Security and Lockdown Policy

# Document Control:

| **Document Control Information** | **Details**  |
| --- | --- |
| Policy Name | Security and Lockdown Policy |
| Policy Number | MSEICB 029 |
| Version | 1.0 |
| Status | Final |
| Author / Lead | Director of EstatesHead of Corporate Governance, MECCGBusiness Continuity & EPRR Officer |
| Responsible Executive Director | Director of Resources / Chief of Staff  |
| Responsible Committee | Audit Committee |
| Date Ratified by Responsible Committee | 20 May 2022 |
| Date Approved by Board/Effective Date | 1 July 2022 |
| Next Review Date | 1 July 2024 |
| Target Audience | Board members, sub-committee members and all staff working for, or on behalf of the Integrated Care Board (ICB) |
| Stakeholders engaged in development of Policy (internal and external)  | Director of EstatesHead of Corporate Governance, MECCGHead of Emergency PlanningLocal Security Management SpecialistInformation Governance Lead |
| Impact Assessments Undertaken *(Delete if non-applicable)* | * Equality and Health Inequalities Impact Assessment
 |

# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author (Name and Title) | Summary of amendments made |
| 0.1 | 12/04/22 | Jo Martindale | Draft ICB Policy |
| 0.2 | 12/04/22 | Sara O’Connor | Significant changes made to make policy brief and in line with ICB policy template.  |
| 0.3 | 21/04/22 | Sara O’Connor | Revised following review by LSMS |
| 0.4 | 13/05/22 | Jo Martindale | Revised following review by further CCG stakeholders |
| 0.5 | 22/05/22 | Jo Martindale  | Reviewed against Policy checklist, Policy leads to be confirmed  |
| 1.0 | 31/12/22 | Sara O’Connor | Final version with responsible officers’ details.  |

**Contents**

[1. Introduction 5](#_Toc123305324)

[2. Purpose / Policy Statement 5](#_Toc123305325)

[3. Scope 6](#_Toc123305326)

[4. Definitions 6](#_Toc123305327)

[5. Roles and Responsibilities 7](#_Toc123305328)

[5.1. Chief Executive 7](#_Toc123305329)

[5.2. ICB Board 7](#_Toc123305330)

[5.3. Audit Committee 7](#_Toc123305331)

[5.4. Security Management Director (SMD) 8](#_Toc123305332)

[5.6. Local Security Management Specialist (LSMS) 8](#_Toc123305333)

[5.7. NHS Alliance Directors, Executive Directors and Other Managers 9](#_Toc123305334)

[5.8. All Staff 10](#_Toc123305335)

[6. Policy Detail 11](#_Toc123305336)

[6.1. Violence and Aggression 11](#_Toc123305337)

[6.2. Reporting of Crime/Security Incidents 11](#_Toc123305338)

[7. Key Aspects of Security/Potential threats and hazards 11](#_Toc123305339)

[7.2. Children’s Act (1989 & 2004), Safeguarding Vulnerable Groups Act (2006) as amended by the Protection of Freedoms Act s66 (2012)(2006), and Care Act (2014) 12](#_Toc123305340)

[7.3. Staff Identification 12](#_Toc123305341)

[7.4. Access and Egress 12](#_Toc123305342)

[7.5. Security of Goods 13](#_Toc123305343)

[7.6. Vehicle Security 14](#_Toc123305344)

[7.7. Fraud 14](#_Toc123305345)

[7.8. Information Security 14](#_Toc123305346)

[7.11. Verbal & Physical Assault or Unreasonably persistent individuals demonstrating unacceptable behaviour 16](#_Toc123305347)

[7.12. Lost Property 16](#_Toc123305348)

[8. Lockdown Procedure 16](#_Toc123305349)

[8.1. Lockdown 16](#_Toc123305350)

[8.2. Lockdown roles and responsibilities 17](#_Toc123305351)

[8.3. ICB Fire Marshals 17](#_Toc123305352)

[8.4. Managers/Directors 17](#_Toc123305353)

[8.5. Other Staff 18](#_Toc123305354)

[8.6. Head of Communications 18](#_Toc123305355)

[9. Procedures and Processes 18](#_Toc123305356)

[9.1. Major Incident Plan 18](#_Toc123305357)

[9.2. Business Continuity during Lockdown 18](#_Toc123305358)

[9.3. Activation of a Lockdown (refer to actions cards) 18](#_Toc123305359)

[9.4. Full Lockdown 19](#_Toc123305360)

[9.5. Partial and Progressive Lockdown 19](#_Toc123305361)

[9.6. Staff Deployment 19](#_Toc123305362)

[9.7. Maintaining a Lockdown 20](#_Toc123305363)

[9.8. Stand Down 21](#_Toc123305364)

[9.9. Lessons learnt 21](#_Toc123305365)

[10. Dissemination and implementation process, including training 21](#_Toc123305366)

[10.1. Dissemination and implementation 21](#_Toc123305367)

[10.2. Monitoring Compliance 21](#_Toc123305368)

[10.3. Policy development 21](#_Toc123305369)

[10.4. Staff Training 21](#_Toc123305370)

[11. Arrangements For Review 22](#_Toc123305371)

[12. Associated Policies, Guidance And Documents 22](#_Toc123305372)

[13. References 23](#_Toc123305373)

[Appendix A - Equality Impact Assessment 24](#_Toc123305374)

[Appendix B – Bomb Threat Action Plan 27](#_Toc123305375)

[Appendix C – Theft 28](#_Toc123305376)

[Appendix D – Harassment 29](#_Toc123305377)

[Appendix E – Suspicious Packages 31](#_Toc123305378)

[Appendix F – Action Cards 33](#_Toc123305379)

[Appendix G – Lockdown details 35](#_Toc123305380)

## Introduction

The ICB recognises its responsibility to have effective security measures in place to provide a safe environment for all MSE ICB personnel, property, and assets. This policy sets out the ICB’s security arrangements and outlines the response procedures should a lockdown be required in the event of a major incident occurring.

## Purpose / Policy Statement

Mid and South Essex (MSE) Integrated Care Board (ICB) is committed to providing a secure environment for the protection of patients, staff and legitimate visitors and where possible protecting them from harm, or fear of harm, arising from crime or other incidents.

The ICB is also committed to protecting the property of the NHS (both physical and intellectual) from fraud, theft, loss and damage and will provide reasonable measures and resources to create and maintain a secure environment to support this commitment.

