NHS
Herts Valleys
Clinical Commissioning Group

Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

	Yes/No/ Unsure	Comments
Title of Document		HVCCG Security Policy
Could this policy be incorporated within an existing policy?	N	
Does this policy follow the style and format of the agreed template?	Y	
Has the front sheet been completed?	Y	
Is there an appropriate review date?	Y	
Does the contents page reflect the body of the document?	Y	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Y	
Are all appendices appropriate and/or applicable?		
Have all appropriate stakeholders been consulted?	Y	
Has an Equality Impact Assessment been undertaken?	Y	
Is there a clear plan for implementation?	Y	
Has the document control sheet been completed?	Y	
Are key references cited and supporting documents referenced?	Y	
Does the document identify which Committee/Group will approve it?	Y	

Plans for communicating policy to – staff; practice membership; public (as appropriate)	Y	Policy to be posted on the intranet and circulated in the weekly newsletter

Individual Approval

If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.

Name	Caroline Hall	Date	December 2017
Signature			

Committee Approval

If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.

Name	Kathryn Magson	Date	December 17
Signature			

NHS
Herts Valleys
Clinical Commissioning Group

SECURITY POLICY

Version Number	1.3
Ratified By	HVCCG Exec Team
Date Ratified	December 2017
Name of Originator/Author	Amanda Yeates
Responsible Director	Chief Finance Officer
Staff Audience	All Staff
Date Issued	December 2017
Next Review Date	December 2019

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
1.0		New Plan	Jan 15	AY
1.2		Review by Health & Safety Advisor – no changes suggested.	Sep 15	AY

NHS
Herts Valleys
Clinical Commissioning Group

CONTENTS

1. INTRODUCTION

Herts Valleys Clinical Commissioning Group (HVCCG) is committed to promoting and improving security for all of its staff and visitors. The CCG aims to provide and maintain a calm, pleasant and secure working environment where, visitors and staff are confident of their personal safety and security of their property, buildings and equipment are safeguarded.

The CCG can be exposed to a number of security risks relating to staff, patients, premises and assets. Security breaches can have a significant impact on the organisation and its staff. Whilst the CCG recognises that it may be impossible to prevent every security incident, it will provide resources to assist in handling such matters. All CCG employees have a responsibility to ensure that security measures and procedures are observed at all times. Managers of the CCG should take a leading role in promoting and developing a security conscious culture.

This policy fits within the framework of the CCG’s health and safety arrangements and associated risk management processes. The incident reporting process is important, in the management of security risks. Members of staff are actively encouraged to report all types of incidents, no matter what their severity, to support proactive as well as reactive risk management.

2. PURPOSE

The purpose of this policy is to detail the responsibility of HVCCG for the effective management of security in relation to staff visitors and property. The CCG will do its utmost to safeguard against crime and against loss or damage to property or equipment. The main aim of the policy is to minimise potential losses by strict control, as well as preventing violent or aggressive behaviour towards staff, but it also aims to:

- Protect the safety, security and welfare of staff, contractors and the general public while on CCG property
- Provide safe systems and safeguard against crime, fraud, loss, damage or theft of property, equipment or other CCG assets
- Ensure the detection and reporting of suspected offenders committing offences against patients, staff or property within CCG premises
- Educate staff in proactive and general security awareness

To achieve this it is important for the CCG to:

- Develop a culture which recognises the importance of security
- Undertake security risk assessments to evaluate and resolve any security problems

