Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: GR8
Issue number: 9

Security policy (incorporating Lock Down procedure)

Lead executive	Director of Operations
Authors details	Security Services Manager - 07827307334

Type of document	Policy
Target audience	All CWP staff
Document purpose	*The policy complies with external requirements for managing the risks associated with the physical security of premises and other assets. The policy includes; the duties and responsibilities of Local Security Management Specialist (LSMS); review and monitoring processes.*

Approving meeting	Health & Safety Sub-Committee	Date 14-Jun-19
Implementation date	14-Jun-19	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
GR1	Incident reporting and management policy
GR7	Major incident plan
GR9	Bomb threat guidance (includes suspect packages)
GR11	Hostage and siege policy
GR33	The lone worker policy
CP6	The management of violence and aggression
CP36	Securing or locking of access doors to inpatient areas
CP39	After care of those who have been exposed to PAVA (Captor) spray or post deployment of 'taser' device
CP10	Safeguarding adults policy
CP40	Safeguarding children's policy
HR13	Guidance on accessing staff support and counselling
CG1	Fraud theft corruption policy

Document change history	
What is different?	New GR1 template New GDPR guidance included Amends to 'security of monies'
Appendices / electronic forms	Have appendices been added, or changed since the last issue, if so explain the reasons why?
What is the impact of change?	Improved security and safety

Training requirements	No - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Modern Matrons/HoOPS

Corporate services	EP Lead
External agencies	Who within this service have you spoken to

Financial resource implications	None

External references
1. www.securedbydesign.com. 2. www.securedbydesign.com/pdfs/SBD_Hospitals_110405.pdf. 3. http://www.ukresilience.info/preparedness/risk.aspx. 4. Department of Health's Emergency Preparedness Division's1 website: www.dh.gov.uk/Emergencyplanning 5. Department of Health's Estates and Facilities' Knowledge and Information portal: http://195.92.246.148/nhsestates/knowledge/knowledge_content/home/home.a sp 6. Department of Health's Emergency Preparedness Division (EPD), EPD, will provide best practice advice on evacuation http://www.dh.gov.uk/en/Managingyourorganisation/Emergencyplanning/inde x.htm. 7. Civil Contingencies Act http://www.ukresilience.info/preparedness/ccact.aspx. 8. www.mindtools.com/pages/article/newPPM_07.htm 9. NHS Protect Standards for Provdiers 2017/18 Security management 10. Workplace Regulations 1992 11. Health and Safety at Work Act 1074

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
Select		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A No No	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	Low	

Contents

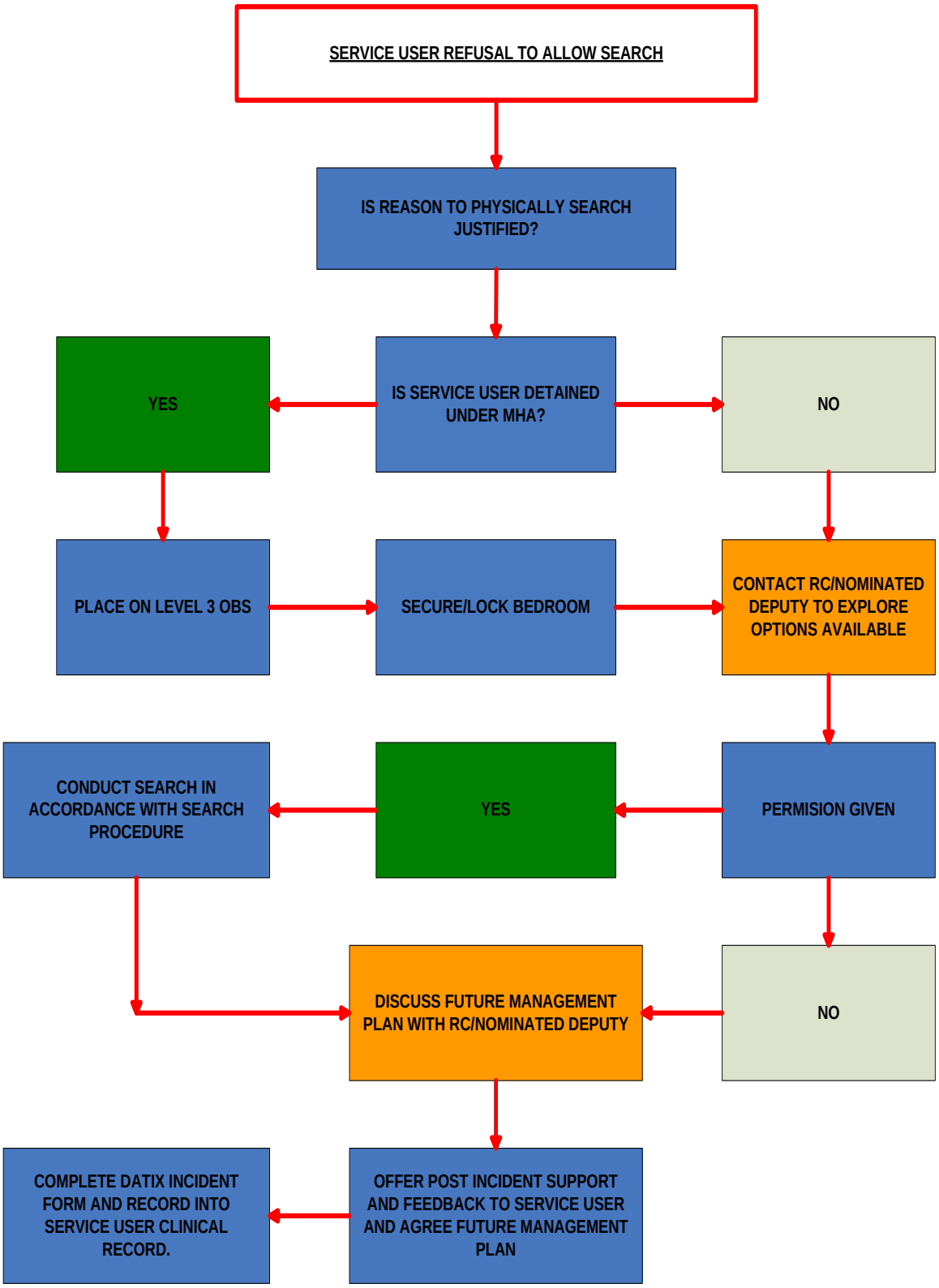
Quick reference flowchart 1 - Service user refusal to personal search 5
Quick reference flowchart 2 - Room Search protocol 6
Quick reference flowchart 3 - Person search protocol 7
Quick reference flowchart 4 - Procedure flowchart for Police Dog searches within Inpatient settings 8
Quick reference flowchart 5 - Procedure for post PAVA spray care 9
Quick reference flowchart 6 - Procedure for post 'Taser' deployment care 10
Quick reference flowchart 7- In-patient hostage and siege incident 11
Quick reference flowchart 8 – Protocol for the management of illicit substances 11

1. Introduction 13
2. Definitions 13
3. Procedure 13
3.1 How the organisation risk assesses the physical security of premises and assets 13
3.1.1 Premises 13
3.1.2 Assets 13
3.1.3 Assets register 13
3.2 How action plans are developed and followed up as a result of risk assessments 14
3.2.1 Premises 14
3.2.2 Assets 14
3.3 Operational building protocols 14
3.4 Security of monies and personal effects 14
3.5 Parking 15
3.6 Vehicles, traffic and the Law 15
3.7 Police and the information sharing 15
3.8 Identification badges 15
3.9 Trust keys and fobs 17
3.10 Access and control points to CWP areas 17
3.11 Building Alarms 18
3.13 Close Circuit Television Control 18
3.14 Involvement of inpatients and recording of images 18
3.15 Contacting the police 18
4. The securing of access doors to inpatient areas 18
4.1 Automated Access Controls 18
5. Search procedure for service users and environments 18
5.1 Consent and Juveniles / patients under the age of 18 years 19
6. The management of Taser and PAVA contaminant spray incidents 19
7. Hostage and Siege incident management procedure 19
8. The Management of Illicit Substances 19
9. Bomb Threat Procedure 19
10. Lock Down of CWP main inpatient buildings 19
10.1 Lockdown remit 20
10.2 Community services 20
10.3 Staff working away from their office base 21
10.4 Defining site/building lockdown 21
10.5 Arrangements for producing a lockdown risk profile for each organisational site or building 21
10.6 Operational staff roles and responsibilities 23
10.7 Internal communications 23
10.8 External communications with stakeholders 23
10.9 Safe and control zones 24
10.1.0 Traffic management 24
10.1.2 Workforce factors 24
10.1.3 Crowd management and control 24
10.1.4 Evacuation 24

