression.
  - Staff carrying medication, equipment or valuables.
  - Staff travelling between site/homes/offices.
  - Staff handling cash and/or banking.

2. Scope

All Adult Community and Primary Care Services staff (*including all management and admin staff*).

Lone workers who provide services in more than one location or who work between sites will be issued with a personal safety device to offer enhanced protection when working away from their base.

3. Staff Responsibilities

On any occasion where a member of staff can be a lone worker, it is their responsibility:

- To assess and reduce the potential risk of violence, aggression or attack and to take necessary steps to protect against all forms of violence
- Ensure Conflict Resolution training has been completed. Bespoke Conflict Resolution Training/Lone Work Awareness training is available on request from the Security Management Team
- Ensure equipment is working (including any personal safety devices and mobile phones)

4. Management Responsibilities

- Ensure staff are released to undertake training
- Provide staff with personal safety device
- Contact police/emergency services immediately as appropriate

5. Prior Considerations

5.1 Adult Community and Primary Care Referrals

Home visits should only be offered as an exception rather than the rule and the following reasons for home visits have been agreed:

- Patients that are truly housebound in line with The Walsall Healthcare NHS Trust Elective Access Policy, Including DNA (Did not attend) Guidance
- The patient has a debilitating progressive or general illness and is not well enough to attend a clinic appointment
- Intervention is best provided in the home setting for clinical reason

All new referrals will be screened for background information which may indicate a potential risk.

All referrals will be checked against the Trust's PAS/EMIS for alerts/warnings. Where there is a history of violence concerning the patient or site location that is deemed a high risk, staff must work in pairs. Where possible, the visit should take place at a neutral location or within a secure environment, for example, health centre/GP practice.

Alteration to staff uniforms will be permitted where there is a perceived or known risk (e.g. wearing polo t-shirts in place of tunics). If there is continued violence/aggressive behaviour to staff then the Walsall Healthcare NHS Trust Security Policy (Attachment 2) is to be followed. Escalation to Senior Management Team is required to implement this policy.

Due consideration needs to be given to time of visit and seasonal variations.

Risk assessments (individual patient and generic) should be undertaken and locally held.

5.2 Staff Considerations

All staff should undertake a "10 Second" assessment prior to putting themselves in a potential risk situation. Consider the following signs/triggers:

- Negative Body language
- Signs of agitation
- Negative/aggressive verbal behaviour
- Evidence/suspicion of intoxication of any substance
- Imposing Groups
- Premises: seclusion/poor lighting/damage/unexpected open doors

N.B. This is in addition to staff following:

- Buddying procedures (when not starting from or returning to base)
- Red folder" code word (Adult Community only)
- Personal alarm use
- Frequent calls to base or "buddy"

In the event of identifying a risk, staff should contact office/colleague and arrange a 5 minute call back. This will provide the opportunity to leave the situation without causing suspicion.

In a clinic environment the member of staff should activate any panic alarm facility available or use either the landline or mobile telephone to make a discreet call to a colleague/reception staff. If no panic alarm facility exists follow advice below.

Managers should ensure a list of staff members along with car details (registration/make/model) should be kept in a secure location but accessible to designated leads. This would enable a formal vehicle search to be undertaken should concerns for a lone worker arise.

Managers should ensure emergency contact sheet is kept up to date for each member of staff, and consider holding a photograph of each staff member on their personal file. This should be reviewed annually for any update in appearance where a new photograph may be required. IMEI numbers for Trust mobile phone and iPad SIM cards should be held on individual personal files, as these can be GPS tracked in the event of an emergency. Staff members should ensure use of Patient Visit Manager (PVM) as this acts as a live allocation (Adult Community only).

6. "In Situ" Considerations

6.1 Dealing With Animals

If a lone worker is confronted by an aggressive animal on a first visit to a patients home address, they should cancel the visit and inform their line manager of the problem – this should also be treated as an incident and a Datix completed.

