Security Policy

Ref: MECCG129

Target Audience	Board members, sub-committee members and all staff working for, or on behalf of, Mid Essex Clinical Commissioning Group (the CCG).
Brief Description (max 50 words)	This policy sets out the principles by which the Mid Essex Clinical Commissioning Group will manage Security procedures across the organisation.
Action Required	Following approval of this policy all staff will be advised of its availability on the CCG website.

Compliance with all Mid Essex CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Document Information

Title of Policy	Security Policy V1.7
Accountable Executive Director	Director of Governance and Performance
Responsible Post holder/Policy Owner	Head of Corporate Governance
Approved By Audit Committee (Committee & Date)	4 September 2019
Date Approved by CCG Board:	26 September 2019 (extended by 6 months at Board 26 March 2020)
Review Date	March 2022 (Agreed at Audit Committee 23 Feb 2021 to extend the review date for this policy to March 2022)
Stakeholders engaged in development/review	Head of Corporate Governance Head of Emergency Planning Local Security Management Specialist
Equality Impact Assessment	**EQUALITY IMPACT ASSESSMENT** This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This Policy is applicable to the Board, every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national

	origins), sexual orientation, religion or belief, marriage or civil partnership, and those who work on behalf of the CCG

Amendment History

Version	Date	Reviewer Name(s)	Comments
1.0	26/08/2015	Local Security Management Specialist and Head of Corporate Governance.	Draft developed for review by Audit Committee
1.1	09/11/2015	Audit Committee	Minor amendments requested by Audit Committee, 09/11/15.
1.2	25/05/17	Sara O'Connor, Head of Corporate Governance	Name and contact details of LSMS amended (Committee approval N/A)
1.3	03/01/2018	Sara O'Connor, Head of Corporate Governance and Jackie King, Head of Emergency Planning	Job titles updated and other minor amendments.
1.4	08/01/2018	Local Security Management Specialist	Updated to reflect NHS security management structure and procedural changes. Revised case law and procedures.
1.5	02/05/19	Head of Corporate Governance and Director of Governance & Performance	Updated to reflect changes in job titles, organisational changes and minor updates.
1.6	25/6/19	Local Security Management Specialist	Minor amendments
1.7	24/04/20	Charlotte Tannett, Corporate Governance Support Officer	Name and contact details of LSMS amended.

Associated Policy Documents (this list is not exhaustive)

Reference	Title
MECCG001	Risk Management Policy
MECCG002	Health & Safety Policy
MECCG008	Anti-Fraud and Bribery Policy
MECCG011	Lone Worker Policy
MECCG012	Whistleblowing Policy and Procedure
MECCG014	Serious Incident Management Policy
MECCG036	Management of Violence & Aggression Policy
MECCG084	Dignity at Work Policy
MECCG104	Recruitment Policy
MECCG118	Incident Reporting & Management Policy
MECCG123	Information & Cyber Security Policy
MECCG133	Lockdown Policy

Contents

1. Introduction

Mid Essex Clinical Commissioning Group 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 such incidents. The organisation will also protect the property of the NHS (both physical and intellectual).

Mid Essex Clinical Commissioning Group will provide reasonable measures to create and maintain a secure environment to support this commitment. Overall responsibility for security will rest with the Accountable Officer.

The organisation expects all members of staff to consider, as part of their normal course of work, security issues whether they pose a potential or actual threat to people or property.

The organisation recognises that it would be impossible to prevent every unforeseen security incident and will provide security resources to assist in handling such matters. Emphasis will be placed on the prevention of security incidents and the organisation will emphasise to all staff the need to take security responsibilities seriously.

The organisation operates controlled access to the building to allow appropriate staff to operate with the minimum of hindrance and also affords free movement to legitimate visitors in areas where it is appropriate for them to have access.

The services located within the building will take steps to limit access to specific areas within to those people who have a legitimate reason for entry.

Mid Essex Clinical Commissioning Group expects that all members of staff wear recognised identification at all times whilst working.

It should be noted that although the Security Policy relates to Mid Essex CCG staff, Wren House is not solely occupied by the CCG, so it will be necessary to work with the other occupiers in the event of a security incident.

2. Security Policy

It is the policy of Mid Essex Clinical Commissioning Group to seek to ensure, as far as is reasonably practicable, the personal safety at all times of staff and visitors and the protection of property against fraud, theft and damage.

The organisation will ensure provision of safeguards to protect the safety of those who work for the organisation and those using the premises and property for legitimate purposes.

It is the intention to work towards the reduction (and wherever possible) the elimination of all security breaches, whether directed at staff, patients, visitors, Mid Essex Clinical Commissioning Group property or appropriate private property brought onto the organisation’s premises.

In line with NHS Security Management guidance the organisation has in place an accredited Local Security Management Specialist (LSMS) responsible for security.