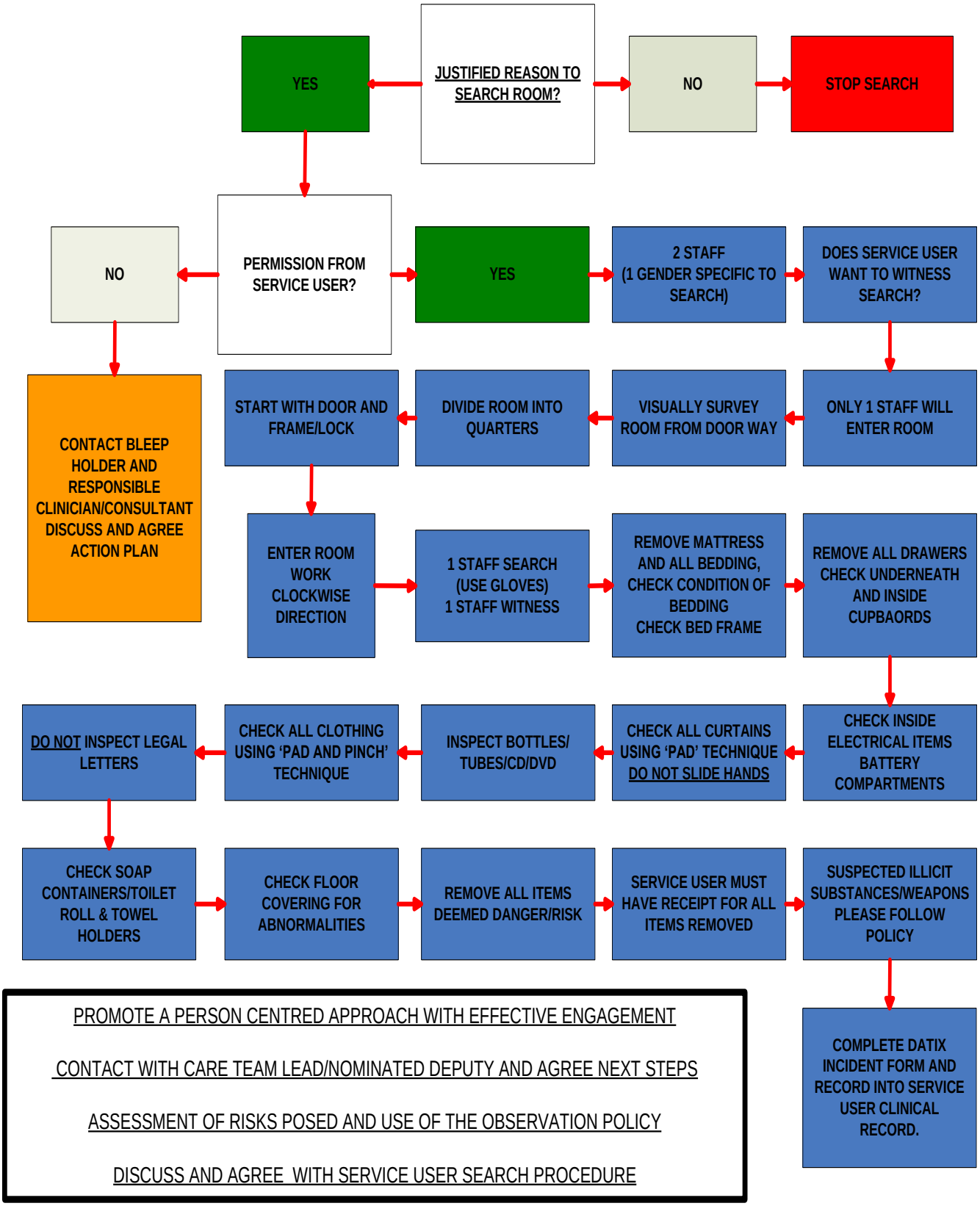
10.1.5 Lockdown stand-down 24
10.1.6 Recovery 24

Appendix 1 – Lock Down Risk Profile 25
Appendix 2 - Operational roles of key CWP staff during a lock down activation and deployment 26
Appendix 3 – Local incident team lead 27
Appendix 4 - Incident Support Staff (Porter / Security on duty) 28
Appendix 5 - Incident Support Staff (Estates Officers) 29
Appendix 6 - General designated staff response protocol 30
Appendix 7 - Incident in progress 31

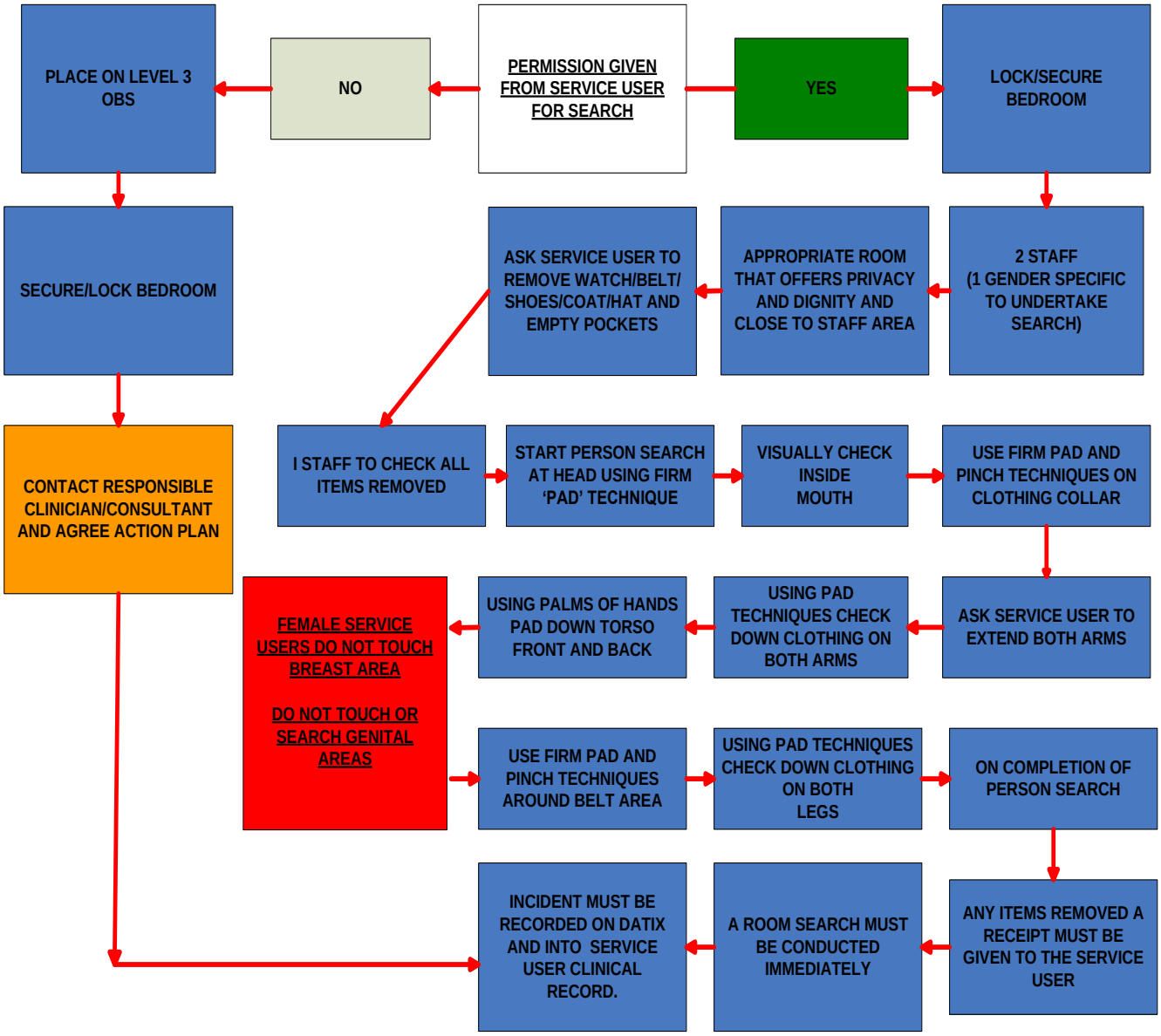
Quick reference flowchart 1 - Service user refusal to personal search



Quick reference flowchart 2 - Room Search protocol



Quick reference flowchart 3 - Person search protocol



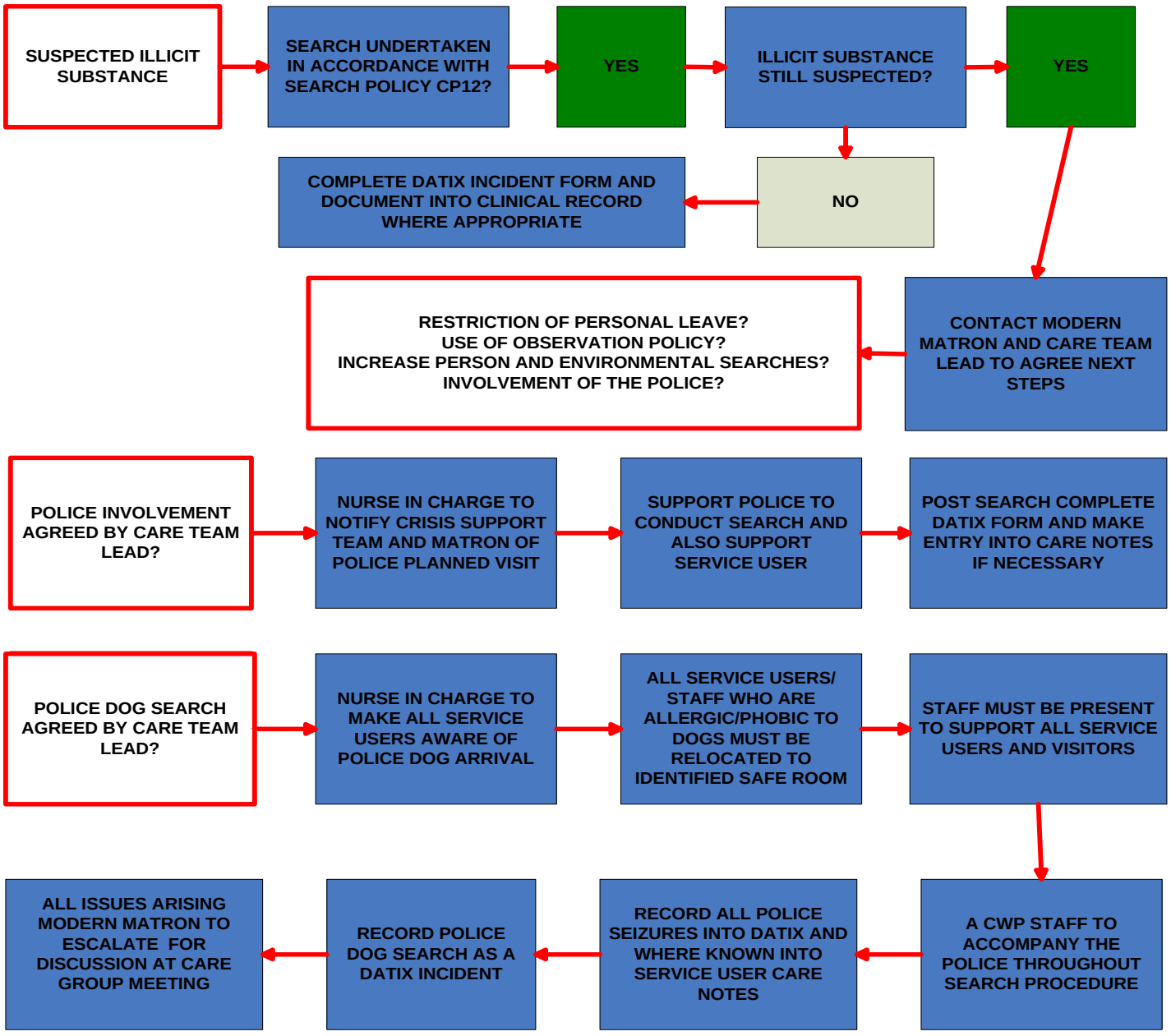
PROMOTE A PERSON CENTRED APPROACH WITH EFFECTIVE ENGAGEMENT

ANY SUSPICIONS REGARDING ITEMS BEING SECRETED INSIDE ANY UNDERWEAR THE N.I.C MUST MAKE CONTACT WITH CARE TEAM LEAD/NOMINATED DEPUTY AND AGREE NEXT STEPS

