NHS
Vale of York
Clinical Commissioning Group

SECURITY POLICY

November 2016

Authorship:	
Reviewing Committee:	**Audit Committee**
Date:	**November 2016**
Approval Body	**Governing Body**
Approved date:	
Review Date:	
Equality Impact Assessment	**TO BE COMPLETED**
Sustainability Impact Assessment	**TO BE COMPLETED**
Related Policies	**COR01a Business Conduct Policy** **COR02 Health and Safety Policy** **COR03 Risk Management Policy** **COR11 CCG Serious Incidents, Incidents and Concerns Policy** **COR12 Whistleblowing Policy** **COR13 Local Anti-fraud, Bribery and Corruption Policy** **COR16 Business Continuity Policy** **COR17 Emergency Resilience Response Policy** **IG05 Information Security Policy** **NHS Vale of York CCG Lone Working Procedure**
Target Audience:	All Staff
Policy Reference No:	**COR21**
Version Number:	**1.1**

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
1.0		New Policy		
1.1	Business Support Manager	LSMS Policy Amendments		

To request this document in a different language or in a different format, please contact:
Sharron Hegarty, Communications Manager
Telephone: 07702 657449
Sharron.hegarty@nhs.net

CONTENTS

1. INTRODUCTION

1.1. This policy covers the general security arrangements within the organisation and notes the relationship with other security related policies. In addition it covers the CCGs responsibilities as commissioners for ensuring that the services they commission are safe and secure.

1.2. NHS Protect leads on work to safeguard NHS staff and resources from crime. It provides support, advice and guidance in this area to organisations across the NHS. NHS Protect works closely with NHS England to ensure organisations commissioning and providing NHS services meet nationally mandated standards in regard to anti-crime work.

2. POLICY STATEMENT

2.1. This policy has been developed based on the knowledge and experience of the Corporate Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3. IMPACT ANALYSES

Equality

3.1. As a result of performing the screening analysis, the policy does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage. The results of the screening are attached.

Sustainability

3.2. A Sustainability Impact Assessment has been undertaken. Positive or negative impacts were identified against the twelve sustainability themes. The results of the assessment are attached.

4. SCOPE

4.1. This policy and guidance is applicable without exception to all staff working within NHS Vale of York CCG whether directly or indirectly employed. It also applies to all visitors to the buildings whether in a business capacity or as a member of the public (e.g. attending a meeting).

5. POLICY PURPOSE/AIMS & FAILURE TO COMPLY

5.1. The purpose of this policy is to detail NHS Vale of York CCG's responsibility for the effective management of security in relation to its corporate responsibilities for staff, patients, visitors and property and for its responsibilities as a commissioner for the security of commissioned services. The CCG is committed to the provision of safeguards against crime and the loss or damage to its own property and to the services its commissions.

5.2. To achieve this it is important for the CCG to:

- Develop a culture which recognises the importance of security;
- Provide and maintain a working environment that is safe and free from danger of crime
- for all people who may be affected by its activities including employees, patients/clients and visitors;
- Prevent loss of or damage to CCG assets and property as a result of crime, malicious acts,
- Damage and trespass;
- Prescribe good order on premises under CCG control;
- Detect and report offenders to management and ensure a robust response in line with the
- National NHS Protect policies;
- Provide support for staff involved in a security incident and supply up to date information
- For all parties especially after an incident;
- Comply with the NHS Protect Security Management Standards for Commissioners including the nomination of an NHS Protect accredited Local Security Management Specialist
- Standards set out a framework for ensuring CCGs have proportionate security
- Management arrangements within their organisation and also in ensuring that the services
- They commission are safe and secure.

5.3. The CCG will ensure it has arrangements in place to meet the requirements of the NHS Protect Security Management Standards for Commissioners. The CCG will determine its level of compliance through completion of a self-review tool (SRT). This is an annual requirement and will be returned to NHS Protect by the specified deadline. The SRT covers the key area of activity outlined in the standards and will be used to inform the development of an on-going review of the annual work plan by the LSMS in conjunction with the Executive Lead.

5.4. The policy covers specific responsibilities relating to:

- Corporate Security Management;
- Security Management in Provider Organisations.

6. PRINCIPAL LEGISLATION AND COMPLIANCE WITH STANDARDS

Health and Safety

6.1. In principle the same considerations should be given to the remote working environment as to the working in the normal office environment. You should ensure your immediate working environment is free of trip hazards, electrical connections are safe etc. It is the employee's duty to always consider the risks surrounding their working environment, and take steps where appropriate.

Theft

6.2. A laptop or other mobile device is a prime target for theft, as they are small, expensive, and generally easy to dispose of. You should:

- Never leave devices unattended
- Never leave devices on view in a motor vehicle. Ideally always take equipment with you, however if you have no choice but leave equipment in a vehicle ensure it is locked in the boot and not visible
- Such equipment can also be an issue in a high-risk environment, such as a housing estate. An individual carrying what is clearly a laptop bag is a prime target, so wherever possible ensure you are aware of the risks surrounding you. The use of rucksacks or other non-obvious bags to carry a laptop may be advisable in some circumstances

Privacy and Information Governance

6.3. The rules applying to information governance in the workplace similar apply to remote working using IT equipment. You should take all steps that are necessary to ensure that information is not disclosed.

