NHS
Herefordshire and Worcestershire
Clinical Commissioning Group

Local Security Management Policy

Document Reference Information

Version:	1
Status:	Ratified
Author:	Local Security Management Specialist
Directorate responsible:	Corporate
Directorate lead:	Associate Director of Corporate Services
Ratified by:	Joint Commissioning Committee
Date ratified:	8 January 2020
Date effective:	1 April 2020
Date of next formal review:	1 year from effective date
Target audience:	All permanent and temporary employees of the CCG, Governing Body members, contractors, agency staff and any other parties who have a business relationship with the CCG.

Version Control Record

Version	Description of change(s)	Reason for change	Author	Date
1.0	First draft			November 2019

Contents

1. Introduction

1.1 The Clinical Commissioning Group (CCG) is committed to ensuring the health and safety of their employees whilst at work and of any patients, visitors and contractors whilst on our premises.

1.2 The Security Management Policy, of which this statement is a part, contains details of the arrangements and management systems in place to ensure the objectives outlined below are fully met.

2. Scope

2.1 The CCG recognises that, under the Health and Safety at Work Act 1974, it has legal duties to ensure so far as is reasonably practicable, the health, safety and security of its employees and the health and security of patients, members of the public and other persons who use its premises. The policy will apply to any person that is carrying out authorised duties on behalf of the CCG.

2.2 This Policy provides staff with an outline of the CCG's approach to meeting its security management responsibilities and supports the CCG's need to comply with statutory Health and Safety and security requirements.

3. Equality Statement and Due Regard

3.1 The CCG aims to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all. This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex, gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

3.2 In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the CCG is responsible, including policy development, review and implementation.

4. Definitions

4.1 The following are commonly used terms throughout the course of this policy:

LSMS: Local Security Management Service

SMD: Security Management Director

5. Reason for Development

5.1 Security Management forms an integral part of the organisation's Governance Structure. The Policy has been written to meet the requirements of the Department of Health's Organisation with a Memory (DOH2000) and the Health and Safety Executive's Managing for Health and Safety Document (HSG 65)*.

* Managing for Health and Safety is a Risk Management Model used by the Health and Safety Executive.

6. Aim

6.1 The aim of this policy is to set a framework to enable the CCG to continually improve their security management arrangements and encourage the workforce to improve security management performance by challenging work practices and participating in Committees and Forums to drive and enable change.

7. Statement of Intent

7.1 It is the policy of the CCG to comply with the Health and Safety at Work Act 1974 and other relevant legislation as appropriate, in order to ensure, so far as is reasonably practicable, the health, safety and security of its employees (while they are at work), patients and any other person who may be affected by our undertaking. This is extended, so far as is reasonably practicable, to patients' homes and other accommodation in the community that employees may visit in order to undertake their duties.

7.2 The responsibilities set out in this policy and associated procedures are intended to ensure that work will be carried out safely, in accordance with all relevant statutory provisions and consistent with good practice. Adequate resources will be made available to ensure that this objective is met.

8. Roles and Responsibilities/Duties

8.1 The CCG's Governing Body has overall responsibility for the health, safety and security of all employees and for public safety. It will ensure that these matters are integral to the way in which the CCG manages its business.

8.2 Day to day responsibility for ensuring that this policy is implemented within the CCG is delegated to the Directors of the CCG who will keep the Accountable Officer informed of security matters via the agreed Committee routes.

8.3 CCG's Governing Body

8.3.1 The Governing Body will do its reasonable best to ensure that the health care and health services commissioned are of a high quality and are safe. The Governing Body will demonstrate its commitment to security management through:

- The endorsement of the Security Management Policy and associated procedures and guidance.
- The receipt and review of regular reports that detail progress towards the full implementation of the Security Management Policy.
- The receipt and review of regular reports of security management activity within the CCG.
- The Governing Body will require all staff to fulfil their responsibilities in relation to security management.

8.4 The Chief Finance Officer

8.4.1 The Chief Finance Officer has overall responsibility, on behalf of the Governing Body, for:

- the organisation and management of security measures across the CCG
- monitoring the implementation of this Policy throughout the CCG
- ensuring that, at least annually, a Local Security Management Specialist (LSMS) Security report is presented to the Security Management Director (SMD) by the LSMS, informing them of the current state of security management within the CCG.