ASSESSMENT OF RISKS POSED AND USE OF THE OBSERVATION POLICY

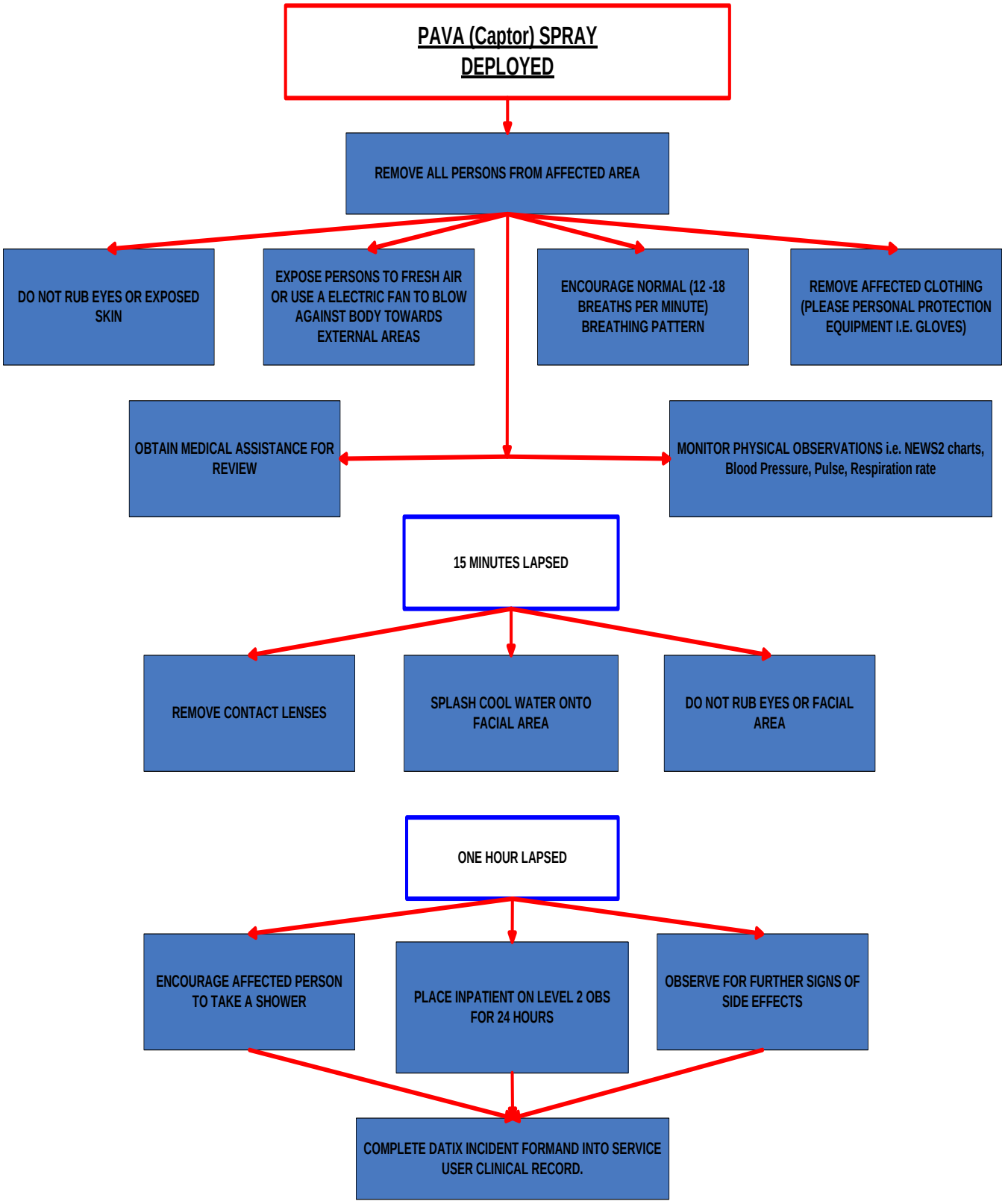
DISCUSS AND AGREE WITH SERVICE USER SEARCH PROCEDURE

Quick reference flowchart 4 - Procedure flowchart for Police Dog searches within Inpatient settings

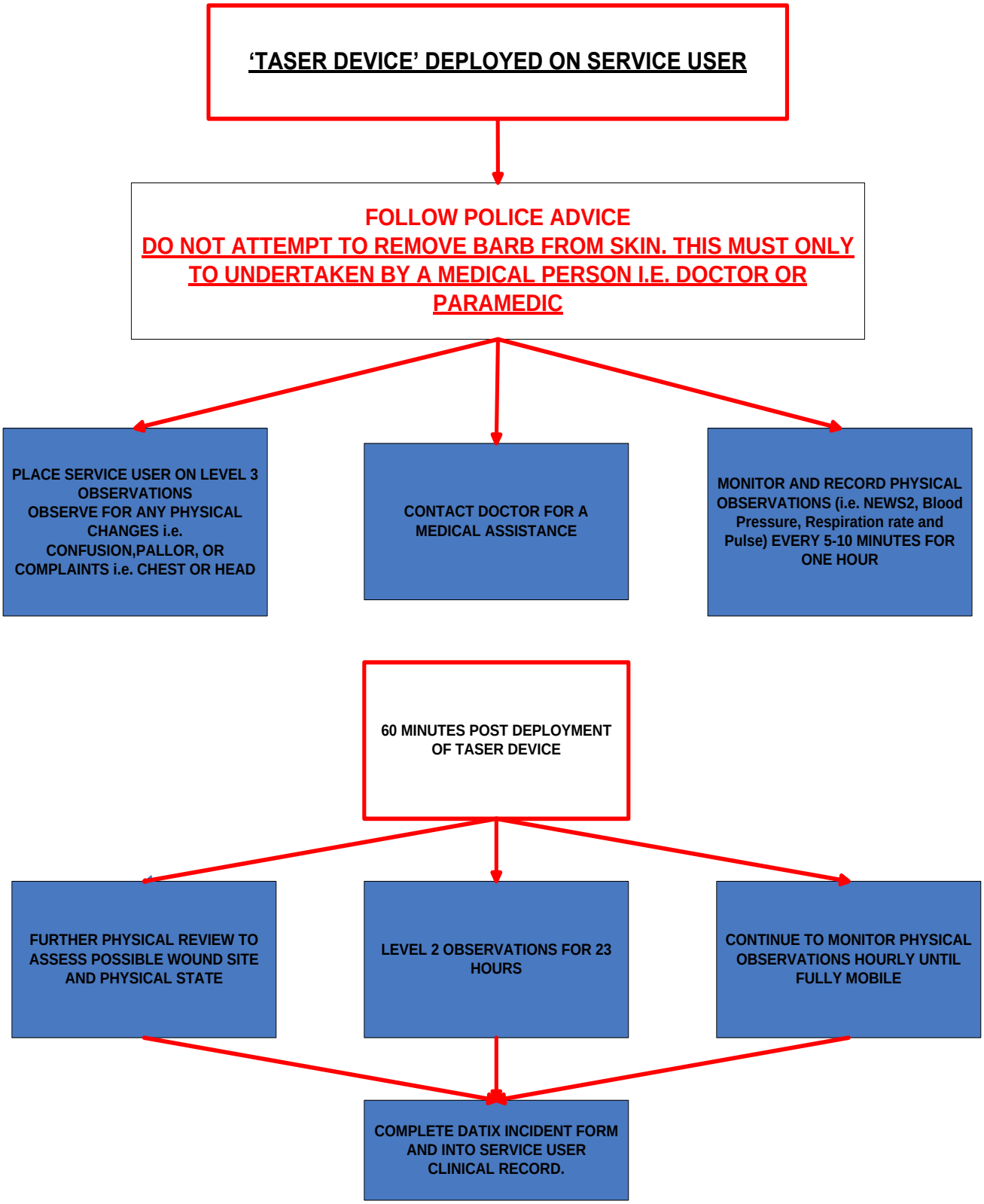


PROMOTE A PERSON CENTRED APPROACH WITH EFFECTIVE ENGAGEMENT WITH ALL SERVICE USERS AND OTHERS
REASONABLENESS, PROPROTIONALITY AND NECESSITY