This individual is in place to ensure compliance with NHS national guidance and strategies and the promotion and implementation of the security management standards.

3. Security management principles

The founding principles of security management are:

1. **Strategic Governance -** This area ensures that security management is embedded throughout the organisation, with focus on the Security Management Director (SMD) and Local Security Management Specialist. The aim is to ensure that anti-crime measures are embedded at all levels across the organisation.
2. **Inform and Involve –** This area sets out the requirements in relation to raising awareness of crime risks against the NHS and working with NHS staff, stakeholders and the public to highlight the risks and consequences of crime against the NHS.
3. **Prevent and Deter** - This area sets 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 section sets out the requirements in relation to detecting and investigating crime, prosecuting those who have committed crimes and seeking redress.

4. Management Responsibilities

Security is a management responsibility and the provision of a security service in no way relieves management at any level of its obligations to fulfil the stated purpose of security in the organisation.

Managers are required to exercise preventative aspects and to take appropriate action where necessary in respect of those who offend against the law, commit misconduct or other breach of security in contravention of the policies of the service.

The Organisation is responsible for ensuring local procedures exist for all security related functions, including –

- Assistance for those requiring support
- Enhancing security capability, physical measures should be integrated across the CCG. For example, panic alarms lockable doors and access control.
- Maintenance of security measures. This includes testing alarms and changing lock codes regularly.
- Secure storage and use of equipment and valuables
- Specific risks relevant to the building use
- Safe use and storage of drugs

- Safe use and access to patient information and corporate, confidential data

5. Employee Roles and Responsibilities

Employees are expected to cooperate with management to achieve the aims of the security policy. Major policy changes which directly affect employees such as rules of conduct during their employment will be discussed through the established consultative forums.

All Staff

All members of staff, whether directly employed, seconded or aligned to the CCG, are responsible for contributing to and participating in crime prevention and implementing the security policy, and systems. All staff are responsible for identifying and highlighting their specific training needs and attending relevant training according to their needs. Great emphasis should be placed on the importance of personal safety.
It is expected that all staff will:

- Comply with security procedures relevant to their workplace.
- Familiarise themselves with local security risks and controls. E.g., access control, risk assessments etc.
- Report actual or suspected security breaches (e.g. stolen equipment, signs of attempted break-in, suspected bogus member of staff). Reports should be made immediately to a manager for the service, the Director of Governance and Performance/Head of Corporate Governance, or the LSMS, and recorded 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" (especially when 'lone working' – see Lone Worker Policy MECCG011).
- 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, electronic swipe card systems etc.
- Take responsibility for ensuring the security of their own possessions brought onto NHS property. Staff are advised to keep personal possessions at work to a minimum and not to bring valuable or sentimental items to work.
- Maintain vigilance at all times, reporting to the relevant persons when potential security breaches arise or where security systems are misused (e.g. when other staff are observed gaining unauthorised access through using ID cards other than their own, or "tailgating" through security doors).

CCG Governing Body (Board)

It is the responsibility of the CCG Board to ensure the implementation of this security strategy. The Board needs to be confident that they are aware of the security risks within the CCG, that there are controls in place to manage these risks and where appropriate that action plans are in place to reduce the risks and that crime against the organisation is being prevented as far as possible.

The Audit Committee

The Audit Committee will feed into the CCG Board assurances around security compliance. The LSMS will submit a progress report to each Audit Committee meeting and will provide an annual report to show activities undertaken against the security work plan each year.

Accountable Officer

The Accountable Officer has overall responsibility for the quality and safety of services provided by the CCG. In this respect, he/she is responsible for ensuring that the infrastructure required in supporting the delivery and implementation of this document is available. He/she will delegate the full implementation of this document to a relevant Executive Director.

Security Management Director (SMD)

. Within Mid Essex CCG, the Director of Governance & Performance is the Executive Director with ultimate responsibility for security management. The role of the SMD includes:

- That adequate security management provision is available within their NHS health body;
- Ensuring that an effective security strategy and systems are in place; and
- Approving the Organisational Crime Profile, the Annual Report, the Security Review Tool and the security management work plan.
- Reporting security progress and significant risks to the Board.

Head of Corporate Governance

The Head of Corporate Governance, supported by the Corporate Business Manager, is responsible for ensuring that the security policy, strategy, plans, procedures and systems are in place, implemented, monitored and reviewed.

Local Security Management Specialist (LSMS)

The LSMS has responsibility for providing a comprehensive, inclusive security management service for the CCG and for working towards the creation of a pro-security culture within the CCG, as defined in the Security Management Standards document.

The LSMS is specifically recognised as the CCG's subject matter expert in relation to the management of security within the organisation.

The LSMS will work with NHS England and prepare an annual work programme to help meet defined national security standards. The LSMS will ensure that there are effective arrangements in place to facilitate the reporting of breaches of security and weaknesses in security related systems.