8.5 **The Executive Lead with lead responsibility for security is the CCG's Security Management Director (this is currently the Chief Finance Officer)**

8.5.1 The Security Management Director has responsibility for:

- the formulation, implementation and maintenance of an effective Security Policy, in consultation with staff representatives, and ensuring that Managers co-ordinate and implement the Policy in their respective areas
- monitoring the performance of the CCG and Directorates with regard to the implementation of this policy
- ensuring that adequate security management provision is made within the CCG.

8.6 Departmental Heads

8.6.1 Departmental Heads on behalf of the Accountable Officer are responsible for ensuring that the CCG's Security Policy is implemented within the organisation.

8.6.2 This will include responsibility for:

- Planning the capital investment required to address matters arising from the risk assessments.
- Security risk assessment within their areas and for ensuring that staff for whom they are responsible are aware of these risks.
- Preventative measures and appropriate action in respect of persons who are suspected of committing a criminal offence, misconduct or other breach of security in contravention of the policies of the CCG.
- Ensuring staff awareness of this policy and their responsibilities and also ensure that staff receive training appropriate to the risks involved.
- Ensuring that security arrangements within their Directorate are being observed and any deficiencies are reported.
- Ensuring that any particular security problems known to them are reported accordingly.
- Actively reviewing the security arrangements within their Directorate by carrying out routine audits themselves with the co-operation of staff organisations, in line with the CCG's risk assessment procedures.
- An on-going commitment to staff training, carrying out risk assessments, identifying areas at greatest risk and eliminating or controlling these risks.

8.7 Lay Members

8.7.1 To challenge and scrutinise the CCG's responsibilities for security management (as part of their role on Clinical, Quality and Governance) whilst ensuring security has a high profile and appropriate level of consideration in the CCG's Strategic Direction.

8.8 Local Security Management Specialist (LSMS)

8.8.1 The Local Security Management Specialist reports to the Security Management Director. The LSMS' remit is to help deliver an environment, within the CCG, that is both safe and secure. The responsibilities and functions of the LSMS are as follows:

- To undertake the duties of an LSMS in accordance with the NHS standards for commissioners on measures to tackle violence and general security management measures, and compliance with security standards set out by the NHS;
- Ensuring that appropriate steps are taken to create a pro-security culture;
- Delivering security awareness presentations to staff;
- Undertaking Crime Reduction work - such as Crime Reduction Surveys and security management risk assessments relating to the physical security of persons, property, and assets;
- To develop and review both local and organisation wide action plans to implement solutions to security risks identified following risk assessments;
- To implement and maintain active and reactive monitoring, by audit and inspection to ensure adherence to security policies and physical security requirements;

- Undertaking investigations of security breaches as directed by the SMD in a fair, objective and professional manner;
- Ensuring that where a member of staff has been assaulted that appropriate support /counselling has been made available;
- Ensuring that the lessons learned from security incidents or breaches are fed into further risk analysis and Crime Reduction work;
- Ensuring that security incidents or breaches are actioned and reported as required by NHS Security Standards;
- Working with the SMD, the Police, CPS and the CCG's Solicitors to ensure cases are progressed, sanctions are applied, and that redress is sought as appropriate;
- Ensuring that security incidents are publicised as appropriate and in accordance with NHS Security Standards;
- The provision of advice and guidance as required to the CCG on security matters;
- Ensuring that, at least annually, an LSMS Security Management Progress report is presented to the SMD by the LSMS, informing them of the current state of security management within the CCG.

8.9 Estates

8.9.1 The Manager with responsibility for Estates shall be responsible for:

- Advising on the physical security of premises and compliance with statutory regulations and good working practices;
- Ensuring that access points to premises are maintained in good working order to facilitate appropriate ingress and egress;
- Maintaining accurate records of alarm testing and planned preventative maintenance schedules that affect the security of CCG premises;
- Ensuring that the CCG's Specialist Fire Safety Officers are consulted in respect of programmes of work or changes in working practice associated with security needs; to ensure that they do not compromise any of the CCG's fire safety precautions, practices or procedures.

8.10 Managers

8.10.1 Managers are responsible for:

- Informing staff of the security policy and making it readily available;
- Ensuring that local procedures and protocols are developed as required to maintain the security and safety of all persons, property and information within their areas of responsibility;
- Ensuring staff comply with the security policy and follow the procedures and protocols;
- Assessing the training needs of their staff with regard to security issues for example Conflict Resolution Training, Lone Worker, Violence and Aggression;
- Ensuring staff attend courses as per the CCG's training needs analysis;
- Ensuring that staff have access to appropriate information and

instructions regarding the security of personal property and CCG premises;
- Reporting security related accidents, incidents and near misses through the CCG's Incident Reporting system; and
- Seeking advice on security matters as necessary through the CCG's LSMS.
- Act upon recommendations brought forward in security audits.