If the problem with animals is known, the patient should be contacted prior to the visit, and asked politely, if they would remove or secure the pet before arrival – clinical procedures can provoke a hostile/protective reaction from animals if they think their owner is being harmed

If the lone worker is not happy with animals being present when a visit is taking place, the above protocol should be followed. All possible efforts should be made when dealing with these situations so that by asking for the removal of a pet does not provoke a negative reaction with the patient.

All efforts should be made to ensure that the situation is managed and de-escalated should any hostilities become evident. If this is not possible, an alternative arrangement must be made
– rescheduling so a fellow colleague (who is at ease with animals) can accompany the lone worker on the visit or encouraging/facilitating the patient to attend a clinic environment.

6.2 Incident Occurs

Staff to be aware to dial 999 followed by 55, in the event of an emergency incident. This will trigger the call to be recorded by Emergency Services and for the call to be discreet as the caller is at risk.

Staff to activate personal alarms and/or Sky Guards in the event of an incident. Member of staff not returned as expected / call or text to nominated number not received – make immediate telephone call to check circumstances.

If no contact made – alert line manager/senior on duty who will notify the on call manager of concerns.

7. If Incident Occurs / Aftercare

All incidents should be notified to Line Manager/Service Lead in line with ACSG Escalation Process.

All incidents should be inputted into Datix. An alert/flag should be added to PAS/EMIS following an incident. All employees should be offered support and provided with suitable aftercare or counselling following an incident or violence or aggressive behaviour.

Risk assessments should be undertaken, and alternative visiting arrangements instigated as appropriate. Additional training/debrief sessions can be arranged post any incident.

8. Additional Support / Equipment

Issue/Query	Job Role	Colleague Name	Contact Details
Support with security/staff safety issues	Local Security Management Specialist (LSMS)	Head of Car Parking and Security	Ext. 754382
	Head of Health & Safety	Governance Officer	Ext. 3090

All staff to be issued with personal alarms where deemed necessary by Service Leads/Line Managers, this will include lone workers.

Individual teams to adhere to lone working risk assessment for service as well as protocol.