The ICB recognises that it is not possible to prevent every unforeseen security incident. Emphasis will be placed on the prevention of security incidents and advising staff on how to deal with any breaches.

The ICB’s premises are:

* Wren House, Hedgerows Business Park, Colchester Road, Chelmsford, CM2 5PF.
* Phoenix House, Christopher Martin Road, Basildon SS14 3HG.
* Civic Offices 2nd Floor, New Road, Grays RM17 6SL.

Controlled access to ICB premises will be maintained to allow staff to operate with the minimum of hindrance and to afford legitimate visitors access to appropriate areas.

MSE ICB premises are not solely occupied by the ICB. It will therefore be necessary to work with other occupiers to implement security arrangements or in the event of a security incident.

In line with NHS Security Management guidance the organisation has in place an accredited Local Security Management Specialist (LSMS) responsible for security who will ensure compliance with NHS national strategies, guidance and security management standards.

The founding principles of security management are:

* + 1. **Strategic Governance** - This ensures that security management is embedded throughout the organisation, led by the Security Management Director (SMD) and Local Security Management Specialist (LSMS). The aim is to ensure that anti-crime measures are embedded at all levels across the organisation.
		2. **Inform and Involve** – This involves setting out the requirements in relation to raising awareness of crime risks faced by the NHS and working with NHS staff, stakeholders and the public to highlight these risks and the consequences of crime against the NHS.
		3. **Prevent and Deter** - This involves setting out the requirements in relation to discouraging individuals who may be tempted to commit crimes against the NHS and ensuring that opportunities for crime to occur are minimised.
		4. **Hold to Account** - This involves setting out the requirements in relation to detecting and investigating crime, prosecuting those who have committed crimes and seeking redress.

## Scope

This policy applies to the following (collectively known as members of staff):

* + - Mid and South Essex (MSE) Integrated Care Board (ICB) members
		- Members of staff (including temporary/bank/agency/voluntary/work experience staff).
		- Contractors engaged by the ICB.
		- Members of staff from other MSE Health and Care Partnership (HCP) organisations who are members of ICB Committees/Sub-Committees, advisory groups/other groups or otherwise involved in ICB business.
	1. The policy applies to all areas of the ICB’s responsibilities and activities and all ICB premises and other assets.

## Definitions

* **Incident -** An event or circumstance which could have resulted, or did result in, unnecessary damage, loss or harm to staff members, visitors or members of the public.
* **Local Security Management Specialist (LSMS)** –an accredited specialist with responsibility for advising the ICB on security matters.
* **Major Incident** - any occurrence that presents serious threat to the health of the community or causes such numbers or types of casualties, as to require special arrangements to be implemented.
* **Security Management Director –** Executive member of the ICB Board with responsibility for Security. The [insert job title] will perform this role.
* **Security Threat –** a malicious event instigated by an individual or group which has the potential to cause loss or damage to an asset. This could include cyber-attacks or a terrorist attack.
* **Hazard –** source of potential danger or adverse conditions.

## Roles and Responsibilities

### Chief Executive

* + 1. The Chief Executive of the ICB has overall accountability for security and lockdown management within the ICB, including provision of adequate resources and infrastructure, in line with legislation, guidance and standards issued by NHS England and Improvement (NHSE/I).

### ICB Board

* + 1. The Board is accountable and responsible for ensuring that the ICB has an effective programme for identifying and managing security risks and that local procedures exist for situations requiring the lockdown of ICB premises. The Board will seek regular assurance from a range of sources, including from its committees, that security and lockdown arrangements are effective and will ensure further mitigating action is taken where necessary.

### Audit Committee

* + 1. The Audit Committee has responsibility for monitoring the ICB’s compliance with this policy and is the ‘sponsoring committee’ referred to in Section 10 below. The Committee will escalate any significant security risks to the attention of the ICB Board.
		2. The Audit Committee will approve the annual security work plan and receive regular reports from the LSMS, and an annual report, confirming activities undertaken against the security work plan each year.
		3. The Chair of the Audit Committee will be the Non-Executive Member of the Board who will maintain oversight of security.

### Security Management Director (SMD)

* + 1. Within Mid & South Essex ICB, the Director of Resources is the Executive Director with responsibility for security management, which is delivered via the governance team. The role of the SMD includes:
* Developing the Organisational Crime Profile, the Security Review Tool and the security management work plan.
* Reporting security progress and significant risks to the Board.
* Overseeing the preparation, planning and response to a major incident including lockdown and security management, ensuring on-going business continuity, whilst leading on issues relating to the functionality of buildings and building resilience.
* Advising on identifying critical assets and assessing risk.
* Liaison with police and other emergency services during a lockdown.
* Liaison with other occupiers of ICB premises during a lockdown.
* Enhancing security capability, including implementing physical measures such as panic alarms, lockable doors and access control.
* Maintenance of security measures, including testing alarms and changing lock codes regularly.
* Secure storage and use of equipment and valuables.
* Management of specific risks relevant to the building use.
* Safe use and access to patient information and corporate, confidential data.

**Collaboration Hub Programme Lead**

* + 1. The Collaboration Hub Programme Lead has operational responsibility for ensuring that this policy and associated plans, procedures and systems are in place, implemented, monitored, and reviewed.
		2. The Collaboration Hub Programme Lead will support the SMD in identifying critical assets, assessing risk and will be instrumental in ensuring staff are aware of this policy and their roles.

### Local Security Management Specialist (LSMS)

* + 1. The ICB will nominate a suitably qualified individual as the Local Security Management Specialist (LSMS). The LSMS is responsible for providing a comprehensive security management and professional advisory service to the ICB.
		2. The LSMS will prepare an annual workplan which will cover the key elements included within 2.8 above and which:
* Helps to prevent and or target security related incidents
* Helps to reduce the impact of security incidents to MSE ICB
* Manages all security risks within the including, Violence & Aggression, Abuse (physical & verbal) harassment, criminal damage, theft, and risks to lone workers both in the community, working at home and working alone in offices.
	+ 1. The LSMS will:
* Identify any security related risks relevant to the ICB through proactive work undertaken or as they emerge locally or nationally.
* Provide support to the ICB in meeting all relevant security standards and requirements.
* Reviewing all security related policies, procedures and guidance and provide input as required.
* Review the arrangements for the security of staff and assets throughout the ICB with through targeted proactive reviews and crime risk assessments.
* Review collated incident related data to identify trends, target areas where specific security awareness is required, to provide support and assistance to staff involved in incidents and, to pursue sanctions where required.
* To provide advice, guidance, and awareness to all ICB staff on security related risks and emerging issues and the requirement for the effective reporting of all relevant incidents and of their responsibilities for security within the ICB.
* To compete and advise on all security related risk assessments.
* To provide advice, support, and input to all security related training for staff including (but not limited to) Conflict Resolution, Lone Working and De-escalation.
* To review evidence and risk assessments supporting compliance with the new Violence Prevention and Reductions Standard and to assist in the interpretation of the requirements of the criteria within the standard.