8.11 Employees

8.11.1 Every staff member has a responsibility for:

- Ensuring that they read and understand the Security Management Policy;
- Following the CCG and its site-specific procedures and protocols regarding the security of people, property, information and premises;
- Making full and proper use of equipment provided to maintain security, and reporting any damage, faults or defects;
- Informing their managers of any unsafe or potentially unsafe working practices or security problems that may pose risks to them, their colleagues, patients, private or CCG property, or CCG premises;
- Informing their managers of any security related accidents, incidents or near misses that they are involved in and completing the relevant documentation;
- Reporting all incidents involving criminal activity; and
- In accordance with their job descriptions, individual members of staff may have responsibilities for: The appropriate use of security equipment (including secure doors, CCTV systems, alarms and detectors) provided by the CCG for the health and safety of their staff, and compliance with the Data Protection Act on CCTV and the Human Rights Act, and reporting any faults/breaches to their manager.
- Arming/disarming security alarms, following the set procedure, when required.
- Staff are reminded that the CCG cannot be held responsible for the loss or damage of their private property, including motor vehicles. They are advised not to bring large amounts of cash or valuables into work and ensure they act responsibly in safeguarding their own belongings, especially if using shared changing facilities.
- All employees have a responsibility/duty of care, to safeguard themselves and others together with their property. Staff must remain vigilant at all times while on CCG property and challenge any persons who are not known to them when safe and appropriate to do so, staff should not put themselves at risk.

8.12 Other persons on CCG premises

8.12.1 All other persons on CCG premises shall observe the CCG's Security Management Policy and rules.

9. Organisational Security Arrangements

9.1 Specific Areas of Security

9.1.1 Basic Security Requirements

9.1.2 In order to achieve maximum security levels the following principles must be applied:

- All contractors and visitors entering a property must register at a reception point by signing in. They must also sign out when they leave the property. The reception point should be at the main entrance.
- Contractors, including maintenance repair people, window cleaners etc. must only be admitted into a property or allowed onto a site if they are in possession of their company ID badge and authorisation for the particular work. If a contractor does not have written authorisation then staff must refuse him/her access into or onto the property.
- For each CCG site, local written procedures should be devised to ensure effective entrance control, including the use of alarm systems, both during the day and particularly at night and at weekends. Such procedures will be consistent with the practical needs of the users of the premises and will reflect fire precaution requirements.
- For each CCG site written procedures should be devised for effective key security. These will cover control and issue and return of keys to staff, locking of doors and windows, and arrangements for obtaining keys for emergency purposes. Such procedures will reflect fire precaution requirements.
- In case of fire a means of escape should be maintained at all material times i.e. when the premises are occupied. Where doors on escape routes are openable only by the use of a key, then all staff who are employed in the premise should carry a key on them at all times. (This applies only in areas where patient security is a requirement).

9.2 Protection of Assets

9.2.1 An inventory shall be maintained of all equipment that has been identified as vulnerable, subject to misuse or a potential breach of security following a local risk assessment.

9.2.2 Wherever equipment included in the register shall be that which is attractive in terms of personal usage, portable and potentially vulnerable to misappropriation, this equipment should be permanently security marked.

9.2.3 Staff responsible for equipment shall carry out a check of all items at least once per year. Any discrepancies shall be notified in writing to the Chief Finance Officer who may also undertake such other independent checks as considered necessary.

9.2.4 Any damage to the CCG's premises, vehicles and equipment, or any loss of equipment or supplies shall be reported by staff using the appropriate incident reporting system.

9.3 Reporting and Recording

9.3.1 All criminal activity must be reported immediately to the Police and to the LSMS and recorded on the CCG's incident reporting system.

9.3.2 All Security incidents must be reported in accordance with the CCG's incident reporting procedure.

9.3.3 The loss of ID badges/access cards should also be reported as an incident using the CCG's incident reporting system.

9.4 Security of CCG Owned Property

9.4.1 All staff will be expected to be concerned with the security of property owned by the CCG and to report any incident where such property is at risk. They will be expected to co-operate in any enquiry into such incidents or where loss by theft or otherwise, is or may be expected.