6.4. In particular, ensure that you are not overlooked when using any system. If you are in a public place, then find a location where it is not possible for anyone to see over your shoulder. CCTV is also prevalent in today's world, particularly in the UK, so it is advisable to be aware of any cameras overlooking your point of work that might be able to see information on your screen. Privacy screens are available on request from the IMT Department. These screens fit over the laptop's monitor and reduce the viewing angle of the screen so that it is only visible when looked at squarely to the screen.

6.5. The risks associated with a breach of the information governance rules are:

- Accidental breach of patient confidentiality
- Disclosure of other sensitive data of the organisation to unauthorised individuals
- Loss or damage to critical business data
- Damage to the organisation's infrastructure and e-services through spread of un-trapped malicious code such as viruses
- The creation of a hacking opportunity through an unauthorised internet access point
- Misuse of data through uncontrolled use of removable media such as digital memory sticks and other media
- Other operational or reputational damage

Data and Device Encryption

- All mobile devices MUST be equipped with encryption software
- Laptops supplied by the EMBED will have this pre-installed
- Other devices, such as Smartphones should also be encrypted. Any device supplied by the IMT department will already be encrypted, however devices ordered directly from the manufacturer

or distributor may not. If you are in any doubt, please contact the IMT Service Desk. As a guide an encrypted device will require a password at power-on, whereas an unencrypted one will not. Where a device is required for work purposes it should be obtained through the IMT Department to ensure it is properly encrypted before being put into use.

Identifying Labels

6.6. Remote devices should not carry any identifying labels which immediately indicate they are NHS property. It is considered good practice for users to make a note of any serial or asset numbers on the devices you have been issued with. These will be required when any loss or theft is reported.

7. CORPORATE SECURITY MANAGEMENT

7.1. The CCG is committed to providing a safe place of work. To this end this policy is designed to introduce proactive procedures that will ensure, so far as reasonably practicable, not only the health and safety of its staff but the security of its buildings and resources.

7.2. This policy applies to staff employed by the CCG as well as contracted staff undertaking CCG duties, patients, visitors and others.

7.3. The central aim of this policy is to highlight the CCG's strategy in addressing the security and crime risks that confront the organisation with the objective of minimising potential losses through robust security control measures. This aim includes:

- The protection, safety, security and welfare of staff, patients, visitors, contractors and all who attend CCG premises;
- The provision of efficient and effective security control measures to minimise criminal activity including incidents of violence and aggression, loss, damage and/or theft of CCG property and assets;
- Minimising disruption to or loss of service to patients and staff.

7.4. The CCG strives to promote a pro-active security culture throughout the organisation. The CCG utilises a security and crime awareness approach, where staff are actively encouraged to support security and report all incidents and matters of concern as part of an effective security risk management process.

7.5. This process will ensure that adequate security measures are present through:

- Ensuring that security surveys and risk assessments are carried out on the CCG premises and by departments to identify any security risks and recommend measures that are proportionate and commensurate with the risks highlighted;
- Ensuring adequate monitoring of such risk assessments to ensure compliance;
- Providing a secure environment for staff and all who interact with the organisation and, without prejudice to the interest of the organisation, their personal property;

- Regularly liaising with the Police (both local and national levels), other relevant law enforcement and regulatory agencies (e.g. Environment Agency) and NHS Protect to identify security and crime risk trends;
- Providing support and assistance to staff, patients and visitors, as appropriate, who have been subject of a criminal act or exposed to an untoward security related incident.

Key Principles

7.6. In order to reduce crime, it is necessary to take a multi-faceted approach that is both proactive and reactive. The CCG has therefore adopted the three key principles designed to minimise the incidence of crime, and to deal effectively with those who commit crimes against the NHS:

- **Inform and Involve** those who work for or use the NHS about crime and how to tackle it. NHS staff and the public are informed and involved with a view to increase understanding of the impact of crime against the NHS.
- **Prevent and Deter** crime in the NHS to take away the opportunity for crime to occur or to re-occur and discourage those individuals who may be tempted to commit crime, by implementing robust systems, which will be put in place in line with policy, standards and guidance developed by NHS Protect. Successes may be publicised so that the risk and consequences of detection are clear to potential offenders.
- **Hold to Account** those who have committed crime against the NHS. Crimes must be detected and investigated, suspects prosecuted where appropriate, and redress sought where possible. Where necessary and appropriate, this work will be conducted in partnership with the police and other crime prevention agencies. Where recovery of monies lost to crime is viable, this will be pursued. In relation to crimes against NHS staff, criminal damage or theft against NHS property, investigation and prosecution will be undertaken in liaison with the police and CPS or where necessary NHS Protect.

Roles and responsibilities for Corporate Security Management

7.7. The **Accountable Officer** has responsibility to ensure that systems are in place to ensure that the risk to employees is minimised as far as reasonably practicable.