The LSMS will:

- Facilitate the annual completion of the Security Self Review Tool.
- Aid determination of the annual work plan priorities.
- Raise strategic and operational risks which are identified or foreseeable.
- Provide support and assistance with security management issues and will ensure that security measures are implemented to meet relevant requirements of the NHS Security Management Standards .
- Collate, analyse and identify security incident trends, providing advice and practical support to identify and implement suitable crime reduction measures.
- Investigate breaches of security, as necessary, within the organisation.
- Ensure that security management work, including incident reporting and risk assessment, is integrated into systems for risk management throughout the organisation.
- On request, carry out security inspections and risk assessments in NHS premises used by the organisation.
- Advise on strategic effectiveness of Conflict Resolution Training to meet the National Syllabus requirements as previously set out by NHS Protect.
- Liaise with the security lead at NHS England and other relevant agencies or authorities.
- Monitor physical assault incidents.
- Encourage the development of a pro-security culture.
- Support managers and their staff with casework for potential criminal and/or civil proceedings.
- Review and evaluate security, or security related, information from incident reports, risk assessments and other information sources that may become available. Outcomes from this activity will be shared with the SMD.
- Evaluate and liaise on security alerts issued by NHS England.

- Liaise with key stakeholder agencies such as the Police and Crown Prosecution Services

Departmental Managers

- Departmental Managers will make themselves fully aware of and understand the policies and procedures for security, the contingency plans for the area and know and understand their role within the plan.
- They are responsible for ensuring all staff are aware of their roles within the security policies and procedures, any local systems and arrangements in place.
- They will ensure their staff exercise good security practice e.g. reporting suspicious behaviour, ensuring the appropriate use of identity badges, challenging those whose presence may be questionable or untoward.
- They will encourage patient/carer/relative/visitor awareness of crime prevention.
- They will ensure that risk assessments are carried out in the areas they and their staff work, and take into account risks associated with lone working and working in the frontline.
- They will identify training requirements for staff, including where mandatory training such as Conflict Resolution Techniques is applicable and ensure that these are maintained on training plans and attended.
- They will escalate identified risks as per the Risk Management Policy and procedure and take appropriate action.
- In case of serious breaches of security e.g. theft, criminal damage or physical assaults on CCG Staff, the police should be informed immediately and the LSMS must be notified.

6. Violence and Aggression

Employers and employees have a general duty under section 2 of the Health and Safety at Work Act 1974 to ensure the safety of people who use their premises.

The definition of work related violence as advanced by the European Commission DFV(3) defines violence “Incidents where persons are abused, threatened or assaulted in circumstances related to their work, involving an explicit or implicit challenge to their safety, wellbeing or health”.

The CCG’s arrangements in place for violence and aggression are contained within the Management of Violence and Aggression Policy.

7. Organisation for Security

7.1 Responsibility for Security

The Director of Governance & Performance is responsible to the Mid Essex Clinical Commissioning Group Board for the effective implementation of the security policy.

The directors of all services are responsible for the overall coordination and implementation of the policy within the organisation's directorates.

7.2 Audit and Quality & Governance Committees

Health & Safety issues and policies are discussed and actions agreed at the Quality and Governance Committee. Security issues are discussed at the Audit Committee. This Policy will be subject to approval by Audit Committee.

7.3 Reporting of Crime / Security Incidents

All staff have responsibility to report any crime/breach of security. This reporting falls into the following categories.

- Where a crime/security incident of a serious nature is happening there and then, staff should call the police immediately by telephoning 9 999.

- Where a security incident is discovered, the information should be passed to the appropriate line/service manager/director as soon as practicable.

- Staff should complete the Datix incident report form and forward to the appropriate line/service manager/director/risk team as soon as practicable.

Procedures for reporting security breaches have been included in **Appendices 1, 2, 3 and 4**. Also see the Violence & Aggression Policy (MECCG036) for reporting physical and non-physical assault incidents and the Whistleblowing Policy MECCG012.

The need for overall effective monitoring of crime to enable effective decision making within the overall security and risk management strategy is paramount: to this end, recorded data on incidents occurring within Mid Essex Clinical Commissioning Group is reported to the Quality & Governance Committee.

7.4 Training

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

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.

Conflict resolution training requirements are assessed in accordance with guidance issued by NHS Protect in 2013. .

8. Key Aspects of Security

8.1 Rehabilitation of Offenders Act 1974

All persons applying for a post must have completed the section on the application form entitled Rehabilitation of Offenders Act 1974. This section states that ‘because of the nature of the work for which you are applying, this post is exempt from provisions of Section 4(2) of the Rehabilitation of Offenders Act, 1974 (Exemption) Order, 1975.’