9.4.2 Staff will not use the CCG's property for their private purposes. Any unauthorised 'use' of property will be construed as misconduct.

9.5 Management of Violence and Aggression

9.5.1 The CCG will fulfil its statutory duty to ensure, so far as is reasonably practicable, the health, safety and welfare of staff and others, in respect of managing the risks associated with violence, aggression and vexatious behaviour.

9.5.2 The aim is to provide, so far as is reasonably practicable, safe working conditions to every employee, with regard to protecting them from violence, aggression and vexatious behaviour at work. (See Appendix A for further guidance).

9.6 Release of Information to Police and Media

9.6.1 Guidance on the release of information relating to a security incident will be given by the Accountable Officer or Communications Lead. If a request is made out of office hours the Manager on-call should be contacted.

9.7 Suspicious Packages

9.7.1 Suspicious packages or objects should be reported to the Manager responsible for that area or another senior member of staff.

9.8 Trespassers

9.8.1 People who enter or remain on CCG premises without having a valid reason to do so can be considered trespassers. In such instances, these people should be asked to leave the site, preferably in front of a witness. If they

refuse, warn them that you will call the police. If this has no effect, then call the police to eject them.

9.9 Security Inspections and Risk Assessments

9.9.1 The LSMS will conduct, in accordance with the published work plan, an annual programme of security inspections and risk assessments. These assessments will include an assessment of both the physical security of the area and an assessment of the security of its assets. Following a Security Inspection the LSMS will provide staff with managerial responsibility for a building or area an inspection report identifying risks and recommendations. A review of key themes highlighted from inspections and risk assessments will be undertaken by the LSMS at least annually.

9.9.2 It will be the role of the service manager to ensure that the proposed recommendations in the inspection report are implemented. In the case of issues of a high risk these will be followed up by the LSMS to ensure that they are completed. In issues of a low to moderate risk, these should be addressed in time for the next inspection.

9.9.3 Where service changes/developments are being considered the LSMS must be invited to contribute at an early stage to ensure consideration is given to the security and crime prevention implications of any change. This is particularly relevant where new premises may be occupied or there are changes to the patterns of use of a building currently in use.

9.10 Integrated Security Systems including access controls and CCTV

9.10.1 All buildings should be reviewed on a 3-year basis to ensure that adequate security systems are in place.

9.10.2 Good access controls are a vital component to ensure that any building and any part of it are accessed by authorised people.

9.10.3 All access control points should be checked regularly to ensure that they are working correctly and properly secure.

9.10.4 Premises, departments and offices vacated for any length of time must be secured to restrict any form of unauthorised entry.

9.10.5 Combinations for key pads should not be given to unauthorised persons and should be changed immediately after any security breach.

9.10.6 The importance of CCTV as a component of a security system is widely supported as CCTV can help clarify whether a security alert is real and is often vital in any post incident investigation.

9.10.7 All CCTV systems operated within the CCG should be properly registered with the Information Commissioner's Office on an annual basis.

9.10.8 Appropriate signage, relative to the location and no smaller than A4, should be placed at the perimeter of the area covered by the CCTV system and shall:

- Inform the public that CCTV is in operation
- Identify who is responsible for the scheme
- Define the purpose of the scheme
- Provide appropriate contact details for the CCGs.

9.10.9 All staff involved in the operating or monitoring of CCTV systems operated by the CCG have a responsibility to comply with associated legislation and guidance.

10. Committee Responsibilities

10.1 Joint Commissioning Committee

10.1.1 The Joint Commissioning Committee is the strategic committee that monitors and approves security management related issues. The Committee will:

- Have overall responsibility for the approval and implementation and monitoring the effectiveness of the Security Management Policy.
- Receive regular reports from the Local Security Management Specialist on Security issues within the CCGs.

11. Training Requirements

11.1 Security awareness shall be brought to the attention of Staff as part of the CCG's induction programme.

12. Compliance

12.1 The Joint Commissioning Committee will have overall responsibility for monitoring the Security Management Policy.

12.2 **The Local Security Management Specialist will:**

- Carry out an annual security risk assessment audit.
- Attend Committees as required.
- Support and advise staff regarding security risk assessment
- Develop the LSMS annual work plan.

12.3 The Security Management Policy will be reviewed on the date identified on the front sheet. If there has been significant change or there is reason to believe that the policy is no longer valid, the policy will be reviewed earlier than the date identified.

13. Approval and Ratification Process

13.1 The Joint Commissioning Committee is responsible for approving the Local Security Management Strategy and associated Policy.