7.8. The **Executive Lead** for the CCG would be the Chief Finance Officer and they are required to take responsibility for security management matters. The Executive Lead, on behalf of the Accountable Officer, is responsible for ensuring that the CCG's Security Policy is implemented within the organisation.

7.9. This will include the responsibility for:

- Assisting the Local Security Management Specialist in the performance of their duties, including the investigation of incidents, security assessment of working areas and the reporting of all security related incidents;

- 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 that adequate funding is allocated for necessary security measures within the CCG premises. They should also ensure that security implications are considered as part of tendering processes for new and existing services
- Reports on Security management and any incidents will be reported to the Audit and Governance Committee.

7.10. The CCG is required to nominate an individual as the **Local Security Management Specialist (LSMS)**. NHS Protect are to be informed of any such nomination. The nominated individual must be accredited by NHS Protect to undertake the LSMS role. The LSMS will:

- Report directly to the Executive Lead and be responsible for liaising between the CCG and NHS Protect;
- Report to NHS Protect any weaknesses in security related systems of the NHS body or other matters which the LSMS considers may have implications for security management in the NHS;
- Prepare a written work plan, with the Executive Lead and prepare regular reports on progress against that plan to the Audit and Governance Committee;
- Provide competent advice on the CCGs management of security;
- Review security policies;
- Conduct security risk assessments; (and include/escalate risks to the risk register in line with the CCG's risk management strategy);
- Review security incidents and report all incidents of violence and aggression, as required, to the police where appropriate and NHS Protect;
- Identify learning from security incidents and review policies and procedures to prevent reoccurrence;
- Attend the relevant committees; and provide progress and annual reports;
- Monitor progress made against recommendations arising from security audits;
- Assist local managers in carrying out investigations into security related incidents, liaising as required with local Police, the Criminal Justice Unit and the Legal Protection Unit and where necessary preparing case files for submission to Court as part of the prosecution process;
- To foster links with local agencies and bodies, such as Police, Crime and Disorder Reduction Partnerships and other security professionals in neighbouring NHS organisations;
- Ensuring completion of self-assessment tool for review by the Executive Lead.

7.11. **Managers** are responsible for:

- Their own teams' security in terms of providing a safe and secure environment;
- Ensuring their staff understand and comply with this policy;
- Ensuring all significant security risks are identified and measures are implemented to establish a safe and secure environment;
- Actively encouraging the reporting of incidents relating to security issues in accordance with the CCG's incident reporting procedures;
- The initial investigation of any incident related to a security issue and/or violence at work, involving the LSMS at an appropriate stage.

7.12. **Employees** should:

- Familiarise themselves with the content of this policy and associated procedures;
- Familiarise themselves with any special security requirements relating to their place of work;
- Safeguard themselves, colleagues, visitors, clients etc., so far as is reasonably practicable;
- Ensure that neither equipment nor properties are put in jeopardy by their actions, either by instruction, example or behaviour;
- Co-operate in the completion of risk assessments;
- Comply with policies/procedures, control measures and safe systems of work;
- Report any security concerns/breaches or incidents as soon as possible;
- Attend appropriate training sessions;
- Provide support and co-operation with any investigations;
- Use all security equipment in accordance with any training and instructions given e.g. panic alarms;
- Remain alert to the presence of unusual and unexplained packages, which cannot readily be identified. Any such package should be reported immediately to a supervisor or line manager. Under no circumstances should a suspect package be handled.
- Wear CCG identity badges at all times unless otherwise directed due to control of infection or personal safety.

8. RISK MANAGEMENT STRATEGY

8.1. Risk Management is at the heart of the Security Strategy. Risk management techniques harness the information and experience of CCG staff (and external expertise if necessary); translating this into positive action to remove or manage hazards and reduce risks.

8.2. A security risk assessment will need to be completed and reflected in the risk register. The risks should be reflected in an annual work plan along with clear objectives that are measurable. The plan will be monitored by the Executive Lead to ensure that resources to mitigate the risks are sufficient). Security risk assessment involves:

- Review of the various activities of the CCG and identification of critical areas for the organisation;
- Identification of the risks that exist:
- What could go wrong?
- How could it happen?
- What would be the effect?
- Assessing those risks for potential frequency and severity;
- Eliminating the risks that can be eliminated;
- Identifying how remaining risks can be mitigated or managed;
- Developing and delivering a plan for implementing the identified changes;
- Provides current measurement and assists target setting for reduction in risks.

8.3. The CCG will carry out appropriate risk scoping on physical security of premises and assets every year. Where properties are leased, the risk assessment may be undertaken in conjunction with the owners of the premises occupied by the CCG. Following a risk assessment on premises or assets an action plan will be developed with timescales and nominated persons to carry out agreed action. Relevant policies will be revised or developed where required to address risks identified through the risk assessment process. Such policies will be monitored for effectiveness via meaningful data and kept under review for changes where required. Policies will be communicated across the organisation.