### NHS Alliance Directors, Executive Directors and Other Managers

* + 1. The NHS Alliance Directors, Executive Directors and other managers are responsible for ensuring that appropriate and effective security processes are in place within their designated areas and scope of responsibility and that they comply with the requirements of the ICB’s security arrangements, including regularly reviewing security arrangements with their staff at directorate/departmental meetings and escalating risks to the appropriate Committee or Board.
		2. They are responsible for ensuring that all members of their staff are aware of security arrangements relevant to their area of work and of their personal responsibilities as set out in section 5.8 of this policy. They must ensure their staff receive appropriate information, instruction and training to enable them to undertake their roles securely and safely.

### All Staff

* + 1. All members of staff, whether directly employed, seconded, or aligned to the ICB, are responsible for contributing to and participating in crime prevention and implementing this policy and associated procedures.
		2. All staff are responsible for identifying and highlighting any specific security training needs and attending relevant training according to their role.
		3. All staff are required to:
* Comply with security procedures and access controls relevant to their workplace.
* Familiarise themselves with general security risks and those relevant to their role.
* Report actual or suspected security breaches (e.g. stolen equipment, signs of attempted break-in, suspected intruders) to their manager and in line with the Incident Reporting and Management Policy.
* Take sensible steps to safeguard themselves, colleagues, patients, and others ‘so far is as reasonably practicable’.
* Where relevant, follow procedures implemented to safeguard staff when ‘lone working’ – see [ICB Lone Worker Policy Ref MSEICB020](https://www.midandsouthessex.ics.nhs.uk/publications/?publications_category=icb-policies)
* Take sensible steps to safeguard equipment and property (both physical and intellectual).
* Attend all security/safety training identified as necessary by the organisation.
* Use effectively (and not damage or tamper with) security equipment such as key-coded locks and electronic security systems/fobs.
* Take responsibility for ensuring the security of their own possessions whilst at work, by keeping personal possessions at work to a minimum and not to bring valuable or sentimental items to work.
* Ensure that that their ID badge is worn while on ICB premises.
* Report loss of an ID badge, swipe card or access fob to the relevant manager.
* Staff working in areas controlled by another organisation should familiarise themselves and follow security procedures for that organisation.
* Be aware that any deliberate or serious neglect of security measures could result in disciplinary action being taken.

## Policy Detail

### Violence and Aggression

* + 1. The Health and Safety Executive (HSE) defines work-related violence as 'Any incident in which a person is abused, threatened or assaulted in circumstances relating to their work.'
		2. The ICB’s arrangements in place for violence and aggression are contained within the ICB’s [Health and Safety Policy](https://www.midandsouthessex.ics.nhs.uk/publications/?publications_category=icb-policies) and the [Management of Violence and Aggression Policy](https://www.midandsouthessex.ics.nhs.uk/publications/?publications_category=icb-policies).

### Reporting of Crime/Security Incidents

* + 1. Where staff observe a crime/security incident and an urgent response is required, staff should call the police immediately by telephoning 9-999 (from land line at ICB premises) or 999 from mobile and other phones but, only where it is safe to do so. Staff should make sure they are not at any risk of harm by making the phone call.
		2. If the incident does not require an immediate response or reporting but does require police assistance or advice, staff should contact the police on 101 which it the non-emergency number.
		3. If staff need any support or advice about reporting security related incidents, then they should contact their line manager, the SMD or the LSMS, as soon as possible who will advise on the most appropriate course of action.
		4. Staff should complete an incident form in accordance with the ICB Incident Reporting Policy.

## Key Aspects of Security/Potential threats and hazards

The ICB must have clear and defined arrangements to deal with actual or potential threats and hazards by:

* The identification of all relevant hazards to the protection of all staff
* Completion and on-going review of suitable and sufficient risk assessments (with LSMS support)
* Undertaking crime reduction surveys to identify any risks of loss, theft, or damage to ICB assets
	+ 1. Information about these threats and hazards will be available to the ICB through risk registers, local and regional resilience fora, police forces, other emergency services, the LSMS and Counter Terrorism Security Advisors.
		2. Other considerations are set out in Sections 7.2 to 7.12.

### Children’s Act (1989 & 2004), Safeguarding Vulnerable Groups Act (2006) as amended by the Protection of Freedoms Act s66 (2012)(2006), and Care Act (2014)

* + 1. The organisation will also use the Disclosure and Barring Service (DBS) for eligible positions/roles under current legal provisions to make safer recruitment decisions and prevent unsuitable people from working with children and adults.

### Staff Identification

* + 1. Every employee within the first week of commencing employment will be issued with an identification card/badge by the ICB’s Human Resources (HR) Department. Upon termination of employment the line manager must recover and return the card/badge to the HR Department for destruction.
		2. All staff should always wear their ID badge whilst on ICB premises, or when representing the ICB.
		3. Temporary ID cards/ badges will be issued to all persons undertaking work experience, voluntary work or employed by the ICB. The issuing of temporary ID badges should be strictly controlled and badges must be collected at the end of the assignment period.
		4. Staff should be mindful of the need to challenge anyone they do not recognise regardless of whether they are wearing an ID badge and not allow them access to any building without valid reason.
		5. Staff should make sure that all doors are appropriately locked behind them when entering buildings and not allow any opportunity for tailgating by individuals they do not recognise.
		6. The loss of an ID badge must be reported immediately by the employee to their manager and the HR Department. An incident form must also be completed.