14. Review and Revision Arrangements

14.1 This Strategy and associated Policy will be reviewed annually or sooner in the event of significant changes to organisational structure, systems or processes.

15. Dissemination and Implementation

15.1 Policy documents are available via the CCG's website and intranet. Security awareness will be brought to the attention of staff as part of the CCG's induction programme.

16. Monitoring

16.1 The CCG will monitor and review this policy in partnership with its staff. It will be valid for 3 years, but in order to monitor the implementation and effectiveness of this policy and associated local protocols, local statistics and incident reports will be reviewed regularly by the Joint Commissioning Committee.

17. References

17.1 Security management is part of all relevant policies and procedures, and it is advised that the Security Management Policy is read in conjunction with:

- Anti-Fraud and Corruption Policy
- Lone Working Policy
- Information Technology Policies
- Business Continuity Plan
- Information Governance Policy
- Risk Management Strategy.

Appendix A – Management of Violence and Aggression

1. NHS definition

Physical Assault

"The intentional application of force against the person of another without lawful justification, resulting in physical injury or personal discomfort"

Non Physical Assault

"The use of inappropriate words or behaviour causing distress and / or constituting harassment"

Vexatious

Someone developing a behaviour which is disruptive, excessively persistent, harassing and/or annoying to the organisation or a staff member, over any given period of time.

2. Examples of Physical and Non-Physical Assaults

2.1 Non-Physical Assault

Whilst a non-physical assault is more common than a physical assault, it is still a small number of people we deal with who will display any of the following signs of behaviour. Staff members should have already undergone prevention and handling of violence and aggression training and be equipped with skills to deescalate a situation. Examples of a non-physical assault may include the following:

- Swearing
- Abuse
- Intimidation or attempts to intimidate
- Aggressive behaviour
- Shouting
- Threats to harm
- Harassment
- Inappropriate behaviour or language

This is not an exhaustive list.

2.2 Physical Assault

Whilst a physical assault can be very serious, the likelihood of it happening is very low. Staff members should have already undergone Conflict Resolution Training (CRT) and be equipped with skills to deescalate a situation. Examples of a physical assault may include the following:

- A punch
- A grab
- A kick
- A bite
- A slap
- A push - causing injury
- A head-butt

This is not an exhaustive list.

2.3 Vexatious behaviour

Vexatious behaviour presents itself in a number ways such as harassing, disruptive, unreasonably persistent, serial or habitual complainants and/or annoying behaviour. They could be a combination of all these and could include non-verbal assaults too. This type of behaviour often manifests itself via the complaints process, and the CCG's Complaints Policy outlines in more detail how habitual complainants should be managed.

2.4 Conflict resolution

At all times, staff members should try to follow these principles of conflict resolution:

Try to:

- Remain calm
- Request behaviour to stop
- Signal non-aggression
- Let them vent their feelings
- Acknowledge you have received the message
- Express concern for subject and situation both verbally and non-verbally
- Remind the subject of what they may have to lose
- Sit them down if possible
- ***Leave!***

Try NOT to:

- Create a challenge or aggression
- Intimidate verbally or by use of negative/aggressive body language
- Shout or lose your temper
- Inflame the incident
- Deny a person their dignity
- Threaten any intervention unless you're prepared to use it
- Force them into a corner or no win situation.

Appendix B – General Security Advice for Staff

Proper security creates a better, safer environment in which to deliver healthcare, which benefits both staff and patients alike. A secure environment is safer and more efficient as it helps save money by reducing damage to property and equipment and losses through theft.

1. Report all security incidents (If you see or hear anything suspicious, or are a victim of an incident, you should report as much detail as possible).

Reporting an incident;

- Stay calm
- Give as much information as possible
- After the incident has been sorted out, complete the CCG's incident return.

Details of the incident (the following information will be useful to the police or the LSMS)

- An exact description of what you have seen
- The time
- The place
- The person involved (gender, approx. age, height, build, colouring, unusual characteristics, clothing and any other distinguishing features)
- Any vehicle involved (registration numbers, make, model, colour and direction it was travelling).

2. Preventing theft of personal belongings (many thefts are not planned – they happen because of opportunities created by carelessness)

- Keep credit cards with you, in a buttoned or zipped pocket
- Don't carry large amounts of money
- Keep your purse or wallet and any other valuable items in a locker if provided, or a locked drawer or cupboard
- Don't leave personal belongings lying around in offices or staff rooms
- Don't bring valuable items to work if you don't need them.