8.4. If new premises or assets are commissioned within the CCG these will be risk assessed prior to operational use of them, in line with this policy.

8.5. A security assessment check sheet is included at Appendix 3 of this policy.

Security-specific risk management measures

8.6. Following risk assessment, managers are responsible for developing any local procedures required to ensure security of premises, for example, arrangements for the items listed below. This list is not exhaustive and managers may identify other issues:

- Unlocking and locking of premises;
- Responding to violent, aggressive or abusive behaviour;
- Access to CCG premises including staff identification badges, access controls;
- Lone working/personal safety;
- Relevant arrangements for contractors to access premises as required.

Identification Badges

8.7. ID badges are issued to all staff on commencement of employment following an induction with City of York Council where the CCG co-locates. ID badges must be worn at all times whilst on CCG premises or business. Persons not wearing an ID badge should be challenged and asked to identify themselves.

8.8. When staff leave CCG employment, all ID badges should be returned to the Manager and destroyed. If an ID badge is lost or stolen this must be reported to the Manager and reported via the CCG incident reporting system.

8.9. The ID badge is also used a building entry and exit pass which must be swiped when entering and exiting the premises.

Visitors / Contractors

8.10. All visitors / contractors are to be signed in and out of CCG premises via City of York Council Reception. For security reasons all visitors must be escorted to and from their destination within the City of York Council building.

CCG Property / Assets

8.11. Managers are responsible for undertaking risk assessments regarding the security of assets held within their departments and this should be included in the service / departmental general risk assessment. Where appropriate, items should be placed on the asset register or an appropriate inventory depending on value. The Business Support Manager maintains the asset register and a review of CCG property held by staff takes place on a regular basis to ensure that all items are securely managed. All mobile assets such as laptops and smartphones should have a VOYCCG security asset number sticker which is added to the asset register.

8.12. All managers and staff should take all reasonable steps to safeguard CCG property whilst it is in their care. Members of staff should not remove property belonging to the CCG without prior authority from their line manager or the custodian of the equipment. Failure to obtain authority could result in disciplinary action or criminal proceedings being taken.

Personal Property

8.13. Staff should be aware that the CCG cannot accept liability for loss or damage to staff property brought onto its premises.

8.14. Staff are advised to take adequate precautions to ensure the safety of their possessions and not bring valuables to work. Where storage has been provided for personal use, the individual to whom it is allocated will be responsible for ensuring it is locked.

8.15. Staff must report any loss of, or damage to, their belongings and co-operate in any consequent inquiry into the loss or damage. If private property has been stolen then it is the owners and not the CCGs responsibility to report the matter to the Police. This should be after notifying a line manager and reporting the incident. Any reference number assigned should also be recorded in the incident log.

Security of Motor Vehicles

8.16. The CCG cannot accept liability for any private motor vehicle or its contents when they are parked on a CCG site or when the car is being used by an employee on CCG business.

Lease Cars

8.17. In the event of an incident or accident involving a lease car, the employee must notify their manager and the lease car management company in accordance with the lease car policy issued to them.

Prevention of Violence to Staff

8.18. The CCG has a duty to provide a safe and secure environment for all employees and visitors and has a zero tolerance approach to violence or abusive behaviour. The CCG takes a very serious view of violence, abuse and aggression at work and recognises its responsibility to protect employees and others who may be subjected to any acts of violence, abuse or aggression whether or not the act results in physical or non-physical assault and whether carried out by members of the public, patients, relatives or by members of staff. Violent or abusive behaviour will not be tolerated and decisive action will be taken by the CCG to protect staff, patients and visitors.

Bomb Threats and the Law

8.19. The vast majority of bomb threats are hoaxes. Making such malicious calls is an offence contrary to Section 51 of the Criminal Law Act and should always be reported to the police. Any member of staff receiving such a call should seek the immediate advice of the most senior manager available.

Personal Safety and Lone Working

8.20. Managers must ensure that a risk assessment is undertaken and documented, for all staff considered to be lone workers. The risk assessment should include precautions to reduce the likelihood of harm occurring. See Appendix 4.

Information Security

8.21. All staff must abide by the code of confidentiality issued by the CCG 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.

8.22. There is a suite of Information Governance policies available which must be referred to within the NHS Vale of York CCG. Please familiarise yourself with these.

Incident Reporting

8.23. All security related incidents / near misses should be reported to local line management and the LSMS, using the CCG incident reporting procedure, (see CCG Serious Incidents, Incidents and Concerns Policy). If urgent but not criminal a local investigation should be initiated by managers.

8.24. All incidents of crime should be reported to the local Police Station. The LSMS should be notified as soon as possible by telephone / email and by the completion of a CCG reporting form.

8.25. Examples of reportable incidents include, but are not limited to:

- Physical assault or verbal abuse by a patient, visitor or another member of staff towards a member of staff;
- Physical assault or verbal abuse by a member of staff towards a patient or visitor;
- Theft of staff or CCG property;
- Leaving workplaces open at the end of the working day;
- Damage to premises that was the result of criminal activity (including arson)

8.26. If you are in any doubt as to what is reportable and what isn't, you should contact the LSMS.

Assisting the Police with Investigations

8.27. From time to time the police may contact the CCG for information relating to an on-going investigation. An individual who is contacted in such a manner should refer the Police to the LSMS or the Executive Lead.