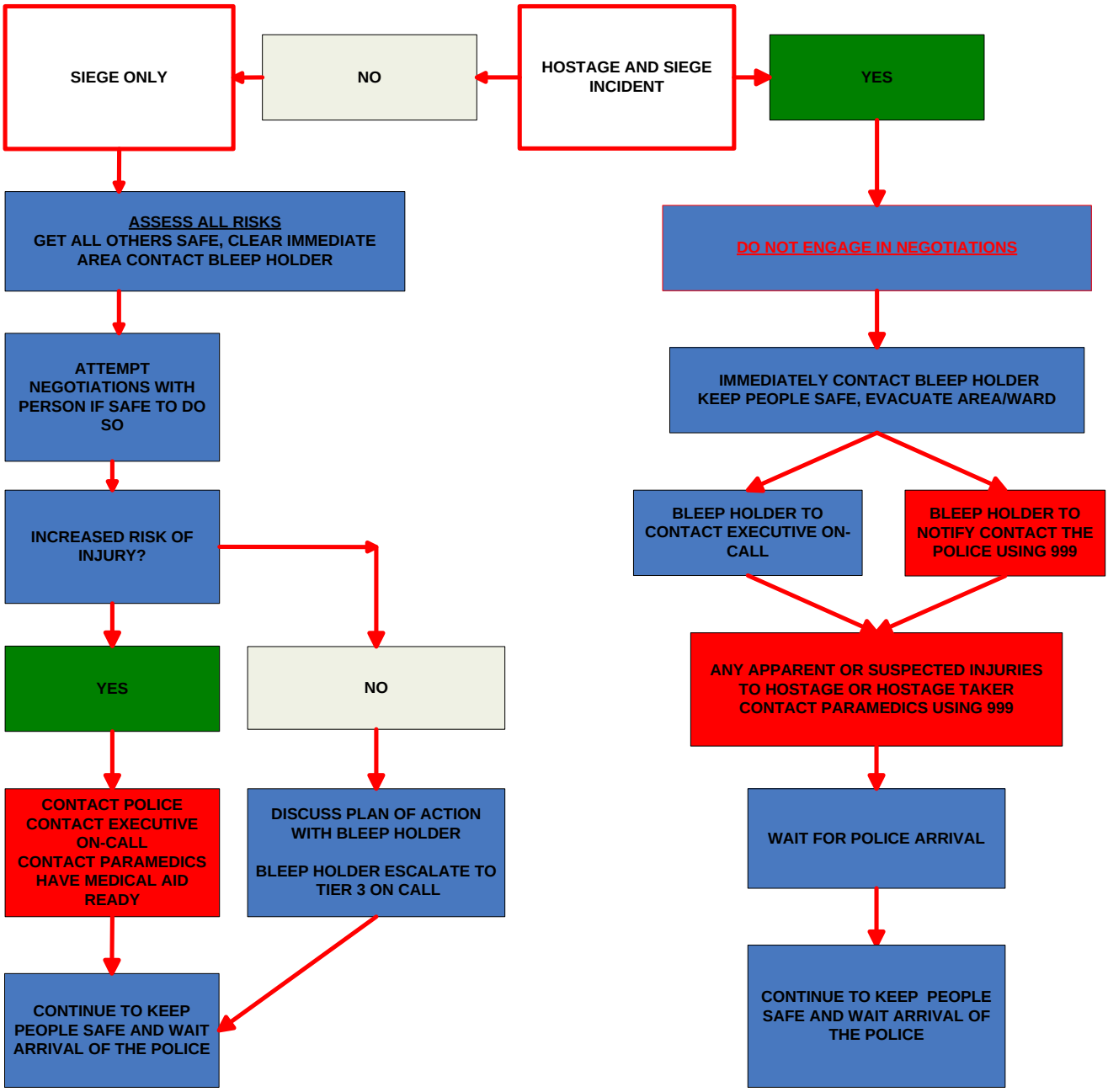
Quick reference flowchart 5 - Procedure for post PAVA spray care



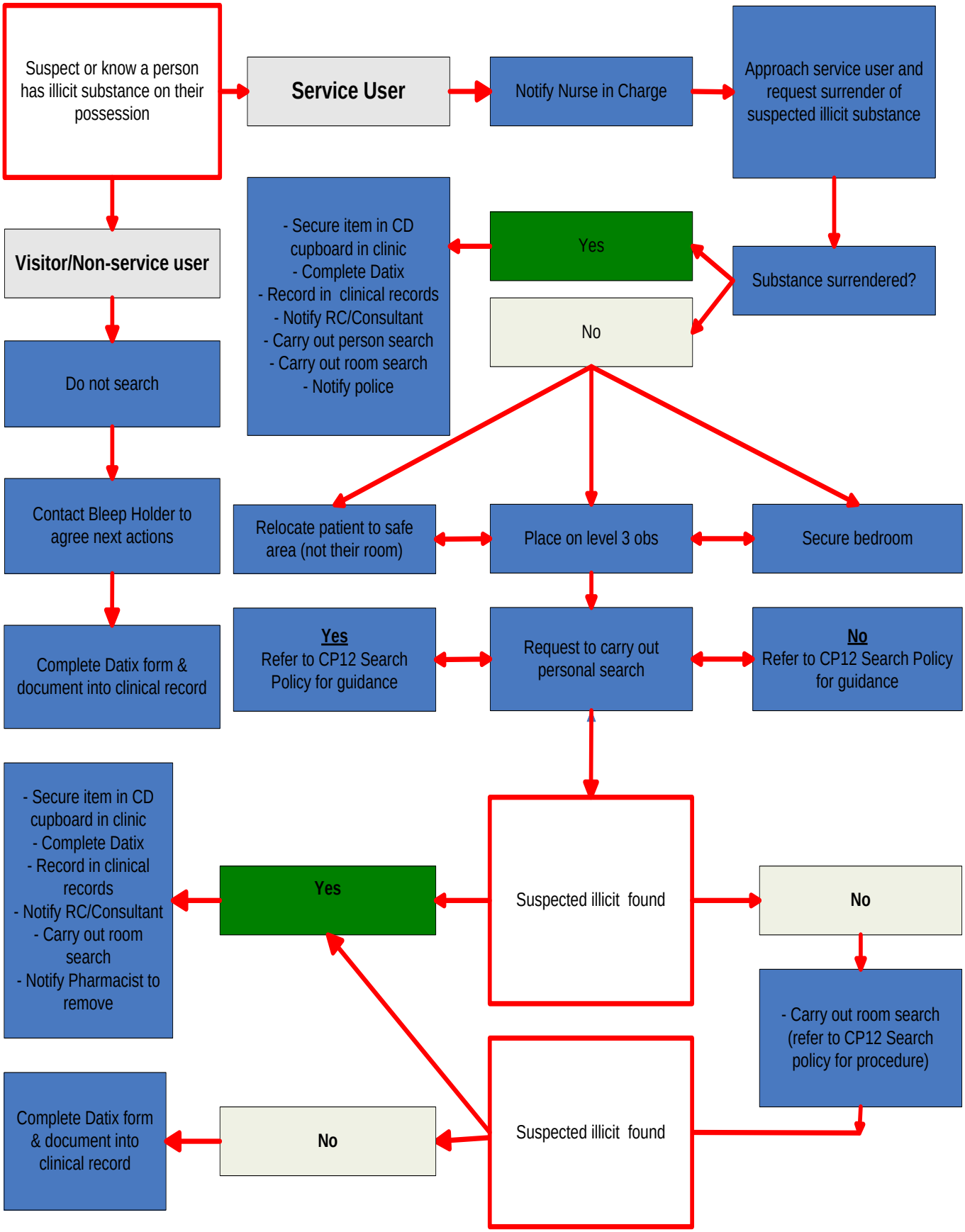
Quick reference flowchart 6 - Procedure for post 'Taser' deployment care



Quick reference flowchart 7- In-patient hostage and siege incident



Quick reference flowchart 8 – Protocol for the management of illicit substances



1. Introduction

This policy has been developed to assist the Trust to comply with the statutory obligations and directions imposed by NHS Protect Standards for Providers 2017/18), Health and Safety Executive (HSE) for Trust staff to understand their own responsibilities regarding promoting a pro-security culture.

It is recognised by the Trust Board that a secure and safe environment for clients, visitors and staff is essential in achieving the highest possible standard of service provision. To achieve this aim the organisation is committed to support the delivery of high quality services though the provision of a secure environment and to implement and regularly review procedures for the physical security of CWP areas and equipment.

Within this policy is also the requirement to undertake appropriate risk assessments and inspections regarding the physical safety and security of premises and assets.

2. Definitions

Security refers to the strategic and operational measures to protect CWP staff, service users and assets.

Operational Building Protocol refers to a standardised template that would be used to detail how each building will respond to emergencies and reporting of incidents.

Building refers to any premises where CWP provides a service from.

Assets refers to any CWP resource or property.

The Civil Contingencies Act 2004 is an Act of the Parliament of the United Kingdom that establishes a coherent framework for emergency planning and response ranging from local to national level.

3. Procedure

3.1 How the organisation risk assesses the physical security of premises and assets

3.1.1 Premises

Under the Health and Safety at Work Act (1974) CWP has a legal duty to ensure as far as reasonably practicable the health, safety and welfare at work of all employees. The H&S Work Place Regulations (1974) places a requirement to maintain the workplace and any equipment so that it is safe and that buildings are in good repair. NHS Protect Standards for Providers 2017/18 state that organisations should establish a safe and secure physical environments that has systems and polices in place to protect NHS staff from violence, harassment and abuse; safeguard NHS property and assets from theft, misappropriation, or criminal damage; and protect resources from fraud, bribery and corruption. All security incidents are reported to all Care Groups through the Learning from Incidents report. Local Health and Safety groups are responsible for monitoring any improvement and actions agreed relating to security. Building risk assessments are reported through the local H&S groups..

3.1.2 Assets

The Estates department is responsible for the CWP medical devices catalogue any equipment and undertakes a scheduled review of risk assessments on an annual basis as required. All risks identified by the Estates department are summarised in the annual report to Operational Board and Health and Safety Sub Committee.

3.1.3 Assets register

The Trust finance department hold an asset register which details all equipment which is deemed capital in nature as defined in Monitor's Capital Accounting Manual. The Trust capitalised fixed assets are subject to an annual equipment verification exercise carried out by the Capital Services Accountant and audited by an external provider.