### Access and Egress

* + 1. Every employee within the first week of commencing employment will be issued with a ID Card by Human Resources which is designed to enable access to Wren House and Phoenix Court. Employees must then contact the Collaboration Hub Programme Lead to configure the card for door access.
		2. At termination of employment the Line Manager must ensure the fob is returned to Human Resources who will liaise with the Collaboration Hub Programme Lead to disable access.
		3. Access to the building will be restricted out of hours (between 22.00- and 07.00 hours at Wren House ad 20.00-07.00 at Phoenix Court) using locks/digital locks. Further restrictions to access will be applied in the event of a major security incident or in response to the National Threat Level being escalated.
		4. Access to certain areas within the building, e.g. Information Technology Room server rooms, will be controlled by the use of digital locks, electronic alarm systems and/or restricted access to keys.
		5. Windows will be fitted with restrictors limiting the extent to which they can be opened (unless the relevant fire risk assessment states otherwise) and must be closed by staff at the end of each day.
		6. Keys to premises will remain under the responsibility of the Collaboration Hub Programme Manager and must be labelled clearly and stored in an orderly way. All keys must be held in a lockable cabinet and a record maintained of the issue and return of keys.
		7. Visitors should be asked to report to reception and be met by the person who has invited them. Visitors should also be accompanied to reception when leaving the building and asked to sign-out.

### Security of Goods

* + 1. Goods received into departments must be checked against delivery notes prior to signing for acceptance.
		2. Any member of staff who signs for any goods on behalf of the ICB is accountable for any discrepancies which may occur. All packages delivered must be identified and checked against delivery notes prior signing. The delivery note must not be signed unless you are sure that all items have been accounted and any discrepancies noted.
		3. Any discrepancies outstanding must be recorded accurately along with name and signature of the person delivering. The supplies department / stores must be informed.
		4. Packages must not be left in a position where they may create a safety/fire risk.
		5. Records must be updated as soon as possible, including any inventory or stock control.
		6. Staff should not attempt to open and parcel, envelope or package that looks suspicious and should refer to Appendix E for guidance in handling suspicious packages.

### Vehicle Security

* + 1. Staff using private vehicles for work must ensure that at no time is patient sensitive information, other personal identifiable information or commercially sensitive information left unattended or on view in vehicles, this includes either in hard paper copy, on laptops or memory sticks.
		2. Where it is essential that confidential documents are transported in staff cars, they must be stored in the boot of the car and remain out of sight.
		3. All medical equipment transported from the organisation premises for use by clinicians in clinics or patients’ homes remains the responsibility of the clinician using or person transporting the equipment.
		4. All equipment must be stored out of sight. At no time should MSE ICB property be left unattended in staff vehicles overnight.
		5. Providers of parking facilities will not accept liability for any theft or damage to motor vehicles.
		6. It is the responsibility of the user of a motor vehicle used on ICB business to ensure that the correct public road user documents (namely a current insurance certificate or cover note, which includes cover for business use; MOT test certificate; and vehicle excise licence) are valid for the vehicle.
		7. Staff should also refer to the ICB Lone Working Policy in relation to vehicle safety measures where applicable.

### Fraud

* + 1. The Chief Finance Officer and/or the ICB Local Counter Fraud Specialist must be alerted immediately of any suspicions of fraud. Please refer to the [Anti-Fraud and Bribery and Corruption Policy](https://www.midandsouthessex.ics.nhs.uk/publications/?publications_category=icb-policies) for further information.

### Information Security

* + 1. The objective of information security is to ensure faith in the bond of confidentiality between the organisation and its patients/clients and staff. It should aim to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.
		2. The Senior Information Risk Owner (SIRO) has direct responsibility for ensuring the Information and Cyber Security Policy is maintained and providing advice and guidance on its implementation. Details on who holds the post of SIRO, and the responsibilities associated with the role, are available in the ICBs [Information Governance Framework and Policy](https://www.midandsouthessex.ics.nhs.uk/publications/?publications_category=icb-policies).
		3. The [Information and Cyber Security policy](https://www.midandsouthessex.ics.nhs.uk/publications/?publications_category=icb-policies) ensures that:
* Information will be protected against unauthorised access.
* Safeguards are in place to protect the confidential information.
* The integrity of information will be maintained.
* Regulatory and legislative requirements will be met.
* Business continuity plans can be produced, maintained and tested.
* Information security training will be available to all staff.
* All breaches of security, actual or suspected, will be reported to and investigated by the LSMS and the Information Governance Lead and the MSE ICB Information Governance Team. Standards will be produced to support the policy. These may include virus control, access control, passwords and encryption.
* Business requirements for the availability of information and information systems will be met.
	+ 1. The Chief Finance Officer has direct responsibility for ensuring the Information and [Cyber Security Policy](https://www.midandsouthessex.ics.nhs.uk/publications/?publications_category=icb-policies) is maintained and providing advice and guidance on its implementation.
		2. It is the responsibility of each employee to adhere to the policy. All staff must abide by the code of confidentiality issued by the ICB which seeks to ensure all information matters relating to the organisation, their employment, other members of staff and the general public comply with the Caldicott Principles and Government legislation, for example: -
* Data Protection Act 1998.
* The Computer Misuse Act 1990.
* Copyrights and Patents Act 1998.
* The Human Rights Act 1998.

**Major Incident**

* + 1. A major incident is defined as any occurrence that presents serious threat to the health of the community or causes such numbers or types of casualties, as to require special arrangements to be implemented. Further information about the types of incidents within the NHS and the relevant response can be found in ‘NHS England Summary of key strategic guidance for health emergency Preparedness, Resilience and Response (EPRR)’.

**Bomb Threat and Suspicious Packages**

* + 1. All NHS staff and premises could be at risk of terrorist threats who may be motivated to plant devices with a view to damaging property or to cause injury or death to individuals. Any suspicious package, parcel or envelopes should NOT be moved and its position should be reported to line management. A copy of the Bomb Threat Action Plan is attached at Appendix B and a procedure for dealing with suspicious packages at Appendix E.
		2. The vast majority of bomb threats are hoaxes but, should always be reported to the police as making such malicious calls is a criminal offence under the Criminal Law Act 1977.

### Verbal & Physical Assault or Unreasonably persistent individuals demonstrating unacceptable behaviour

* + 1. The ICB will provide a secure environment, so far as is reasonably practicable, which protects staff and visitors from physical and verbal assaults or anti-social behaviour. Please refer to the Management of Violence and Aggression Policy.
		2. Unreasonably persistent individuals demonstrating unacceptable behaviour can be a challenge for NHS staff. The Management of Violence and Aggression Policy includes template letters for dealing with this type of behaviour.