8.28. Staff should obtain guidance from Information Governance on when and the extent of confidential information may be disclosed.

Learning from Incidents

8.29. The CCG will ensure that learning from incidents is reviewed and leads to policy and procedural changes to prevent reoccurrence. This will be incorporated in the work plan of the LSMS.

9. ASSURING SECURITY MANAGEMENT IN PROVIDER ORGANISTIONS

9.1. Under the NHS Standard Contract all organisations that are licensed by Monitor or are a Trust providing NHS services (providers) must put in place and maintain appropriate anti-crime arrangements. The NHS organisations which commission the services (commissioners) should review providers' arrangements to make sure they meet the requirements under the contract.

9.2. As a commissioning organisation, the CCG has responsibilities under the NHS Protect Security Standards for Commissioners for ensuring that the services they commission are safe and secure.

9.3. The primary areas of activity to be undertaken by the CCG will be to ensure providers of commissioned services comply with the current security standards for providers.

Roles and Responsibilities for Assuring Security Management in Provider Organisations

9.4. The **Accountable Officer** has responsibility to ensure that systems are in place to ensure that the risk to employees is minimised as far as reasonably practicable.

9.5. The **Chief Finance Officer** has been designated as the Executive Lead to take responsibility for security management matters.

9.6. The **Local Security Management Specialist (LSMS)** is to:

- To review the security management provisions put in place by the provider, in accordance with Service Condition 24 of the NHS Standard Contract;
- To liaise with providers and appropriate regulators and advisory bodies on security issues on an on-going basis;
- To review findings from investigation of serious incidents and ensure these lead to improvement in arrangements.

9.7. The **Contracting Team** are to:

- Work with the LSMS to review providers' security management arrangements to ensure they meet the requirements of the standard commissioning contract if required (ie. Monitor licensed or a Trust)
- Use the NHS Standard Contract when commissioning NHS funded services

10. POLICY IMPLEMENTATION

10.1. The CCG will ensure that a copy of this policy is freely available to all CCG staff (electronically and/or hard copy). Managers should receive the appropriate advice to ensure the content of this policy is fully implemented

11. TRAINING & AWARENESS

11.1. Managers will determine the level of training required by their staff and reassess this training need as and when their roles / job changes.

11.2. Staff will be provided with access to the policy, and a brief overview of relevant areas, as part of the City of York Council induction. Staff will be expected to read the policy as part of their induction process.

11.3. Health and Safety training is a statutory requirement of legislation and therefore mandatory for all staff of the CCG (aspects of security training cut across health and safety training). A range of training will be available to staff through e-learning.

11.4. All new permanent employees must complete mandatory training at the earliest practicable time after commencing employment. This training includes Health and Safety, Fire, Information Governance and Manual Handling.

11.5. 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 to attend.

MONITORING & AUDIT

11.6. Managers will be responsible for monitoring and reviewing their own local security risk assessments and associated building arrangements. The review of policies will also be based on the prioritisation of risk within the CCG and as a consequence of any serious incidents.

11.7. The LSMS reviews all risk assessments and all incidents relating to security of premises and assets and reports to relevant staff and committees as soon as practicable after the event;

11.8. Risk assessments:

- Trends
- Progress with action plans
- Blocks to implementation

11.9. Incidents:

- Number
- Trends
- Progress with action plans
- Blocks to implementation

11.10. Security breaches and other loss events will be reported on a regular basis to the Audit and Governance Committee. The investigation of such incidents will be used as a tool to identify common causes, assist police, prevent reoccurrence and assess the effectiveness of policy controls.

11.11. Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCGs disciplinary procedure.

11.12. To provide assurance on the effectiveness of the policy, the LSMS will report directly to the Executive Lead and attend the Audit and Governance Committee to provide progress and annual reports.

12. POLICY REVIEW

12.1. This policy will initially be reviewed after 12 months and then on a three yearly rolling basis however it may be reviewed earlier in line with new guidance and with reference to prosecution progress and Risk Assessment findings.

13. REFERENCES

- Health and Safety at Work Act 1974
- Management of Health and Safety at Work Regulations 1999
- NHS Standard Contract (National Commissioning Contract)
- Crime and Disorder Act 1998
- Data Protection Act 1998
- Workplace Health, Safety and Welfare Regulations 1992
- Freedom of Information Act 2000
- Human Rights Act 1998 (in particular article 8 ‘Human Rights Bill 1998 – the right to respect for private and family life’)

- NHS Protect Standards for Commissioners – Security Management

14. ASSOCIATED POLICIES

- COR01a Business Conduct Policy
- COR02 Health and Safety Policy
- COR03 Risk Management Policy
- COR11 Serious Incident and Concerns Policy
- COR12 Whistleblowing Policy
- COR13 Local Anti-fraud, Bribery and Corruption Policy
- COR16 Business Continuity Policy
- COR17 Emergency Resilience Response Policy
- IG05 Information Security Policy
- NHS Vale of York CCG Lone Working Procedure

15. CONTACT DETAILS

Policy and Assurance Manager
Telephone: 01904 555870
Email: pennie.furneaux@nhs.net
Address: NHS Vale of York Clinical Commissioning Group, West Offices, Station Rise, York. Y01 6GA

16. DEFINITIONS

16.1. NHS Protect: This organisation has responsibility for all policy and operational matters relating to the prevention, detection and investigation of fraud and corruption and the management of security in the National Health Service.