Appendix 1

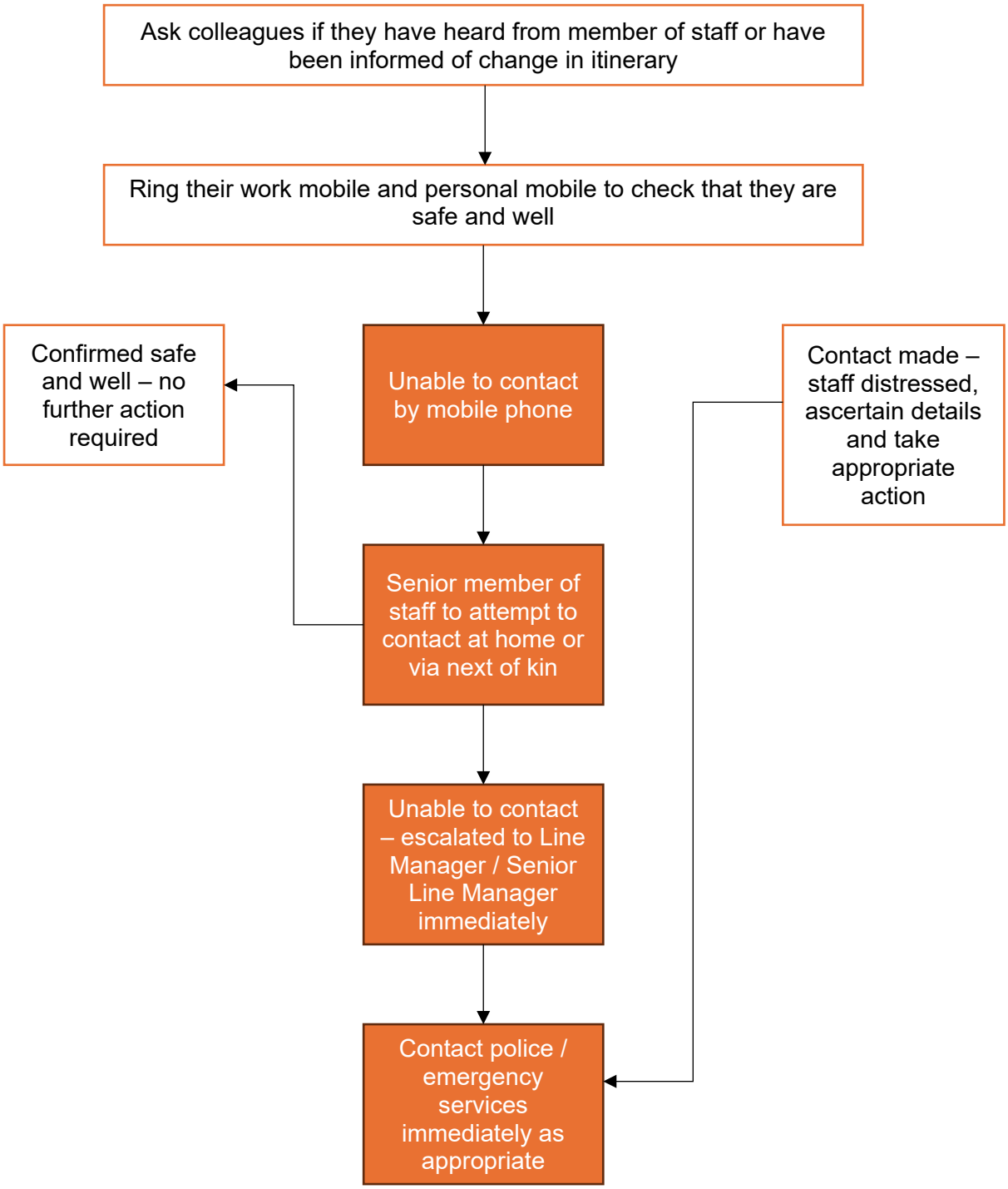
Lone Worker Guidelines

Pre Visit	• Gather as much information from referrer regarding patient (Adult Community only) • Check PAS/EMIS for any alerts/flags If the patient is in contact with other services within WHT/Black Country Partnership i.e. Mental Health services, contact their lead clinician to check for any further alerts. • Where indicated, staff should utilise the personal safety device for additional security and support
During Visit	• When going on home visit, staff must inform the team by phone or text that they are on duty and of any variation to the list of visits scheduled. Where indicated, personal safety device guidelines should be followed • Staff should always have either their own mobile phone or Trust mobile phone in their possession – ensure colleagues have the correct contact details and that a record of the phone number is held at base office • Ensure the Trust Security telephone number is saved on mobiles or written with ease of access • Staff should identify their expected time of return to office
Post Visit	• All staff should telephone their buddy/base to advise that they are going off duty • Staff working in Community health centres and GP practices should sign in and out on arrival and departure • For premises where no signing in/out if available, staff should follow local procedures

Appendix 2

Lone Worker Escalation Procedure
(In Conjunction with ACPCS Escalation Procedure)

When a member of staff does not return to base to confirm their whereabouts as agreed



Attachment 4

Closed Circuit Television (CCTV) – Code of Practice

1.0 Introduction

1.1 The purpose of this Code of Practice is to regulate the management, operation and use of the CCTV system at the Trust and to ensure that the Trust is complicit with the Information Commissioners Office guidelines "CCTV Codes of Practice".

1.2 The Trusts system comprises several fixed and dome cameras located around its Walsall Healthcare NHS Trust site. All cameras are monitored from a central control room.

1.3 This code follows Data Protection Act guidelines.

2.0 Objectives of the CCTV System

2.1 The purpose of the system is:

- Protect members of the public and their personal property
- Increase personal safety and reduce the fear of crime
- The protection of Trust Property and Assets
- Assist in identifying, apprehending and prosecuting offenders
- For the prevention and detection of crime
- Support the Police in a bid to deter and detect crime
- Assist with internal disciplinary matters
- Assist in aspects of traffic management

3.0 Statement of Intent

3.1 The CCTV system is registered with the Information Commissioner under the terms of the and will seek to comply with the requirements both UK General Data Protection (UK GDPR) and the Data Protection Act 2018 and the Commissioner's Code of Practice. The Trust will treat the CCTV system and all information, documents and recordings obtained and used as data which are protected by the Act.