### Lost Property

* + 1. Property that has been found on the ICB premises should be adequately recorded and stored by the receptionist, who will make reasonable efforts to locate the owner of the property.
		2. If the owner of valuable items, e.g. keys, jewellery, mobile phones, is not quickly identified, the receptionist will report lost property to Essex Police using [this link](https://www.essex.police.uk/ro/report/lp/lost-or-found-property/). In the case of credit/debit cards, the issuing bank will be contacted.
		3. Any lost property not claimed within six months will be disposed of or, if appropriate, donated to a recognised charity, subject to written approval by the SMD which must fully document where and when the property was found, action taken to locate the owner, the agreed method and date of disposal.

## Lockdown Procedure

### Lockdown

* + 1. The purpose of this policy includes preparing and planning for serious security incidents or unexpected situations that may require a full or partial lockdown. Any lockdown will need to be managed and controlled to maintain the health and safety of all occupants and security of ICB assets and buildings assets.
		2. The aim of a ‘Lockdown’ is to control movement and access (both entry and exit) of people (staff and visitors) around an ICB site in response to an identified risk, threat or hazard that might impact upon the security of staff and assets, including the capability of a facility to continue to operate.
		3. A lockdown is achieved through a combination of physical measures and the deployment of personnel.
		4. A lockdown may be characterised as a partial (static or portable), progressive or full lockdown. Please refer to Appendix G for a description of types of lockdown.
		5. When a lockdown is instigated roles and responsibilities are broken down into four stages (see Appendix G). There are different types of potential lockdown scenarios:
		- Partial Lock down.
		- Progressive Lockdown.
		- Full lockdown.

Details of the different types of lockdown and the actions required are included in Appendix G.

### Lockdown roles and responsibilities

* + 1. The SMD, ICB director/manager on call or Collaboration Hub Programme Manager will have responsibility for activating and ensuring effective lockdown if required as set out on Appendix G.

### ICB Fire Marshals

* + 1. ICB Fire Marshals will be trained to undertake Lockdowns.
		2. On instruction from the SMD, ICB Director/Manager On Call, Fire Marshals and, depending on the circumstances, other staff will carry out the appropriate level of Lockdown.
		3. The staff involved will not be pulled away from this task until the Lockdown is complete or staff are instructed to do so by any of those listed in 8.5.1. above. [**See action card 2 in appendix F.**](#_Appendix_1_–)

### Managers/Directors

* + 1. Should insufficient Fire Marshal’s be available to effect the Lockdown, managers or directors on-site at the time of an incident must nominate sufficient members of staff to assist. Directors must ensure their staff are made aware of the Lockdown Procedure and their responsibilities. [**See action card 3 in appendix F.**](#_Appendix_1_–)

### Other Staff

* + 1. Staff are expected to fully co-operate with management and follow security procedures in operation to protect the safety of staff/visitors and ICB assets.
		2. In order to support a lockdown, staff might have to carry out activities that are outside of their normal job description.

### Head of Communications

* + 1. The Head of Communications will develop communication channels with staff and visitors and will liaise with external media.

## Procedures and Processes

### Major Incident Plan

* + 1. When a lockdown is instigated roles and responsibilities are broken down into four stages (see Appendix G): There are different types of potential lockdown scenarios:
* Full lockdown
* Partial Lock down
* Progressive Lockdown
	+ 1. During a lockdown the ICB may have to make the decision to move essential business activity and support services to alternative temporary locations. This decision will be made by the ICB Chief Executive or SMD.

### Business Continuity during Lockdown

* + 1. Business Continuity is the maintaining of essential business of the ICB in the event of a disruption or a major incident.
		2. The Business Continuity Plan will be shaped by both the cause and duration of a lockdown.

### Activation of a Lockdown (refer to actions cards)

A decision to initiate a lockdown should be guided by the following four factors:

* The protection of staff, visitors or assets
* The isolation of a threat or hazard
* Establishing a safe distance between /staff/assets and a threat/hazard
* Neutralising the threat or hazard
	+ 1. The SMD or the On Call Director/Manager, are responsible for ensuring that a Lockdown, if called, is carried out and maintained and for liaising with any other occupiers of the premises to ensure that the site is secured.
		2. The ICB’s identified Fire Marshals will assist in the lockdown process as necessary.
		3. Once a lockdown has been initiated, its time and duration will depend on the individual circumstances. Staff will take every effort to minimise the duration as much as possible.

### Full Lockdown

* + 1. If a full lockdown is needed then staff should contact the emergency services immediately for their assistance (if necessary). Cordons can only be officially enforced by the Police. If the On call Director/Manager believes that a situation may warrant such measures they must contact the emergency services. The Police (and Fire Service) may also be able to assist in the management of on/offsite traffic, crowd control and any evacuation.

### Partial and Progressive Lockdown

* + 1. If only a partial or progressive lockdown is needed, the On call Director with staff support should make every effort to manage/contain the situation with a view to contacting the emergency services if the circumstances begin to escalate.
		2. As soon as a lockdown has been called, staff should report to an agreed location. At this point, they will need to identify key resources, all of which should be maintained at a central location:
* Map – of the premises, contained in the Fire Evacuation Procedures
* Keys – to secure doors and window
* Radios or mobile phones – where available as part of the Fire Evacuation Procedures
* Tabards – to identify key staff, where used by Fire Marshals/Wardens
* Signage / barriers – where available to highlight no access routes.

### Staff Deployment

* + 1. The ICB does not employ Security Guards or other full time security personnel. Arrangements for securing an area will therefore depend on the availability of staff who are present in the building at the time of the incident,
		2. Once staff have been issued with the items above, they will need to go as quickly as possible to fulfil their roles. Action must be taken quickly to secure the building. Any access controls should be utilised to speed up the process. A manual lockdown should be undertaken as quickly and safely as possible.
		3. To speed up a manual lockdown, careful consideration needs to be given to the order in which doors and windows will be locked. Senior staff should decide this based on the high-risk areas within their premises, their use and accessibility to the public.
		4. Department staff will be responsible for controlling the movement of visitors within their department areas. Where possible, staff will be positioned at the main entrances/fire exits to explain the situation to people and request their co-operation. It is important that some staff are positioned by the main external fire exit doors as fire legislation may prevent these from being locked.
		5. Staff should remain calm and professional during the deployment in order to keep visitors calm.