This exercise is a fundamental part of the Trusts statutory annual accounts audit and supports the notes in paragraph 1.7 of the Annual Report and Accounts. The verification exercise fulfils the obligations of the Chief Executive as set out in paragraph 13.3 (13.3.1) of the Trusts Standing Financial Instructions, and the statutory accounts are reviewed by Audit Committee and approved by the Board of Directors. The audit report will be evidenced through the Committee's use of an effective assurance framework to guide its work and that of the audit and assurance functions that report to ensure effective systems of integrated governance, risk management and internal control, together with indicators of their effectiveness.

3.2 How action plans are developed and followed up as a result of risk assessments

3.2.1 Premises

All recommended actions following a building risk assessment are fed back to the manager of the service who is responsible for ensuring the actions are completed. This action plan is monitored via the local H&S groups which reports any risks to the Trust Health and Safety Sub Committee.

3.2.2 Assets

All recommended actions identified through the asset risk assessment will be reported to the Estates Department and reviewed at the H&SSC to ensure actions are completed. In addition any risks identified through the asset register audit will be reported to the Audit Committee and Board and an action plan developed and monitored. Consideration will also be given as to the inclusion of any risks identified on the corporate risk register in accordance with the Integrated Governance Strategy. All relevant action plans will be included on the CWP action plan register and will be monitored by the H&SSC.

3.3 Operational building protocols

All CWP buildings should have an up to date Operational Building protocol which is used to detail how each building will respond to emergencies and reporting of incidents. The Operational Building protocol will also detail how staff must act regarding maintaining the safety and security of CWP assets and property.

All CWP staff have a duty to promote a pro-security culture, as such:

- All equipment must be kept securely and not left in areas of easy access. Managers should keep a site inventory of valuable equipment within their department and update this when required;
- Information technology equipment must be clearly marked with the CWP logo and the departmental / ward number as soon as it is purchased and any loans of equipment to other departments / wards should be noted in an inventory sheet;
- Areas normally locked or open - care must be taken that any portable items of equipment of value must be locked away whenever possible when not in use;
- Where locked storage is not available, security items must be stored out of sight.

3.4 Security of monies and personal effects

(see CP62 Procedure for security of a patients cash and valuables on wards)

Whilst CWP will not be responsible for loss of staff property, staff will be encouraged to report any loss of their property and cooperate in any enquiry which may result in connection with the loss.

- All inpatient monies and personal effects must be; secured only within lockable safes; documented and signed by two staff members each shift; safe key secured at all times by the nurse in charge; all withdrawals or transfers must be witnessed and signed by two staff members
- All CWP staff are advised not to bring cash in excess of their daily needs and any cash should be retained securely on their person. Staff should have access to a secure facility to lock away personal property whilst on duty.
- Any service which operates any cash remuneration for service users travel expenses or for the management of small amounts of monies used to promote rehabilitation or daily living skills

must have a robust local operational procedure in place. All affected staff must be made fully aware of the operational procedure and comply with its content.

3.5 Parking

Whilst CWP provides parking facilities, it does not accept liability for any theft or damage to motor vehicles or their contents when they are parked on CWP sites. CWP reserves the right to deny any vehicle access to a site and to require drivers to conform to the designated traffic regulations and signs in order to ensure that:

- All CWP staff should display the CWP car identification sticker if applicable;
- The security of motor vehicles is the responsibility of the owner of the vehicle;
- No obstruction is caused to fire exits;
- No obstruction is caused to load and / or unloading areas or the movement of service users, goods or the provisions of services;
- Parking is permitted on CWP premises in designated areas only;
- Trust property should not be left unattended in vehicles;
- Under no circumstances must a CWP car park be used to store motor vehicles. It will be the responsibility of the user to remove a broken down vehicle as soon as possible;
- Separate arrangements and permits exist for parking on other Trust partnership sites and staff must adhere to their policies.

3.6 Vehicles, traffic and the Law

Anyone using vehicles of any description on the site is expected to comply with the law regarding taxation, licensing, insurance, roadworthiness and the reporting of accidents to the police and CWP. Any member of staff driving a vehicle of any description on site who causes an injury to any person or to property is required to report the matter to CWP without delay as well as complying with the law by notifying the Police as appropriate.

3.7 Police and the information sharing

The sharing of information involving service users or members of the public to the police must normally only be done for the reporting of an incident or crime and strictly in accordance with CWP policy. In the event of a major incident being reported all communications with the police will be through a CWP Executive and / or Emergency Planning Lead as detailed in CWP policy.

In accordance with General Data Protection Regulations 2016/Data Protection Act 2018 when a decision to contact the police has been made, the disclosure of personal information must initially be limited to that which is necessary to enable the police to identify the subject and assess the risks.
It will normally be sufficient to supply the name, date of birth and address of the person concerned. Where there is evidence or a suspicion that a crime has been committed, this must also be communicated. Medical information will not normally be required unless it might:

- Help explain the individual understanding of the situation;
- Help explain the individuals propensity for violence;
- Inform any decision on prosecution;
- Assist the police in carrying out their duties safely.

3.8 Identification badges

This guidance refers to all CWP staff, volunteers and people undertaking CWP business. In compliance with NHS Employers – Identity Checks Standard (April 2016), CWP 'should undertake identity checks prior to allowing any individual to commence any form of work, whether paid or unpaid (volunteering) activities within their organisation' Identification badges will only be issued to people who have had their identity checked in compliance with CWP's Pre-employment checks policy inc. DBS checks

Identification badges (ID) are the property of CWP and under no circumstances will they be permitted to be worn by or transferred to any other non-authorised person. Any authorised person found in breach of this guidance appropriate action will be taken which safeguards all those who may be affected.

a) Issuing of Identification badges

ID badges will **only** be issued by Education CWP in the following instances: -

- When confirmed new starters are due to attend Corporate Induction;
- When communicated by the relevant line manager for changes required due to promotion, name change etc
- When communicated by the relevant line manager relating to a volunteer, a visitor etc.

b) Identification badges

- All ID badges must clearly state the persons job title or role
- All ID Badges must clearly state the person's name in CAPITAL LETTERS.
- All ID badges must display an expiry date.
- All ID badges must contain an up to date photograph which has been developed by Education CWP only.
- All CWP Staff ID badges must only be worn on blue and white NHS logoed appropriate lanyards.
- All Involvement Representative must only be worn on black and white logoed INVOLVEMENT REP lanyards. (this includes Young Person Advisors & Expert Patient Volunteer Tutors)
- All Governor ID badges (non-CWP staff Governors) must only be worn on black and white CWP GOVERNOR logoed lanyards.
- All Volunteer ID badges must only be worn on black and white VOLUNTEER logoed lanyards.
- All identification badges must be worn at all times whilst on duty or when on Trust business.

c) Identification valid period

- All CWP staff ID badges will be valid for 3 years
- All Volunteers and people undertaking CWP business ID badges will be valid for 1 year only

d) Requesting replacements for lost Identification badges

- Any staff, person or volunteer etc who has lost their Identification badge must;
- Report the loss to their line manager
- Complete a Datix incident form or ask line manager to complete same
- Ask their line manager to email Education CWP requesting a replacement badge, stating the staff name and role
- Immediately destroy the old badge if it is located post obtaining a new one.

e) Requesting replacement Identification badges

Any staff/person requesting a replacement Identification badge must;

- When updating due to a change of job title or name ask their line manager to email Education CWP with their up to date details at least 48 hours prior to arriving at Education CWP.
- If the ID badge is out of date, exchange their old ID badge when collecting the new one from Education CWP. A replacement ID badge will not be issued unless the old one is surrendered.

f) When an ID badge holder leaves CWP

When a staff member, person or volunteer etc leaves the employment of the Trust, it will be the responsibility of the line manager to retrieve the ID and immediately destroy it. If there are difficulties with retrieving the ID badge a reasonable plan must be agreed between the responsible line manager and the ID badge holder with actions to retrieve CWP property.

g) Persons suspected or known to be using CWP ID badge inappropriately

Persons not wearing an ID badge and those whose identity is unknown, should be challenged and asked to account for their presence. Where a person is known to be using a CWP ID badge without appropriate authorisation or inappropriately the alerting staff member must;

- Notify their line manager immediately
- Complete Datix form with full details
- Notify the CWP Safeguarding team where there are patients involved
- Report suspicious incidents to immediate line manager or CWP Security Services Manager lead and / or police.

h) Finding a CWP ID badge

Any person finding a CWP ID badge must;

- Return it via internal post to Education CWP, Sycamore House, Lloyd drive, Cheshire Oaks Business Park, Ellesmere Port, CH65 9HQ. Tel (01244) 397255

3.9 Trust keys and fobs

CWP keys **and fobs** are an important security item and are the sole responsibility of the person assigned to them in part or for whole duty;

- All staff (including; bank staff, agency staff, student nurses, medical staff, social care staff) must have access to keys and fobs where they are normally required to undertake their role
- Staff must not be expected to share keys or fobs where they are normally required to undertake their role
- Keys and fobs must not be attached to any CWP ID lanyard
- Under no circumstances must keys or fobs be left unattended e.g. on desks or in doors, or borrowed by unauthorised personnel;
- Duplicate keys must be held in locked cupboards / cabinet;
- Local facilities managers must ensure arrangements are in place for opening and closing of departments, which are cleaned by domestic staff outside normal working hours;
- The method of controlling keys or fobs shall be the responsibility of both the line manager and the designated member of staff;
- A duplicate set of department keys should be clearly marked and retained by the estates / facilities department;
- All broken keys must be reported to the Estates and all key parts securely disposed of;
- Replacement keys are only to be obtained via the estates department and must not be cut by local suppliers. Reimbursement of replacement keys will be through the line managers budget;
- Replacement fobs are only obtained through the line manager and access permission's clearly identified in relation to the fob holders role
- Master keys must only be issued to those staff responsible for whole areas of a building;
- All closed / vacated buildings must have their keys or fobs returned to the estates / facilities department for safe disposal or keeping;
- All clinical cupboards and ward keys or fobs must never be given to non-CWP persons;
- In the event of a missing key or fob all areas must be thoroughly checked and reported through CWP Datix incident reporting system;
- **Clinic keys and controlled drug keys must never be kept together on the same key chain**.