Applicants are, therefore, not entitled to withhold information about convictions which for purposes are ‘spent’ under the provisions of the Act, and in the event of employment, any failure to disclose such convictions could result in dismissal or disciplinary action by the organisation (as outlined in the CCG’s disciplinary policy).

This application form also requests details of any convictions, adult cautions or bind overs, and requires the applicant to sign the statement confirming that the information given is correct. Further information is contained within the Recruitment Policy.

8.2 Children’s Act 1989 and Safeguarding Vulnerable Groups Act 2006

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 vulnerable groups, including children and adults at risk of abuse. The DBS replaces the Criminal Records Bureau (CRB) and Independent Safeguarding Authority (ISA).

8.3 Staff Identification

Every employee within the first week of commencing employment will be issued with an identification card/badge by the organisation’s HR Department. At termination of employment the Line Manager must recover and return the card/badge to the Human Resources Department for destruction.

8.4 Access and Egress

Every employee within the first week of commencing employment will be issued with a swipe card by the Business Support Team.to enable them to gain access to the building
at termination of employment the Line Manager must ensure the swipe card is returned to the Business Support Team.

Access to the building will be restricted between 22.00 hours and 07.00 hours through the use of 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.

Access to certain areas within the building, e.g. the Information Technology Room located on the ground floor, will be controlled by the use of digital locks, electronic alarm systems and access to keys.

All windows at ground level, where appropriate, will be fitted with restrictors limiting the extent to which they can be opened (unless deemed essential in accordance with the local fire procedure).

8.5 Security of Goods

Goods received into departments must be checked against delivery notes prior to signing for acceptance.

8.6 Vehicle Security

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.

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.

All equipment must be stored out of sight. At no time should Mid Essex Clinical Commissioning Group property be left unattended in staff vehicles overnight.

8.7 Fraud

Procedures should ensure that the Chief Finance Officer and the CCG Local Counter Fraud Specialist are alerted immediately of any suspicions of fraud. The policies should ensure that there is a direct and close relationship between Security, the Chief Finance Officer and the Local Counter Fraud Specialist and between security and personnel departments. Please refer to the Anti-Fraud and Bribery Policy (MECCG008) for further information.

8.8 Information Security

Objective

The objective of information 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.

The organisation's Information and Cyber Security Policy has been created to protect the information and assets from all threats, whether internal or external, deliberate or accidental.

The Information and Cyber Security policy 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 Essex CCGs 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.

The Director of Governance and Performance has direct responsibility for ensuring the Information and Cyber Security Policy is maintained and providing advice and guidance on its implementation.

It is the responsibility of each employee to adhere to the policy.

8.9 Major incident

A major incident is a serious unforeseen occurrence causing disruption to the continuation of the CCG's usual services. This may happen suddenly with little or no warning and cause or threaten death or serious injury to patients, staff and members of the public; it may also cause damage or destruction to property which necessitates special mobilisation and organisation.

The Mid Essex Clinical Commissioning Group Major Incident Plan shall be followed for all types of major incidents.

8.10 Bomb Threat and Suspicious Packages

NHS Premises are not immune from the attention of terrorists, who may be politically or otherwise motivated to plant explosive devices with a view to damaging property, maiming or killing people. A copy of the Bomb Threat Action Plan is attached at **Appendix 1** and a procedure for dealing with suspicious packages at **Appendix 4.**

9. NHS England and Security Management Standards for Commissioners

The NHS England Audit Committee has previously set out security management expectations for CCG's with recommendations to adhere to the NHS Security Management Standards for Commissioners which includes the following:

- The requirement for health bodies to have a nominated Executive Director for Security Management to lead work at board level to tackle violence against staff – this is the Director of Governance and Performance of Mid Essex Clinical Commissioning Group.

- A consistent local reporting system for physical incidents, using clear and legally based definitions, to ensure the best possible outcome for the person assaulted.

- The employment within each NHS organisation of a trained Local Security Management Specialist (LSMS) to focus on improving security management awareness within the service and to investigate incidents as and when they occur. The organisation employs an accredited LSMS, currently Julie Hill, West Midlands Ambulance Service, Julie.hill2@wmas.nhs.uk Mobile:07500 225027.

Appendix 1 – Bomb Threat Action Plan

The following Mid Essex Clinical Commissioning Groups 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)
- Accountable Officer or Executive Director
- .
- Other surrounding buildings
- NHS England – Midlands and East (East)

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 2 – 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 via DATIX 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 Accountable Officer, appropriate Executive Director and the Audit Committee.

Appendix 3 – 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 CCG's Dignity at Work Policy (MECCG084) 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 CCG 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 MECCG 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 Head of Corporate Governance 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 Accountable Officer and Security Management Director will be informed of any action taken with regards to harassment by the LSMS.

Appendix 4 – 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.