### Maintaining a Lockdown

* + 1. Once staff are in control of their areas, they should communicate this to the On call Director/Manager. Communication links should be maintained at all times so that staff can be updated on the progress of the lock down.
		2. The ICB has the right to refuse access. If someone enters the premises having been advised not to or is already in the premises but refuses to leave; they may be considered a trespasser. If an individual enters a locked down premises or refuses to leave, they could be prosecuted and the police should be contacted via 999.
		3. In the absence of the police, who are able to enforce a containment cordon, it will only be lawful for ICB staff 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.
		4. Even when the above regulations can be used, specific articles 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.
	+ 1. It is important to remember that staff can only appeal to people to stay inside a locked down area. If people still choose to leave, a safe route must be available for them to do so.

### Stand Down

* + 1. Once the decision has been given to stand down by the On Call Director/Manager, staff should open key doors first. Any signage or barriers should be removed in order of risk/priority to allow access again. Staff should reassure visitors during the stand down in order to keep them calm. The On Call Director will need to contact the Communications Team to inform them of the lockdown outcome and any resolved situations.

### Lessons learnt

* + 1. The ability to learn from any event whether enables organisations to identify good practice and retain it but also to identify areas where they can improve. The process should be led by the Director/Manager on-call.
		2. The key questions to consider are: What went well? Where can we improve? and any recommendations.

## Dissemination and implementation process, including training

### Dissemination and implementation

* + 1. The SMD will ensure that a copy of this policy is freely available to all ICB staff (electronically and/or hard copy).

### Monitoring Compliance

* + 1. The SMD, the Head of Emergency Planning and LSMS will undertake periodic testing of the lockdown process at each relevant location and the results will inform the risk assessment process.
		2. The SMD will ensure that the processes outlined in this policy and any associated policies and guidance are followed.

### Policy development

* + 1. Consultation and communication with stakeholders during development.

### Staff Training

* + 1. All management and staff need awareness raising training, personal safety awareness and dealing with conflict, as well as preventing and reporting crime in the workplace.

Dealing with situations of potential or actual abuse, aggression of violence, must include:

* Understanding the causes.
* Recognising the warning signs.
* Identifying when and where to get help.
* Interpersonal skills/defusing techniques.
	+ 1. Where necessary and/or appropriate staff will be given a local induction where they will be informed of specific health and safety related hazards and controls. Managers are to identify any specific security related training needs for the staff they are directly responsible for and must make adequate arrangements for staff to be able an actually attend. Once training needs have been recognised, the managers should then make arrangements for the member of staff to undertake the next available course. Managers are also responsible for keeping records of all security training for all their members of their staff.
		2. Such training must be included in departmental programmes as part of in-service training, and with periodic refresher courses. Security awareness training will be mandatory for clinical staff with frontline roles. Current guidance is that NHS staff should receive conflict resolution training every three years.
		3. Staff should be made aware of their site’s lockdown plans as part of their local induction. They will also be expected to participate in any major incident training exercise or staged lockdown, whether this is co-ordinated as a real-time on-site session or as a desk-top exercise. Fire Marshalls will also receive regular training/update training and will be made aware when the National Threat Level is increased so that Lockdown arrangements can be reviewed.

## Arrangements For Review

This policy will be reviewed no less frequently than every two years. An earlier review will be carried out in the event of any relevant changes in legislation, national or local policy/guidance, organisational change or other circumstances which mean the policy needs to be reviewed.

If only minor changes are required, the sponsoring Committee has authority to make these changes without referral to the Integrated Care Board. If more significant or substantial changes are required, the policy will need to be ratified by the relevant committee before final approval by the Integrated Care Board.

## Associated Policies, Guidance And Documents

* Violence Prevention and Reduction Standard 2021.
* NHS England EPRR Framework 2022.
* NHS Resilience PAS 2015.
* Developing Dynamic Lockdown Procedures – GOV.
* Bomb Threat guidance, Home Office.

#### [Associated Policies](https://www.midandsouthessex.ics.nhs.uk/publications/?publications_category=icb-policies)

Lone Worker Policy.

Management of Violence & Aggression Policy.

Whistleblowing Policy.

ICB Driving at Work Policy.

Anti-Fraud and Bribery Policy.

Disciplinary Policy.

## References

**Legislation**

* Civil Contingencies Act 2004.
* Human Rights Act 1998.
* Health and Safety at Work Act 1974.

## Appendix A - Equality Impact Assessment

**INITIAL INFORMATION**

|  |  |
| --- | --- |
| **Name of policy:** Security & Lockdown Policy**Version number (if relevant):** 1.0 | **Directorate/Service**: EPRR |
| **Assessor’s Name and Job Title:** Jo Martindale, Business Continuity & EPRR Officer | **Date:** 11/05/2022 |

|  |
| --- |
| **OUTCOMES** |
| *Briefly describe the aim of the policy and state the intended outcomes for staff*  |
| The Policy will support the organisation and its staff to achieve legislative requirements in relation to the effective management of EPRR.  |
| **EVIDENCE** |
| *What data / information have you used to assess how this policy might impact on protected groups?* |
| The ICB regularly monitors the make-up of the workforce, including protected groups. |
| *Who have you consulted with to assess possible impact on protected groups? If you have not consulted other people, please explain why?*  |
| Emergency planning teamGovernance leads |

**ANALYSIS OF IMPACT ON EQUALITY**

The Public Sector Equality Duty requires us to **eliminate** discrimination, **advance** equality of opportunity and **foster** good relations with protected groups. Consider how this policy / service will achieve these aims.

N.B. In some cases it is legal to treat people differently (objective justification).