16.2. Physical Security: This term as understood by Health and Safety professionals relates to buildings and objects as any security hardware including locks, access control, intruder alarms, panic alarms, barriers etc that supports the security function.

16.3. Security: A state of being where the risks to people and property are minimised in relation to any actions that may lead to personal injury, threat to life or the disruption of business activity of the organisation.

16.4. Security Incident: Any act or omission that has the potential to undermine the integrity of the CCGs security objectives and would include non-compliance whether deliberate or otherwise with the CCG Security Policy and/or local security arrangements.

16.5. Criminal Act: Any violation or attempted violation of law whether statute or common law and would include such offences that are more likely to occur within the healthcare setting such as:

- Harassment;
- Assaults and threats of violence;
- Theft and kindred offences such as burglary;
- Criminal damage;

- Offences relating to public disorder;
- Fraud.

16.6. **Premises:** The physical buildings, grounds and all property contained within the CCG boundaries in which NHS staff and professionals work and from which the business of the NHS is delivered.

16.7. **Assets:** Irrespective of their value, 'Assets' can be defined as the materials and equipment used directly or indirectly to deliver NHS healthcare. In respect of staff, professionals and patients, the definition can also apply to their personal possessions they retain whilst on CCG premises or working in or providing a service to the NHS.

17. APPENDIX 1: EQUALITY IMPACT ANALYSIS FORM

1.	**Title of policy/ programme/ service being analysed**
	Security Policy
2.	**Please state the aims and objectives of this work.**
	This policy covers the general security arrangements within the organisation. The CCG is committed to providing a safe place of work. This policy is designed to introduce proactive procedures that will ensure, so far as reasonably practicable, not only the health and safety of its staff but the security of its buildings and resources.
3.	**Who is likely to be affected? (e.g. staff, patients, service users)**
	Staff directly employed on the business of the organisation, (both on and off premises, during working hours); all visitors to CCG offices, (public, business partners and service support staff); temporary staff employed by the organisation.
4.	**What sources of equality information have you used to inform your piece of work?**
5.	**What steps have been taken ensure that the organisation has paid due regard to the need to eliminate discrimination, advance equal opportunities and foster good relations between people with protected characteristics**
6.	**Who have you involved in the development of this piece of work?**
	Internal involvement: Senior Management Team **Stakeholder involvement**: City of York Council **External Advice Sought From:** Internal Audit Counter Fraud **Patient / carer / public involvement**: This is an Internal policy aimed at staff employed by the CCG and contractors working for the CCG. The focus is on compliance with statutory duties and NHS mandated principals and practice. There are no particular equality implications.
7.	**What evidence do you have of any potential adverse or positive impact on groups with protected characteristics?** **Do you have any gaps in information?** **Include any supporting evidence e.g. research, data or feedback from engagement activities**

Disability People who are learning disabled, physically disabled, people with mental illness, sensory loss and long term chronic conditions such as diabetes, HIV)	Consider building access, communication requirements, making reasonable adjustments for individuals etc
N/a	
Sex Men and Women	Consider gender preference in key worker, single sex accommodation etc
N/a	
Race or nationality People of different ethnic backgrounds, including Roma Gypsies and Travelers	Consider cultural traditions, food requirements, communication styles, language needs etc.
N/a	
Age This applies to all age groups. This can include safeguarding, consent and child welfare	Consider access to services or employment based on need/merit not age, effective communication strategies etc.
N/a	
Trans People who have undergone gender reassignment (sex change) and those who identify as trans	Consider privacy of data, harassment, access to unisex toilets & bathing areas etc.
N/a	
Sexual orientation This will include lesbian, gay and bi-sexual people as well as heterosexual people.	Consider whether the service acknowledges same sex partners as next of kin, harassment, inclusive language etc.
N/a	
Religion or belief Includes religions, beliefs or no religion or belief	Consider holiday scheduling, appointment timing, dietary considerations, prayer space etc.
N/a	
Marriage and Civil Partnership Refers to legally recognised partnerships (employment policies only)	Consider whether civil partners are included in benefit and leave policies etc.
N/a	