3.10 Access and control points to CWP areas

All line / team managers must ensure that:

- There are clear procedures for locking up, detailing when the area is to be kept secure and who is accountable;
- All doors and windows must be locked (where possible) and secured whenever an area is vacated;

- Arrangements with CWP Estates Team must be made for combination door codes to be changed regularly;
- Any unknown persons attempting to 'tailgate' through an access or control point must be asked for identification and their purpose of visit;
- Non CWP staff or visitors must be registered or signed in and out of each department;
- Any faults must be reported to the local estates department and also through the incident reporting system.

3.11 Building Alarms

Intruder alarms, where installed:

- All staff required to set or disarm the alarm must receive appropriate training from their line manager;
- Be set at the completion of the working day;
- Alarm codes must not be kept with equipment or left in vehicles;
- All alarms must be serviced by contracted specialist as recommended by the manufacturer.

3.12 Personal Protection Equipment (PPE)

Where normally provided Personal alarms must be allocated to each staff member (including; bank staff, agency staff, student nurses, medical staff, social care staff) either in commencement of work or when requested. When a Personal Alarm is provided individual staff are responsible for:

- Personal alarms must not be attached to CWP ID lanyards
- Ensuring that they have an alarm commencing work;
- Testing it prior to commencing work;
- Reporting any shortages of alarms to the line manager and through the incident reporting process;
- Ensuring that all faults are reported to the local estates department.

3.13 Close Circuit Television Control

(see GR46 Surveillance System CCTV policy)

3.14 Involvement of inpatients and recording of images

The use of Lived Experience persons in organisational activities and developments can be integral to staff learning. Where the Lived Experience person is currently an inpatient and the recording of their images is required for the activity or development i.e. simulation this must not be permitted at any time. It is important that inpatients should be protected from any unintended stimuli which may be harmful to their recovery.

3.15 Contacting the police

All police emergencies contact: 999

The police must be called to CWP premises in the following circumstances when:

- CWP staff feels themselves or service users / visitors are in immediate danger and / or fear of having physical harm inflicted upon them and that the risk of intervening would be too great to safely contain the risk of imminent harm to others;
- Reporting of a crime that was committed or in the course being committed as part of duty of care and / or out of a responsible public duty.

4. The securing of access doors to inpatient areas

(see CP36 Securing or locking of access doors within inpatient areas)

4.1 Automated Access Controls

(see CP36 Securing or locking of access doors within inpatient areas)

5. Search procedure for service users and environments

(see CP12 Search policy & Quick reference charts)

5.1 Consent and Juveniles / patients under the age of 18 years
(see CP12 Search policy & Quick reference charts)

6. The management of Taser and PAVA contaminant spray incidents
The procedure for post PAVA spray care is outlined within Quick reference chart 5 and the procedure for post Taser deployment care is outlined in Quick reference chart 6 .

Any call made to the police will be as a direct consequence of the extreme risk present during an incident in inpatient areas and in accordance with CWP policy. All decisions to discharge any device will be made only by the Police as they will have assumed control of the situation. CWP staff must only act post deployment upon the strict instruction of the Police officer in charge of the incident at the time. Staff must advise the police regarding any known physical conditions that may be complicated by the use of the device on a service user. Once any decision has been made by the Police to use any device, staff must notify their line manager / bleep holder and the on-call medical staff. Immediate concern must be the safety of the service user and staff and also the possible effects on others post incident.

7. Hostage and Siege incident management procedure
(see GR11 Hostage and Siege policy **and refer to** Quick reference chart 7 **for further guidance)**

8. The Management of Illicit Substances
(see GR37 The management of illicit substances policy and **refer to** Quick reference chart 8 **for further advice and guidance)**

9. Bomb Threat Procedure
(see GR9 Bomb threat policy**)**

10. Lock Down of CWP main inpatient buildings
The ability of CWP to lock down their site or buildings fits in with their statutory responsibilities as category 1 responders as defined by the Civil Contingencies Act 2004. The act states that category 1 providers must assess the risks of emergencies occurring and have plans in place to manage them. Locking down a trust site or building may be the most suitable response in a wide range of emergencies. CWP main inpatient hospital buildings are;

- Bowmere Hospital
- Springview Hospital
- Millbrook Hospital
- Soss Moss site

A lockdown will also support other major incident responses such as the evacuation of one of its main inpatient units. The consequences of invoking a proportionate lockdown and the short, medium and long-term effect it may have on NHS services must be fully considered by CWP management. Any decision taken by CWP to implement lock down must be underpinned by the legal reasons for doing so and focus on the right of entry and exit of individuals onto and from an NHS site during the course of a lockdown.

A lockdown should be used to ensure the safety and security of all NHS trusts' personnel, patients, property and assets in the event of a major incident, and by doing so will protect the integrity of the NHS. NHS Protect Standards for Providers (Security) 2017/18

According to law most CWP healthcare sites and buildings are regarded as public areas and that members of the public have an implied license to enter them to receive a service. However, CWP is the owner of any such premises has a right to refuse access to any of these premises in certain circumstances. In this instance, in event of a lock down being implemented, if someone other than CWP employees enters the premises, having been advised not to, or is already on the premises and refuses to leave, they may be considered a trespasser and reasonable force may be used to prevent access or to remove them. If an individual enters the locked down premises or refuses to leave, they

could be prosecuted under criminal law. If a patient attends a locked down CWP site or building, the doctrine of best interest may be applicable. In this instance, although the patient may require treatment, it will be in their best interest to receive that treatment at other, safer, healthcare premises. Consequently, their 'right to treatment' under the European Human Rights Act 1998 will not be infringed upon.

In the absence of the police, who are able to enforce a containment cordon, it will only be lawful for CWP to prevent the exit of a significant number of people from its premises by utilising specific legislative provision (e.g. emergency regulations under the Civil Contingencies Act and/or Public Health (Control of Disease) Act 1984) which provides for the protection of the public from notifiable diseases. Even when these specific regulations can be used, specific tenets of the Human Rights Act 1998 must also be considered for example, a person's right to liberty (Article 5) and an individual's right to a family (Article 12). Without these regulations, it is likely that exit could only be prevented in relation to specific individuals in certain circumstances, which are likely to be limited to the following situations:

- The individual is committing an offence or causing injury or damage to property which may lead to them being arrested;
- They are detained under the Mental Health Act or otherwise lawfully detained.

While CWP can give direction within their premises (for example, stating which exit someone can use), it is unlawful to forcibly prevent exit from its premises unless it is for the reasons stated above. Without these justifications, CWP staff could be open to legal action under the criminal and/or civil law if they prevented a person from leaving. Nonetheless, there may be circumstances when a lockdown which prevents individuals from exiting CWP premises (or part of them) is desirable.
If this occurs, CWP staff can only appeal to individuals to stay in the site and/or building identified for lockdown. If individuals choose to exit, a safe route must be available for them to do so.

10.1 Lockdown remit

This policy of 'site' lock down only refers to all CWP Mental Health and Learning Disabilities inpatient units. In order to prevent the possibility of individual services becoming either contaminated or having excess pressure put upon them, only the CWP Chief Executive (CEO) or nominated deputy will give specific instruction to lock-down, instruct staff to prioritise resources to the area to assist and facilitate either temporary or permanent relocation of services provided and to maintain the safety of its staff and service users. These Inpatient services will be identified as high priority areas where extra assistance may be given in the event of a prolonged lock down period in accordance with CWP Emergency Planning Strategy.

A number of CWP premises are on sites shared with other organisations on these shared sites the main host organisation/Acute Care Trusts lock down procedures will act as the overarching document for the whole site and as a result will take priority on all emergency planning issues. This will include responsibility for traffic management and public access to the site through the main entrances. Overall command of the incident will be from the incident commander of the host organisation/Acute Care Trust in conjunction with CWP Executive or Emergency Planning/Incident Lead. This is in alignment with the hosts responsibilities as Category 1 Responders, as defined by the Civil Contingencies Act 2004. All CWP Mental Health and Learning Disabilities inpatient areas on these sites will be required to secure and control all their access and egress points to staff and visitors.

10.2 Community services

Lockdown of all non-inpatient or community settings will be coordinated internally by the CWP Executive or Emergency Planning/Incident Lead through the local lead for those areas. All affected CWP non inpatient buildings will be required to secure and control all the entrance and exit points to that building but will not normally be required to secure ground / site access or car park points unless directed to do so. All community buildings or services not situated on a CWP site will in the event of an emergency incident receive external direction from the Police who will also liaise with CWP Executive or Incident Lead. Where services are facilitated from shared premises i.e. health centres,

GP surgery's, CWP staff must follow the local emergency planning policy designed for that building or area.

All clinical day facilities will refer to their Business Contingency Plans which prioritise arrangements for service users and staff in consultation with the CWP Emergency Planning Lead. The use of CWP vehicles identified within the Emergency Planning Strategy can be used to transport service users and staff to other areas. Every effort must be made by arrangement with carers and relatives to relocate all unaffected non-residential service users as quickly as possible to enable CWP staff to assist in other essential areas.

10.3 Staff working away from their office base

When a lockdown incident occurs many CWP staff may be away from their office base, working at a remote site working in the community as part of their duties.
Line managers must contact all staff, ascertain their safety and give the instruction/update regarding their returning to the base at the site which may be affected by the lockdown.

This is so that staff can:

- Inform their manager of their current location;
- Receive instructions from their manager about any changes to their duties arising from the incident

10.4 Defining site/building lockdown

A lockdown is achieved through a combination of physical security measures and the deployment of security personnel'.