* ***Positive outcome*** *– the policy/service eliminates discrimination, advances equality of opportunity and fosters good relations with protected groups*
* ***Negative outcome*** *–**protected group(s) could be disadvantaged or discriminated against*
* ***Neutral outcome***  *–**there is no effect currently on protected groups*

Please tick to show if outcome is likely to be positive, negative or neutral. Consider direct and indirect discrimination, harassment and victimisation.

| ProtectedGroup | Positiveoutcome | Negativeoutcome | Neutraloutcome | Reason(s) for outcome |
| --- | --- | --- | --- | --- |
| Age | X |  |  | The Policy will ensure that individuals of all ages are considered in relation to Health and Safety tasks. |
| Disability(Physical and Mental/Learning) | X |  |  | This Policy has a positive impact on any staff who have a physical/Mental impairment by considering their needs regarding H&S and the subsequent policies and procedures that underpin the Health and SafetyStrategy. |
| Religion or belief |  |  | X | The Policy has no impact on sexual orientation. |
| Sex (Gender) |  |  | X | The Policy has no impact on gender. |
| Sexual Orientation |  |  | X | The Policy has no impact on sexual orientation. |
| Transgender / Gender Reassignment |  |  | X | The Policy has no impact on transgender/gender resignment. |
| Race and ethnicity |  |  | X | There are no requirements for translation within the current staff group should the staff group characteristicschange then versions and signage within the ICB in other languages can be obtained. |
| Pregnancy and maternity (including breastfeeding mothers) | X |  |  | The Policy can be accessed by all staff via intranet and policies/procedures are in place which underpin thepolicy’s aims. The ICB also has risk assessment documentation in place toensure all risks are considered. |
| Marriage or Civil Partnership |  |  | X | The Policy has no impact on marriage or civil partnership. |

|  |
| --- |
| **MONITORING OUTCOMES** |
| Monitoring is an ongoing process to check outcomes. It is different from a formal review which takes place at pre-agreed intervals. |
| *What methods will you use to monitor outcomes on protected groups?* |
| Review of policy to take place following an incident debriefing process to implementing lessons learnt. Will also monitor for changes is legislation / best practise which may affect the content of the document. |

|  |
| --- |
| **REVIEW** |
| *How often will you review this policy / service?*  |
| Every 2 years as a minimum and earlier if there are any significant changes in legislation, policy or good practice. |
| *If a review process is not in place, what plans do you have to establish one?* |
| N/A |

## Appendix B – Bomb Threat Action Plan

The following is a reference guide for staff required in response to a Bomb Threat:

**Switchboard**

On receipt of a call the receiver should elicit as much information as possible about the caller.

On completion of the telephone call the receiver should immediately contact the following:

* Essex Police using 999 Emergency Number (or refer to local systems)
* Alliance Director, On-call director/manager or Chief Executive Officer
* Other surrounding buildings
* Neighbouring buildings / co-located services

Arrangements should be made for the immediate evacuation of the Building. Staff should assemble well away from the building and await further instruction from the attending emergency services. Staff **must not** return to the building until instructed to do so by the Essex Police.

An Incident Form should be completed once the situation has been resolved.

## Appendix C – Theft

• Should a suspected theft occur the Police should be contacted immediately using 999. All forms of theft should be reported in this way.

• An incident report must be completed (in accordance with the Incident Reporting & Management Policy) and the LSMS notified.

• The LSMS will contact the Police to monitor the investigation and assist where required, including interviewing and obtaining supporting information.

• The outcomes of any investigations will be reported to the Chief Executive, appropriate Executive Director and the Audit Committee.

## Appendix D – Harassment

Harassment is covered by the following legislation:

* Equality Act 2010
* Protection from Harassment Act 1997

**Harassment** under the Equality Act 2010 refers to unwanted conduct related to relevant protected characteristics, which are sex, gender reassignment, race (which includes colour, nationality and ethnic or national origins), disability, sexual orientation, religion or belief and age, that:

* Has the purpose of violating a person’s dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that person; or
* Is reasonably considered by that person to have the effect of violating his/her dignity or of creating an intimidating, hostile, degrading, humiliating or offensive environment for him/her, even if this effect was not intended by the person responsible for the conduct.

The ICB’s Dignity at Work Policy (MEICB084) sets out the procedure that should be referred to should an employee consider that they have experienced bullying or harassment at work.

Serious bullying or harassment at work may amount to other civil or criminal offences, e.g. a civil offence under the Protection from Harassment Act 1997 and criminal offences of assault.

The Protection from Harassment Act 1997, Section 8, states:-

(1) Every individual has a right to be free from harassment and, accordingly, a person must not pursue a course of conduct which amounts to harassment of another and —

(a) is intended to amount to harassment of that person; or

(b) occurs in circumstances where it would appear to a reasonable person that it would amount to harassment of that person.

(2) An actual or apprehended breach of subsection (1) may be the subject of a claim in civil proceedings by the person who is or may be the victim of the course of conduct in question; and any such claim shall be known as an action of harassment.

(3) For the purposes of this section —

• “conduct” includes speech;

• “harassment” of a person includes causing the person alarm or distress; and

a course of conduct must involve conduct on at least two occasions.

* A ‘course of conduct’ may be inappropriate words, letters or gifts, etc. Each incident will be investigated by the ICB and, where police and/or legal intervention is not judged to be necessary, the following will apply;
* Should an incident of harassment occur where the alleged perpetrator is not a member of MEICB staff, the perpetrator should be given a verbal warning informing them that their behaviour is causing distress and is unacceptable.
* An incident report should be completed via DATIX with all information (see Incident Reporting Policy) detailing that a verbal warning has been given, this should be sent to the Collaboration Hub Programme Lead and the Quality & Safety team who will in turn route to the LSMS.
* Should the perpetrator continue to harass a member of staff an incident form should be completed as above, the LSMS should be notified immediately of this incident.
* On notification of a second incident the LSMS will write a formal letter to the perpetrator informing them that their actions are illegal and if it continues they will be reported to the police with a view to prosecution.
* Should the harassment continue the police will be contacted by the LSMS with a view to investigate under the Protection of Harassment Act 1997.
* The Chief Executive and Security Management Director will be informed of any action taken with regards to harassment by the LSMS.

## Appendix E – Suspicious Packages

Incidents of this nature are extremely rare; however if there is concern that a suspected package has been received sensible steps can be taken to minimise the risk and danger.

**General Mail Handling - What to look for:**

* Look out for suspicious envelopes or packages (see below for some things that should trigger suspicion).
* Open all mail with a letter opener or other method that is least likely to disturb contents.
* Open packages/envelopes with a minimum amount of movement.
* Do not blow into envelopes.
* Do not shake or pour out contents.
* Keep hands away from nose and mouth while opening mail.
* Wash hands after handling mail.

**Some items that can trigger suspicion**

* Discolouration, crystals or surface, strange odours or oily stains.
* Envelope with powder or powder-like residue.
* Excessive tape or string.
* Unusual size or weight for its size.
* Lopsided or oddly-shaped envelope.
* Postmark that does not match return address.
* Restrictive endorsements such as “Personal” or “Confidential”.
* Excessive postage.
* Hand-written, block printed or poorly typed addresses.
* Incorrect titles.
* Title but no name.
* No return address.
* Misspelling of common words.
* No return address.
* Addressed to a person who has left the authority’s employment.