3.2 Cameras will be used to monitor activities within the Trust its car parks and other public areas to identify criminal activity occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the Trust, together with all users of Trust.

3.3 CCTV operating staff is instructed that the cameras are not to focus on property adjacent to the Trust, gardens, and other areas of private property.

3.4 All subject access/disclosure requests for CCTV will be directed to the Trust Security Manger/Deputy Security Manager.

3.5 Materials or knowledge secured because of CCTV surveillance will not be used for any commercial purpose. Discs will only be released to assist the police in the investigation of a specific crime and with the written authority of the Trust. Discs will never be released

to the media for purposes of entertainment.

3.6 The planning and design has endeavoured to give the CCTV system maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.7 Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the CCTV system.

4.0 Operation of the CCTV System

4.1 The system will be administered and managed by the Trust, in accordance with the principles and objectives expressed in this Code of Practice.

4.2 The day-to-day management will be the responsibility of the Security Contracts Manager (or nominated deputy during the day and the SIA Licensed Security Officers out of hours and at weekends).

4.3 The Control Room will only be staffed by the Security Team. The CCTV system will be operated 24 hours every day of the year.

5.0 Control Room

5.1 The Security Contracts Manager (or nominated deputy) will check and confirm that the equipment is properly recording and that cameras are functional.

5.2 Access to the CCTV Control Room will be strictly limited to authorised staff only. For further information please contact the Trust Security Manager.

5.3 Unless an immediate response to events is required, staff in the CCTV Control Room must not direct cameras at an individual or a specific group of individuals.

5.4 Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangement as outlined below. (5.5 below).

5.5 Control Room Operators must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be endorsed in the Control Room signing in book.

6.0 Monitoring Procedures

6.1 Camera surveillance may be always maintained. Monitors are installed in the Control Room to which pictures are continuously recorded.

6.2 Covert CCTV surveillance may be possible in circumstances that require an immediate action to prevent the loss of Trust property or in the prevention and detection of crime, in these circumstances the Trusts Local Security Management Specialist must be contacted for advice and guidance. Covert CCTV surveillance may be considered so long as it is not intrusive or directed and that, there is no expectation of receiving private information about any individual.

7.0 Digital Recording System Procedures

7.1 The following procedures for the use and retention of discs must be strictly adhered to:

- Each disc/USB must be identified or identifiable by a unique mark.
- All subject access/disclosure requests for CCTV will be directed to the Trust Security Manger/LSMS/Security & Car Parking Management Team
- The controller shall register the date and time of disc/USB insert, including disc/USB reference
- A disc/USB required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence store. If a disc is not copied for the Police before it is sealed, a copy may be made later providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence store
- If the disc/USB is archived and remains in the control room until it is required by law enforcement or another agency the reference must be noted
- A master disc/USB must remain in the control room, only the copy may be released to the police or agency other than law enforcement

7.2 Discs / USB may be viewed by the police for the prevention and detection of crime and authorised investigators to the NHS. A record will be maintained of the release of discs to the Police or other authorised applicants. All releases will be documented within the Control rooms “CCTV Evidence pack”/CCTV Release form. Requests by the police can only be actioned under section 29 of the UK General Data Protection (UK GDPR) and the Data Protection Act 2018.

7.3 Should a disc/USB be required as evidence, a copy may be released to the Police under the procedures described above. Discs/USB will only be released to the Police on the clear understanding that the disc/USB remains the property of the Trust, and both the disc/USB and information contained on it are to be treated in accordance with this code. The Trust also retains the right to refuse permission for the police to pass to any other person the disc/USB or any part of the information contained thereon. On occasions when a Court requires the release of an original disc this will be produced from the secure evidence store, complete in its sealed sleeve.

7.4 All CCTV data is stored for a period of not less than 25 days and not more than 31 days except for Body Worn Video Camera Footage which will be stored for 90 days. This is monitored via daily CCTV system checks and Monthly CCTV Reviews. The police may require the Trust to retain the stored discs for possible use as evidence in the future. All requests are processed in accordance with the Data Protection Act Section 29(3) such discs will be properly indexed and securely stored until they are required.