- A **full lockdown** is the process of preventing freedom of entry to and exit from either an entire NHS trust site or from a specific NHS building

- A **partial lockdown** can be defined in a number of ways. In most instances, a partial lockdown is the locking down of a specific part of a trust site or a specific building or part of a building. A partial lockdown is also when entry restrictions are placed on a specific building to control the flow of people into it – via identification checks for example. This is also known as 'controlled access' to a site or building.

- A **portable lockdown** is when an ongoing lockdown is moved from one location on a trust site to another.

- A **progressive lockdown**, which can also be called an **incremental lockdown**, can be a step-by-step lockdown of a trust site or building in response to an escalating scenario.

- **Critical Asset - High risk** – site or part of site/building is a high-profile area/building as it contains a critical asset, either physical or non-physical.

- **Moderate risk** – site or part of site/building is a moderate-profile area/building, the asset is important but not critical and the building and security profile is marginally adequate but could be improved.

- **Low risk** – site or part of site/ building is not a high-profile area/building as it does not contain a critical asset, and the existing building and security profile is adequate.

10.5 Arrangements for producing a lockdown risk profile for each organisational site or building

(For information relating to risk profiles of CWP main inpatient sites please refer to appendix 1 - 2)

Needs Analysis – in order to be able to develop a Lockdown plan a Needs Analysis of the CWP building and a breakdown of the relevant individual sites, buildings and areas that may be affected by

a lockdown will be required. The purpose of this analysis is to identify the capability of CWP to instigate a lockdown in terms of the resources required. The organisation will need to ensure there are the required number of a staff/security personnel, adequate locks and control mechanisms that meet the necessary safety and security standards for each site where CWP has a responsibility to produce and maintain a Lockdown risk profile for, and that once these have been identified the funding can be sourced. This Needs Analysis process will be coordinated by the Emergency Planning Lead

- The Emergency Planning lead will prioritise each area to ensure that resources and funding is allocated appropriately, according to a risk rating.

Identify Critical Assets – each of the identified sites, buildings and areas will need to identify the critical assets contained within them. Some of the CWP buildings and departments contain expensive, business critical kit and equipment and consideration must be given to the clinical and business risk associated with any subsequent loss or damage.
Identify potential threats, hazards, risks – each individual site, building and area must be assessed for the internal threats and risks associated with it. The assessment of the risk of threats and hazards must be carried out in the context of both people and property. (see Diagram 1) illustrates an example of potential threats and hazards which may apply within the organisation).

Diagram 1.

Malicious Threats to Persons	Malicious threats to buildings and estate	Malicious threats to Property	Potential Lockdown hazards
Violence against staff, patients and visitors	Vandalism	Thefts of Hospital Assets and personal property	Flood
Abuse against staff, patients and visitors	Unlawful entry	Thefts of Clinical Supplies and products	Fire
Terrorism	Terrorism	Terrorism	Contamination and CBRN

Site/Building Vulnerability Assessment - In the event of a site lockdown being implemented it is essential that in addition to determining the critical assets and potential risks and hazards within CWP buildings that an assessment is also made of the vulnerability of the specific hospital site or building. This will be carried out by the Emergency Planning Lead with regard to the physical geography and location of the site, particularly in relation to potential hazard or risk areas in conjunction with partner organizations who share the site.

- To minimize the incidents of security breaches on CWP sites during a lock down period a map or site profile of the physical geography of the healthcare site i.e. the size of the site, marking out its perimeter, access and egress points, the location and route of communications and the number of buildings onsite with up-to-date site maps, floor plans and aerial maps, will be available from the respective Estates Department during any lock down period. These plans and maps will be made accessible to all emergency leads such as the police and the CWP Executive or Emergency Planning/Incident Lead.

- Specific consideration must be given to the location and security of fire doors, and no Lockdown Plan can compromise Fire Safety Legislation. The CWP Fire Adviser will provide expertise advice to the project team on matters relating to fire regulations.

- As part of the lockdown plan a security review of the identified locations will also be carried out by the CWP Security Services Manager. The purpose of this is to focus on the existing security measures, considering their vulnerabilities that may hamper an attempt to instigate

a Lockdown within that area. Out of office hours this role will be carried out by the Emergency Planning Lead

Critical Asset Protection

Critical asset protection or the protection of assets which are central to ensuring the day to day continuity of CWP core business will be identified and locally risk rated by the CWP Emergency Planning Lead and operational plans developed to ensure that these areas are prioritised in the development of plans going forward during a lock down period;

- **High risk** – Non-identified
- **Moderate risk** – Fuel storage containers, External generators, CWP vehicles
- **Low risk** – Access and egress points from the main buildings

10.6 Operational staff roles and responsibilities

When lockdown is called by the CWP Executive or Emergency Planning/Incident Lead, either partial or total, this will be managed locally by CWP staff, and these staff will have specific roles and responsibilities they have to carry out a lockdown in a safe and controlled manner. (For further information specific to individual staff/team roles during a Lock Down incident please refer to the action cards detailed in appendices 3 - 7).

Lock down roles will be broken into 4 stages;

I. **'Lockdown activation'** – this stage considers the role of staff at the initiation of a lockdown – for example, where they have to report to, and what resources they may need to facilitate their role.
II. **'Lockdown deployment'** – this stage considers the roles staff may be assigned to during a lockdown, and how these can be facilitated.
III. **'Lockdown maintenance'** – this stage considers some of the features that should be taken into account to maintain a lockdown, and how these can be achieved.
IV. **'Lockdown stand-down'** – this stage focuses on how staff can facilitate the end of a lockdown.

10.7 Internal communications

When a decision is made to implement a full or partial lock down of any main inpatient area by the CWP Executive or Emergency Planning/Incident Lead this will immediately be relayed to the key operational staff via the service leads/bleep holders. All non-clinical staff involved in the lock down process will be provided with a communication device (porters only) and given clear instruction on when and how to use it by the line manager or incident coordinator. All local internal communications between the CWP Executive or Emergency Planning/Incident Lead will be through the local incident coordinator.

10.8 External communications with stakeholders

CWP Head of Communications is part of the Major Incident Team and in the event of any lockdown occurring will be advising on the approach to handling the media, internal and stakeholder communications. This would also involve devising proactive and reactive messages. (In the Head of Communications absence the public relations officer would step-up to fill this role). CWP Communications Team will manage the press office phones on the following phone numbers 01244 397 407/397 406, recording all interactions on the media enquiries form.

Mirroring internal communications between staff, external communications with the police and other emergency services will be robust and through a single point of contact. The command and control system will identify the CWP Executive or Emergency Planning/Incident Lead who the police and emergency services will be liaising with on strategic and operational issues. All communications with other agencies will only be coordinated through CWP Communications team as per policy.

10.9 Safe and control zones

In the event of a major incident which results in a lockdown – whether partial, progressive or full - safe and control zones will be identified in all affected main inpatient buildings.
The nature of the event will determine the location of safe and control zones i.e. building construction and proximity to high-risk areas will determine bomb and blast safe zones. The identified zones are rooms or other areas which people will occupy or use in the event of an incident and also casualties can take refuge here if necessary.

Furthermore these zones will be vital in crowd management as people can be siphoned off into these zones for their own safety especially when surges in people are expected on site. A safe zone can also be 'portable' and used by emergency services if there is a risk of contamination.

10.1.0 Traffic management

All traffic management issues on the main inpatient sites will be the responsibility of the host organisation. CWP Security officers will be asked to facilitate local onsite traffic management during a lockdown. Emergency signage will be needed to direct traffic to ensure the flow of traffic through the site or direct traffic to designated staff and public car parks. Coordination of all traffic will be through the CWP Executive or Emergency Planning/Incident Lead. (Please refer to appendix 7 for signage example to be issued during a lockdown incident)

10.1.2 Workforce factors

To support a lockdown, CWP will calculate its own staff participation requirement, keeping these numbers under frequent review in accordance with the Emergency Plan policy.

10.1.3 Crowd management and control

a) All responsibility for the management of members of the public will be with the Police and CWP Security personnel will take the lead from them either on the ground or through the local incident lead.

10.1.4 Evacuation

An evacuation plan and lockdown plan are mutually supportive and if a lockdown continues to the point at which CWP can no longer adequately function, a partial or full evacuation of a site or building may be necessary. This will be undertaken in accordance with CWP policy and local continuity business plans.