Pregnancy and maternity Refers to the pregnancy period and the first year after birth	Consider impact on working arrangements, part-time working, infant caring responsibilities etc.
N/a	
Carers This relates to general caring responsibilities for someone of any age.	Consider impact on part-time working, shift-patterns, options for flexi working etc.
N/a	
Other disadvantaged groups This relates to groups experiencing health inequalities such as people living in deprived areas, new migrants, people who are homeless, ex-offenders, people with HIV.	Consider ease of access, location of service, historic take-up of service etc
N/a	

8.	**Action planning for improvement** Please outline what mitigating actions have been considered to eliminate any adverse impact? Please state if there are any opportunities to advance equality of opportunity and/ foster good relationships between different groups of people? An Equality Action Plan template is appended to assist in meeting the requirements of the general duty

Sign off
Pennie Furneaux, Policy and Assurance Manager
Date analysis completed
Name and signature of responsible Director
Date analysis was approved by responsible Director

18. APPENDIX 2: SUSTAINABILITY IMPACT ASSESSMENT

Staff preparing a policy, Governing Body (or Sub-Committee) report, service development plan or project are required to complete a Sustainability Impact Assessment (SIA). The purpose of this SIA is to record any positive or negative impacts that this is likely to have on sustainability.

Title of the document	Security Policy
What is the main purpose of the document	This policy covers the general security arrangements within the organisation. The CCG is committed to providing a safe place of work. This policy is designed to introduce proactive procedures that will ensure, so far as reasonably practicable, not only the health and safety of its staff but the security of its buildings and resources.
Date completed	23rd November 2016
Completed by	Pennie Furneaux, Policy and Assurance Manager

Domain	**Objectives**	**Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = n/a**	**Brief description of impact**	**If negative, how can it be mitigated? If positive, how can it be enhanced?**
Travel	Will it provide / improve / promote alternatives to car based transport?	0		
	Will it support more efficient use of cars (car sharing, low emission vehicles, environmentally friendly fuels and technologies)?	0		
	Will it reduce 'care miles' (telecare, care closer) to home?	0		
	Will it promote active travel (cycling, walking)?	0		
	Will it improve access to opportunities and facilities for all groups?	0		
	Will it specify social, economic and environmental outcomes to be accounted for in procurement and delivery?	0		
Procurement	Will it stimulate innovation among providers of services related to the delivery of the organisations' social, economic and environmental objectives?	0		

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = n/a	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced?
	Will it promote ethical purchasing of goods or services?	0		
Procurement	Will it promote greater efficiency of resource use?	0		
	Will it obtain maximum value from pharmaceuticals and technologies (medicines management, prescribing, and supply chain)?	0		
	Will it support local or regional supply chains?	0		
	Will it promote access to local services (care closer to home)?	0		
	Will it make current activities more efficient or alter service delivery models	00		
Facilities Management	Will it reduce the amount of waste produced or increase the amount of waste recycled? Will it reduce water consumption?			
Workforce	Will it provide employment opportunities for local people?	0		
	Will it promote or support equal employment opportunities?	0		
	Will it promote healthy working lives (including health and safety at work, work-life/home-life balance and family friendly policies)?	1	Clear principles and references to operating procedures that promote safety.	
	Will it offer employment opportunities to disadvantaged groups?	0		
Community Engagement	Will it promote health and sustainable development?	0		
	Have you sought the views of our communities in relation to the impact on sustainable development for this activity?	N/a		
Buildings	Will it improve the resource efficiency of new or refurbished buildings (water, energy, density, use of existing buildings, designing for a longer lifespan)?	0		

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = n/a	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced?
	Will it increase safety and security in new buildings and developments?	0		
	Will it reduce greenhouse gas emissions from transport (choice of mode of transport, reducing need to travel)?	0		
	Will it provide sympathetic and appropriate landscaping around new development?	0		
	Will it improve access to the built environment?	0		
Adaptation to Climate Change	Will it support the plan for the likely effects of climate change (e.g. identifying vulnerable groups; contingency planning for flood, heat wave and other weather extremes)?	0		
Models of Care	Will it minimise 'care miles' making better use of new technologies such as telecare and telehealth, delivering care in settings closer to people's homes?	0		
	Will it promote prevention and self-management?	0		
	Will it provide evidence-based, personalised care that achieves the best possible outcomes with the resources available?	0		
	Will it deliver integrated care, that co-ordinate different elements of care more effectively and remove duplication and redundancy from care pathways?	0		

19. APPENDIX 3: SECURITY ASSESSMENT CHECK SHEET

Security Assessment Check Sheet

Name of organisation:
Address of premise:
Identification of area within the premise:
Date of Assessment:
Assessment undertaken by (print name):

Security Management				
	Yes	**No**	**N/A**	**Comments**
1. Has a suitable and sufficient workplace security risk assessment been carried out identifying all significant hazards?				
2. Is the security risk assessment readily available and does it identify control measures to either remove or reduce hazards?				
3. Are risks placed on the Risk Register updated or removed as appropriate?				
4. Have management developed safe systems of work for work activities to protect persons within the premise?				
5. Are staff aware of organisational security procedures and suitable trained?				
6. Does the work place have an effective security alarm system?				
7. Is there suitable monitoring of security measures in place?				
8. Are security arrangements regularly monitored?				
9. Is the workplace risk assessment regularly/annually reviewed?				