7.5 Applications received from outside bodies (e.g. solicitors) to view or release discs will be referred to the Local Security Management Specialist or a member of his nominated Team. In these circumstances discs/USB will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases. The Trust reserves the right to withhold CCTV footage if the relevant criteria are not met or there is a risk of prejudicing a third party.

8.0 Body Worn Video Camera Operational Procedure

8.1 The purpose of this procedure is to regulate the management, operation and use of the Body Worn Video Cameras (BWVC) at the Trust and to ensure that the Trust is

compliant with the Information Commissioners office Guidance “CCTV Codes of Practice V1 15/10/2024”

The Purpose of the Device is:

- Increase personal safety and reduce the fear of crime
- Assist in identifying, apprehending, and prosecuting offenders
- For the prevention and detection of crime
- Support the police in a bid to deter and detect crime
- Assist in aspects of traffic management

9.0 Breaches of the Code

9.1 Any breach of this Code of Practice by Trust staff will be initially investigated by the Security Management or LSMS for the Trust to take the appropriate disciplinary action. The incident will be scored using the IG scoring calculator and will be recorded onto the Trusts Datix/safeguarding system.

10.0 Compliance Advice

a. It is important that the Data Protection Act is complied with because failure to do so may result in action being taken under this Act. Failure to comply with Data Protection requirements will also affect the police’s ability to use the CCTV images to investigate a crime and may hamper the prosecution of offenders. Additional Information about the use of CCTV and Data Protection can be found at: https://ico.org.uk

Attachment 5

Closed Circuit Television (CCTV) – Covert Code of Practice 1

1.0 Introduction

1.1 The purpose of this Code of Practice is to regulate the management, operation and use of the Covert CCTV system at the Trust.

1.2 The system comprises a portable camera that can be located around the Walsall Healthcare NHS Trusts sites, including community premises. The recording system may be housed locally, and the storage device may be removable for the purposes of reviewing the footage. Other means are to connect the device to an existing digital video recording unit.

1.3 This Code follows Data Protection Act guidelines.

2.0 Objectives of the CCTV System

2.1 The purpose of the system is:

- Protect members of the public and their personal property
- Increase personal safety and reduce the fear of crime
- The protection of Trust Property and Assets
- Assist in identifying, apprehending and prosecuting offenders
- For the prevention and detection of crime
- Support the Police in a bid to deter and detect crime
- Footage attained may be used in accordance with the Disciplinary Policy

3.0 Statement of Intent

Commissioner's Code of Practice

3.1 The Trust will treat the CCTV system and all information, documents and recordings obtained and used as data which are protected by the Act.

3.2 The camera will be used to monitor activities within the Trust and other public areas to identify criminal/investigatory activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the Trust, together with all users of Trust premises.

3.3 The CCTV system will not focus on property adjacent to the Trust, gardens and other areas of private property.

3.4 Materials or knowledge secured as a result of CCTV surveillance will not be used for any commercial purpose. Footage will only be released to the media to assist the police in the investigation of a specific crime and with the written authority of the Trust. Discs/USB will never be released to the media for purposes of entertainment.

3.5 The planning and installation will endeavour to give the CCTV system maximum

effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the area covered.

3.6 The Trust will not use the device as a surveillance tool for a specific investigation where it is likely to obtain private information about a person(s) unless the device is required for use in gathering evidence against an individual(s) as part of a criminal investigation. In those circumstances the LSMS is authorised to carry out covert or overt surveillance in response to a specific allegation. And in those exceptional circumstances it will only be granted for a specific purpose and time period and will be constantly monitored and reviewed, ensuring that it is necessary and proportionate, and that third party collateral intrusion has been fully considered.

4.0 Operation of the CCTV System

4.1 The system will be administered and managed by the Trust's LSMS, in accordance with the principles and objectives expressed in this Code of Practice.

4.2 The day-to-day management will be the responsibility of the Trusts Security Manager/LSMS or when nominated the Trusts Deputy Security Manager.