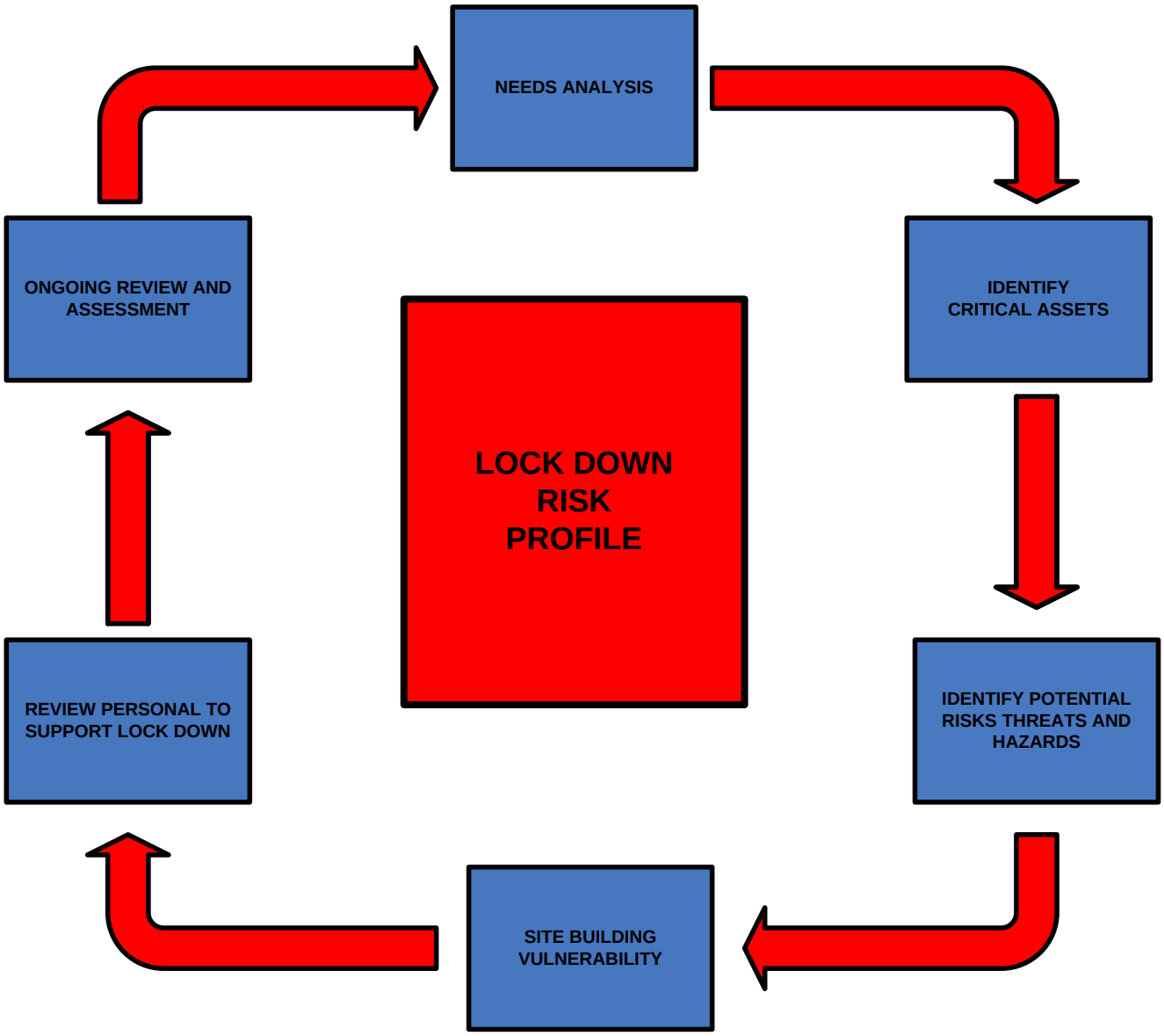
10.1.5 Lockdown stand-down

The CWP Executive or Emergency Planning/Incident Lead will instigate the stand-down authority which will be communicated directly to the local leads who will verify the instruction before taking any action. On stand-down all doors and barriers will be removed in an orderly fashion to enable the trust to return to normal services as promptly as possible. Staff will remain on duty until instructed to leave or reassigned to other duties. A local debrief will take place as soon as is practical with those staff who are involved. Further debriefs will be communicated using normal trust communication service after the event.

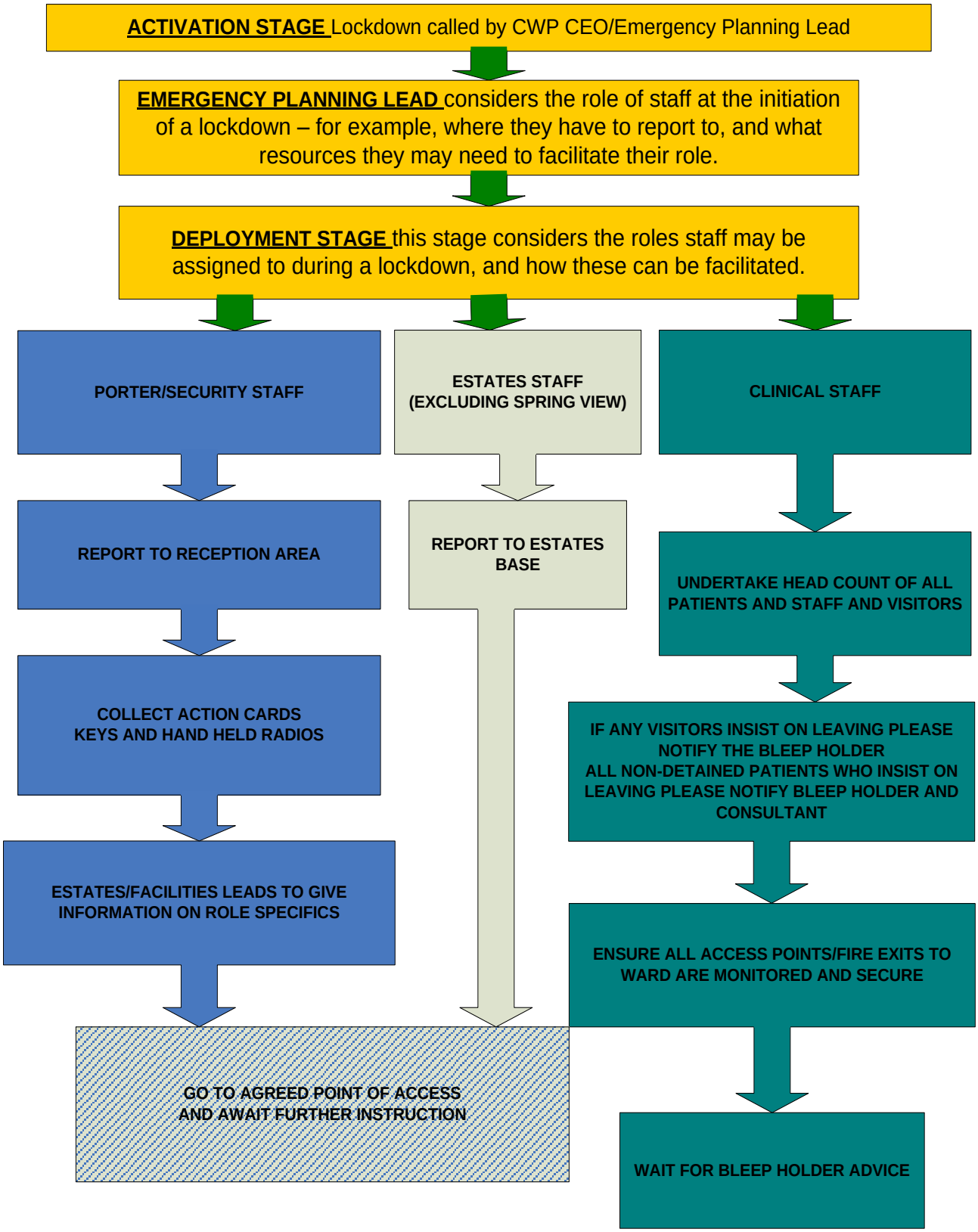
10.1.6 Recovery

A recovery plan will be developed through the Emergency Planning Lead and agreed with Executive Board. The CWP Safety and Security Lead and CWP Security personnel will also be able to ensure the security of buildings during the recovery process**.**

Appendix 1 – Lock Down Risk Profile



Appendix 2: Operational roles of key CWP staff during a lock down activation and deployment



Appendix 3

ACTION CARD – Local Incident Team Lead

Role - Manage the Local incident team

Reports to Trust Incident Officer

1. Agree role with Trust Incident Officer.

2. At first team meeting confirm your role, which is:

- To ensure that team members follow established communications procedure
- To maintain a watching brief on issues management i.e. to ensure that correct links with incident staff is being maintained
- To establish and maintain contact with CWP Incident Lead and to brief them on progress of actions taken and to obtain updates from them.

3. Report timely and accurately information to incident support staff

4. Ensure that incident support staff are supported and rotated at regular intervals

Appendix 4

ACTION CARD – Incident Support Staff (Porter / Security on duty)

1. On receiving the information that a lockdown incident has been declared they should inform their Line Manager.

2. Off duty members of the Portering Staff can be called in for duty, as deemed necessary by the Incident Manager.

3. They will then report to the Local Incident Lead to receive instruction.

4. The Porters, in conjunction with Security, will control access to the site and buildings, ensuring there is access for the Emergency Services.

5. Porters will move furniture and equipment required for the incident.

6. On receiving instruction ensure that they have an operational hand held radio and/or mobile phone

7. If the lockdown occurs during night time or when visibility is poor Porters must have access to a torch

8. Ensure hourly contact is maintained with Local Incident Lead

Appendix 5

ACTION CARD – Incident Support Staff (Estates Officers)

Role - Support Trust Incident Lead and Emergency Services during an incident

1. On receiving the information that a lock down incident has been declared Estates Staff should inform their immediate manager.

2. During normal working hours Estates Staff will be assembled at a local estates department to receive instruction.

3. Outside normal working hours the emergency on call staff will be called in as necessary, to assist with the incident. The most senior estates officer will ascertain the staffing requirements and, if necessary, contact resting staff to attend.

4. The Local Estates Manager will direct the estates team to assist the Emergency Services as requested.

5. The Local Estates Manager will direct the Estates staff to assist the Local Incident Lead as requested.

Appendix 6

Action Card - General designated staff response protocol

Will all staff on receipt of a request to assist with the lockdown of the site/building during a major incident, please return immediately to your designated office area:

- Collect appropriate keys and signage for your area of responsibility.
- Ensure collection of communication device (if appropriate) i.e. mobile, handheld radio and/or landline number is known
- Report to local incident lead and agree duty to be carried out.
- Secure designated area preventing access or egress and directing staff to the controlled area.
- Report regularly to the local lead staff.
- On ‘stand down’, which is declared by CWP Emergency Planning lead or senior executive on-call, through the communication chain, report back to porters office and return emergency equipment etc.
- Return to own office area and return keys to secure cabinet.
- Resume normal duties or agree with line manager shift handover.

Appendix 7 - Incident in progress

A LOCKDOWN OF THIS SITE/BUILDING CURRENTLY IN PROGRESS

FOR YOUR OWN SAFETY AND THE SAFETY OF OTHERS PLEASE DO NOT ATTEMPT TO LEAVE OR ENTER THIS BUILDING.

FOR FURTHER INFORMATION

PLEASE CONTACT

(01244) 39_____