**General Mail Handling - What to do**

If you believe you have received a contaminated package:

* Do not touch the package further or move it to another location. Especially do not put it in a bucket of water.
* Shut windows and doors in the room and leave the room, but keep yourself separate from others and available for medical examination.
* Switch off any room air conditioning/ventilation system.
* Notify your Manager clearly stating why you think it is suspicious.

**Your manager should make arrangements to**

* Confirm as far as possible whether the suspicious package merits calling out the Police and invoking emergency plans.
* Notify the police using the 999 system.
* Activate the fire alarm to evacuate the building
* Switch off building air conditioning/ventilation systems.
* Close all fire doors.
* Close all windows.
* If there has been a suspected biological contamination, ensure that staff in the contaminated room are evacuated to an adjacent unoccupied room away from the hazard.
* If there has been a suspected chemical incident, ensure staff leave the room as quickly as possible. Possible signs that people have been exposed will be streaming eyes, coughs and irritated skin. Seek immediate medical advice.

**Suspicious Packages - What to do**

**If you find a suspicious package either inside or outside a building**

* Do not touch it or move it.
* Inform your manager, clearly stating why you believe it to be a suspicious package.

You manager should make arrangements to

* Notify the police using the 999 system.
* Switch of building air conditioning/ventilation systems.
* Close all fire doors.
* Close all windows.
* Move staff away from the hazard and await instructions from the emergency services.

**If you believe that you have been exposed to Biological/chemical material**

* Remain calm.
* Do not touch eyes, nose or any other part of your body.
* Wash your hands and any other exposed parts of your body in ordinary soap where facilities are provided, but movement outside your room should be avoided as much as possible.
* Do not eat, drink or smoke
* Notify your manager who should call the ambulance service using the 999 system.

## Appendix F – Action Cards

**Lockdown Instructions**

**Action Card 1**

**Director/Manager on-call**

* You will ensure that the ICB fire marshals are made aware of the Lockdown and that they comply with their respective responsibilities
* You will ensure that all access points doors are locked, and window closed. The receptionist and Collaboration Hub Programme Lead have access to entrance keys
* You will ensure that, where safe to do so, a deputised staff member remains at each of the access points including lifts
* You will ensure that fire escape doors are secured but remain ready for us in case of evacuation
* You will ensure that the Chief Executive is regularly updated with a situation report
* You will contact the ICB’s security provider NHS Property Services (NHSPS) helpdesk on 01902 575 050 to advise them that a security incident has occurred
* You will contact the Local Security Management Specialist (LSMS) – Julie Hill on 07500 225 027 to seek further advice if required
* You still stand down lockdown when it is safe to do so ensuring all staff are made aware and communications team are advised if media messages are required
* You will write an incident report following the incident and ensure any lessons identified are formulated into an action plan.

**Lockdown Instructions**

**Action Card 2**

**Fire Marshalls / Receptionist**

On instruction of the On call director/manager:

* You will obtain relevant keys from the receptionist or Collaboration Hub Programme Lead
* You will secure the main building access point/s (front entrance/rear of staff entrance)
* You will secure lifts
* Where safe to do so, you will remain at the locked doors and lifts
* You will follow the directions of the On call director/manager - your task is to prevent anyone from entering the site unless instructed

**Lockdown Instructions**

**Action Card 3**

**ICB Directors**

On instruction of the On call director/manager:

* You will determine as necessary extra staff to assist with the lockdown
* You will ensure staff are made aware of the lockdown procedure and their responsibilities

## Appendix G – Lockdown details

**Types of Lockdown**

|  |  |  |
| --- | --- | --- |
| **Type** | **Details** | **Action to be taken** |
| **Partial lockdown**  | This is the locking down of a specific part of an ICB site or when entry restrictions are in place to control the flow of people into it, e.g. restricting access into a department during investigation of an incident.Partial lockdowns can be static or move with a specific threat | If only a partial or progressive lockdown is needed, the On-call Director, with staff support should make every effort to manage/contain the situation with a view to contacting the emergency services if the circumstances begin to escalate. As soon as a lockdown has been called, staff should report to an agreed location. At this point, they will need to identify key resources, all of which should be maintained at a central location: |
| **Progressive lockdown**  | This is the step by step (incremental) lockdown of a ICB site or building in response to an escalating scenario. |
| **Full lockdown**  | This is the process of preventing freedom of entry to an exit from either an entire ICB site or from a specific building.The objective of lockdown is to ensure the safety and security of all staff, visitors, property and assets in the event of a major incident and thus protecting the integrity of the NHS**.** | If a full lockdown is needed, then staff should contact the emergency services immediately for their assistance (if necessary). Cordons can only be officially enforced by the Police. If the On-call Director believes that a situation may warrant such measures they must contact the emergency services. The Police (and Fire Service) may also be able to assist in the management of on/offsite traffic, crowd control and any evacuation. |

Stages of a Lockdown

Lockdown roles and responsibilities can be broken down into four stages:

 **Lockdown Activation**:

 A decision to activate lockdown should be guided by the following factors:

* The potential for harm to people or property
* Whether it is possible to isolate or neutralised the sources of the threat or hazard
* How far people or property are from the source of the threat or hazard
* Possibility of cross contamination

 During this stage, staff should be aware of who to report to and what resources they need to facilitate their role. Refer to Action Cards

 **Lockdown Deployment**:

Staff are designated specific roles during lockdown. So that this process is swift and efficient it is important that:

* Staff are fully trained in the requirements of the lockdown policy and are familiar with the location of all items they will require
* This will potentially be a stressful situation for staff and the more familiar they are with their responsibilities the better, if anyone is not comfortable with fulfilling any roles they must let make their line manager aware.

 **Lockdown Maintenance**: staff consider some of the features that should be considered to maintain a lockdown and how this can be achieved.

 Communication will be key during this phase. It is important that all staff involved maintain control of their respective areas and provide regular updates.

 **Lockdown Stand-Down**: focuses on how staff will facilitate the end of a lockdown.

 No member of staff should stand down until it has been declared safe to do so. Once the decision to stand down has been given staff should follow the instructions given.

 All staff involved in the lockdown should be de-briefed as soon as possible after the incident so that details can be recorded and used as lessons learned for future lockdowns and training purposes.