4.3 An application for the use of the system must be completed in full and signed by the relevant manager. The application will be reviewed by the Trusts.

LSMS; the application may be referred to the trusts Human Resources Department for final approval. (Attachment 1)

4.4 The system will be subject to a specified duration; if further time is required then the requesting manager must complete a further application form and submit this to the LSMS.

4.5 The installation will be subject to completion of Attachment 2.

4.6 Any installation costs incurred will be met by the requesting Manager.

4.7 The system will only be installed in the specified location once written authority has been obtained.

4.8 The investigative criteria must be met before any installation takes place, is the installation an adequate response to an incident or for the prevention and detection of crime, the Trusts LSMS will advise on this matter.

5.0 Control

5.1 The Security Contracts Manager (or nominated deputy) will check and confirm that the equipment is properly recording and that cameras are functional.

5.2 Access to the CCTV Control Room will be strictly limited to authorised staff only. For further information please contact the Trust Security Manager.

5.3 Unless an immediate response to an event is required, the CCTV System will not be directed at an individual or a specific group of individuals.

6.0 Monitoring Procedures

6.1 Directed covert (hidden) and overt (visible) CCTV surveillance where an individual(s) or area is targeted in order to gain personal information in response to a specific allegation

is only permitted in exceptional circumstances. Only specially trained personnel (the LSMS, Police and other law enforcement agencies) may use such surveillance with written permission from the Home Office, Surveillance Commissioner and only when specific investigative criteria are met.

7.0 Digital Recording System Procedures

7.1 The following procedures for the use and retention of Data must be strictly adhered to:

- All data collated must be identified by a unique mark or identifiable by a unique mark
- The controller shall register the date and time of card/disc/USB insert, including card/disc/USB reference
- Any data required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence store. If data is not copied for the police before it is sealed, a copy may be made later providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence store
- If the data is archived the reference must be noted

7.2 Data obtained may be viewed by the police for the prevention and detection of crime and authorised criminal investigators to the NHS. A record will be maintained of the release of the data to the Police or other authorised applicants. A register will be available for this purpose. Requests by the Police can only be authorised under section 29 of the Data Protection Act 1998.

7.3 Should data be required as evidence, a copy may be released to the Police under the procedures described above data will only be released to the Police on the clear understanding that the data remains the property of the Trust, all data and information obtained are to be treated in accordance with this code. The Trust also retains the right to refuse permission for the Police to pass to any other person the data or any part of the information contained thereon. On occasions when a Court orders the release of original data, this will be produced from the secure evidence store, complete in its sealed sleeve.

7.4 All CCTV data is stored for a period of not less than 25 days and not more than 31 days. Police may require the Trust to retain the stored data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until they are needed by the Police.

7.5 Applications received from outside bodies (e.g. solicitors) to view or release footage will be referred to the Local Security Management Specialist. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

8.0 Breaches of the Code (Including Breaches of Security)

8.1 Any breach of this Code of Practice by Trust staff will be initially investigated by the Security Management or LSMS for the Trust to take the appropriate disciplinary action. The incident will also be recorded onto the Trusts Datix/safeguarding system.

9.0 Compliance Advice

9.1 It is important that the Data Protection Act is complied with; failure to do so may result in action being taken under this Act. Failure to comply with Data Protection requirements will also affect the police's ability to use the CCTV images to investigate a crime and may hamper the prosecution of offenders. Additional Information about the use of CCTV and Data Protection can be found at: https://ico.org.uk.

Attachment 6

Application for the Installation of Covert CCTV Systems

Date:

Person Requesting and Job Title	
Location of Installation	
Duration of Installation	
Reasons	
Objectives	
Any additional information	
LSMS Approval, Signature Required	
CEO Approval, Signature Required	
HR Approval (if required)	
Further Comments	

Attachment 7

Application for the Installation of Covert CCTV System

Installation Checklist

Date:

Person Requested and Job Title	
Installed by	
Duration of Installation	
Reasons	
Objectives	
Any additional information	
Installation Comments	