3. Making sure CCG property and premises are safe and secure

- Where there are physical measures in place, such as access controls, alarms and staff identity badges make sure you know how to operate them and make sure you use them
- Make sure that valuable equipment is locked away when not in use
- Make sure that doors and windows are locked when rooms and buildings are empty

- Close blinds and curtains, especially in ground-floor rooms so that people can't see in
- Keep unattended offices and store rooms locked
- Use keys, keypads and swipe cards properly
- Make sure doors are locked behind you as appropriate
- Look after keys and swipe cards. If they are lost or stolen, report to your manager immediately
- Return any keys and swipe cards if you stop working for the CCG
- Report any suspicious behaviour, strangers or unauthorised staff seen in secure areas
- Where you feel it is safe to do so, challenge those who do not appear to have any rightful authority to be where they are or who may be acting suspiciously. If you do not feel confident to challenge someone, immediately inform your local security staff or a responsible manager.

4. Personal Safety

General safety rules when walking alone around CCG premises

- Keep to well-lit public areas as much as possible
- Plan ahead, be alert, be aware of your surroundings
- Consider carrying a personal alarm and have it ready to use
- Try to look positive and confident; don't wait around longer than you have to
- Keep handbags and valuables close to you.

General safety rules for cars

- Always lock the car – even when paying for fuel
- Always have the car keys ready, so that you don't have to fiddle around looking for them
- Park in well-lit areas if possible. If parking in day-light for a long time, think how the car park will look in the dark
- When parking, reverse into the gap if possible, so you can pull away easily
- Listen and look around before getting out
- Keep car doors locked whilst driving and consider winding up windows when in slow moving traffic
- Be aware of what people are doing around you
- Use the middle lane, if there is one, when waiting at junctions or lights, so that your car is harder to get at from the pavement
- Do not stop to help if someone has broken down (pull over at the next garage or police station and call for help)
    - If someone tries to pull you over for no reason, drive to the next garage or police station
    - Sometimes car-jackers may "accidentally" bump into your car, aiming to get you out of the car so they can steal it. If this happens stay in the car and wind your window down a little bit to talk to them
    - Keep valuables and bags out of sight and out of reach.

5. Security of Information (protecting patient confidentiality at all times)

Keep records safe.

- All paper-based records should be locked away in desks, filing cabinets or cupboards when they are not in use
- Always keep keys in a safe place
- Use equipment safely
- Place equipment appropriately within secure areas – make sure people cannot see your computer monitor
- When you are going away from your desk, close computer files by using the lock screen function (ctrl, alt, del) and lock documents away
- Know the security procedures for portable equipment such as laptops, tablet PC and mobile phones if you take them out of the workplace
- Remove documents from photocopiers and printers when you have finished. Use secure print (where applicable) for printing.
- Do not leave “Smartcards” unattended in the computer keyboard or laptop
- Make sure only authorised staff can collect incoming letters and emails
- Computer users
    - Make sure you follow proper log-on procedures
    - Choose a secure password and change it often
    - Never give anyone your password or use another person’s password
    - Do not give out details of codes, passwords and other information to those who are not entitled to receive it
    - Do not let written information about codes or passwords be visible to others
    - Only use authorised software. Pirate software is illegal and can damage your computer
    - Take virus controls seriously – always check files transferred from other machines, even those on the same network
    - If there is a systems failure, tell your supervisor or manager immediately.

6. General computer laptop/tablet PC advice

- Don’t leave a laptop/tablet PC in an unlocked vehicle, even if the vehicle is on your driveway or in your garage, and never leave it in plain sight. If you must leave it in a vehicle for a short time, the best place is in a locked boot or glovebox
- Be aware that extreme temperatures can cause damage to computers
- Carry your laptop/tablet PC in a nondescript carrying case, briefcase, or bag when moving about
- If going to lunch or taking a break don’t leave a meeting without your laptop/tablet PC, take it with you
- Don’t let unaccompanied strangers wander around the workplace. Offer assistance and escort the visitors to their destinations
- Be vigilant that you lock the laptop/tablet PC in the boot, if you no longer need it
- This should be done before your journey begins, so that when you arrive at your destination, an opportunist does not see you leaving and locking

your valuables in the car

- Do not use your laptop/tablet PC in a home or any other location, if you feel vulnerable
- Laptops/tablet PCs to be retained in a locked cabinet when not in use and overnight.