Security Prevention – General				
	Yes	**No**	**N/A**	**Comments**
10. Is there an effective system for ensuring that access to the premise is suitably secure and persons within the premise are readily identifiable?				
11. Is there an effective procedure/system for ensuring external/internal accommodation is secured when un-occupied?				
12. Is there an effective system for the recording of organisational assets and equipment within the workplace?				
13. Are all employees provided with and display photographic/name identification?				
14. Are all employees in high risk areas properly informed of the particular risks and the means to control the risks?				
15. Is external lighting (where provided) suitable to illuminate persons wishing to gain entry to the premise?				
16. Are all security related incidents recorded and reported in accordance with CCG Risk Management Policy using the Incident Reporting Form?				

Security Prevention – Employees				
	Yes	**No**	**N/A**	**Comments**
17. Has a security training needs analysis been completed for staff within the workplace (i.e. Personal Safety Plan)?				
18. Are training records readily available?				
19. Has a Lone Worker Assessment been undertaken and control measures identified implemented?				
20. Are staff made aware that the CCG will not accept liability for the loss of personal belongings within the workplace?				

Security – Access				
	Yes	**No**	**N/A**	**Comments**
21. Is there an effective procedure for the registration security, monitoring and distribution of keys?				

22. Are keys issued against a name, date, and signature?				
23. Are distributed keys checked on a regular basis by management?				
24. Are security codes for doors fitted with digital access recorded and changed regularly or on change of staff?				
25. Are suitable procedures available for staff to challenge unidentified persons or persons in unauthorised area within the premise?				
26. Is there an effective procedure for recording all persons within the workplace?				

Security - Confidential Information				
	Yes	**No**	**N/A**	**Comments**
28. Are adequate arrangements in place for compliance with CCG Policies and Procedures on Confidentiality of Information for: • Patient Medical Records • Employee Personnel Records • Complaints • Financial • Contracts for Services and Goods				
29. Is all data information contained on electronic retrieval systems securely protected in accordance with CCG Policy?				

Security Assessment Check Sheet Results

If all answers to the questions above are 'Yes' or 'N/A', security arrangements are considered to be adequate; no further action is required at this time. Simply sign and date the form in the space provided below.

If one or more answers to the questions above are 'No', your security arrangements may be considered inadequate and needs to be addressed if applicable to the workplace.

20. APPENDIX 4: NHS VALE OF YORK CCG LONE WORKING PROCEDURE

Introduction

This procedure document has been developed to support staff and line managers to ensure staff safety when lone working. This procedure document is to be read in conjunction with the NHS Vale of York CCG Lone Working Risk Assessments.

Scope

This Procedure document applies to all staff within NHS Vale of York CCG

Procedure

- Managers to identify all staff within their team who may lone work.
- Register of lone working staff to be completed by Line Managers and forwarded to Chief Operating Officer (Template attached at appendix 5)
- All lone working staff to have a lone working risk assessment completed by line manager in line with the organisational risk assessment for lone working, and forward completed assessments to Chief Operating Officer .

Safe System of Work

- All staff within the team will fully open their diaries to other members of the team.
- The intrinsic security of the building will not be compromised by lone workers, e.g. security doors will not be propped open, other people who should not be on the premises will not be brought on the premises by lone workers, etc.
- Full contact details of all off site working and meetings including full addresses of the venue, any applicable accommodation and full names, addresses (if applicable) and telephone/email addresses of contacts and other attendees to be notated in the diary entry.
- Corporate mobile phones to be in use at all times the staff member is lone working, to be able to alert others or to summon help if required.
- If attending meetings at home addresses, contact should always be made with people with knowledge of the person meeting so a risk assessment can be completed if required.If the risk assessment deems it necessary escalation procedures such as attending in two's, open communication whilst in the meeting etc. should be implemented.
- ICE contact to be incorporated in the mobile phone.
- If agreed, personal mobile phone numbers to be shared within the team.
- Informal buddy system to be put in place with definite timescales for escalation noted.
- Escalation procedure to be maintained.

Escalation Procedure

If a staff member is lone working and has been out of contact with their buddy for 1 hour after the expected timed response the following procedure will be undertaken.

Contact with the staff member via mobile phone (corporate and personal if applicable), text message and email to be made. If no response within 15 minutes escalation to senior manager to be initiated and personal contact details to be requested from HR.

Contact to be made with next of kin or ICE contact details held on file. If contact unsuccessful or negative response gained. Senior manager to make decision to escalate to Police.

21. APPENIDIX 5: REGISTER OF LONE WORKING STAFF

Register of Lone working staff

Team……

Line Manager completing register……

Staff Name	Type of lone working [1]	Frequency of lone working[2]	Lone working risk assessment completed[3]

[1] E.g. attending meetings off site, lone working in building outside normal working hours, lone working in community locations

[2] Could be daily, weekly, monthly, annually, ad-hoc, etc.

[3] Insert date lone working risk assessment was completed