	• Provide support to staff involved in a security incident and supply up to date information for all parties, especially after an incident. • Continually improve performance with regard to security through the participation, commitment and support of other organisations and all staff This policy applies to all CCG leased premises, vehicles, assets and activities. It applies to all members of staff, patients, contractors and visitors.
3.	**DEFINITIONS**
3.1	The term "security" applies to the elimination or reduction of risk of crime across the CCG. It includes: • Offences against individuals – assault and bodily harm, harassment and theft • Offences against property – criminal damage, burglary and theft • Offences against assets – fraud, theft, bribery or corruption
3.2	"Security management" can be defined as an environment where the risks to people and property are minimised from any actions that may lead to personal injury, threat to life or the disruption of business activity of the CCG.
4.	**ROLES AND RESPONSIBILITIES**
4.1	**Roles and Responsibilities within the Organisation**
4.1.1	The **Chief Executive** has overall responsibility on behalf of the CCG Board and is responsible for the organisation and management of security measures across the CCG.
4.1.2	The **Chief Finance Officer** has been designated as the Director to take responsibility for security management matters.
4.1.3	The **Head of Corporate Support** is responsible for: • The development, implementation and maintenance of an effective security policy, and other security related documents, ensuring compliance with current guidance; • Assisting other managers in carrying out investigations into security related incidents, liaising as required with the owners of CCG occupied sites, local police, Criminal Justice Unit and the Legal Protection Unit; where necessary preparing case files for submission to Court as part of the prosecution process; • Instigating regular campaigns to highlight the importance of security and the responsibilities of CCG employees; • Arrangements are in place for a senior Executive or appointed deputy to be summoned directly in the event of any serious incident

4.1.4	The **Office Manager** is responsible for ensuring that: • Sound arrangements are in place to retrieve IT equipment and ID badges, keys and access fobs etc. from staff leaving the organisation • All staff are issued with staff identification badges (ID badges)
4.1.5	All **Managers** are responsible for ensuring compliance with the CCG Security policy requirements in the areas for which they are responsible including: • So far as is reasonably practicable, the areas under their control are safe and secure; • Any security risks and procedures are explained in a local on-site induction; • Where necessary, local security procedures for their departments and other areas of responsibility are developed, based on the overall CCG Security policy; • Work areas under their control are operated in accordance with this policy and any associated procedures; • Lone working/personal safety risk assessments are completed where appropriate and appropriate procedures put in place • Ensuring all significant security risks are identified and measures are implemented to establish a safe and secure environment; • Ensuring all security incidents are appropriately reported and investigated; • Disciplinary procedures are initiated for staff who breach security arrangements; • Ensuring that any suspicion of fraud is reported to the local counter fraud service • Ensuring a response is made at the earliest opportunity to any request from employees for advice on security concerns; • Providing appropriate support to staff involved in any security related incident • Ensuring their staff understand and comply with this policy;
4.1.6	All CCG staff, including temporary and agency staff, are responsible for: • Familiarising themselves with the content of this policy and associated procedures; • Co-operating with management to achieve the aims of this policy, making themselves aware of any security requirements relating to their place of work or work practices and following prescribed working methods and security procedures at all times; • Reporting all security incidents, including violence and aggression, theft or loss through the CCG’s Incident Reporting procedure, ensuring that line management are fully aware of the circumstances; • Safeguard themselves, colleagues, visitors etc. so far as is reasonably practicable

- Reporting any shortcomings relating to security arrangements as soon as possible;
- Be responsible for their own personal property whilst at work and not to leave such items in plain view and open to potential theft;
- Ensuring the security of CCG equipment which they have responsibility or custody of;
- Ensuring that their ID badge is worn and visible at all times, while on CCG premises. The loss of an ID badge, and swipe cards or access fobs must be reported immediately;
- Challenging those without ID badges;
- Undertaking mandatory conflict resolution training;
- Remaining alert to the presence of unusual and unexplained packages which cannot be readily identified. Any such package should be reported immediately to line manager. Under no circumstances should the suspect package be handled.
- Be alert to the possibility that others might be attempting to deceive and if they suspect fraud or on-going fraudulent activity they must report the matter in line with the CCG's Anti-Fraud and Bribery policy;
- Staff working in areas controlled by another organisation should familiarise themselves with the security procedures for that organisation

Any deliberate or serious neglect of security measures could result in disciplinary action being taken.

4.2 Consultation and Communication with Stakeholders

The following stakeholders have been consulted in relation to this policy:

- HVCCG Exec Team
- Local Counter Fraud Specialist
- Office Managers
- Human Resources
- Risk Manager
- Pharmacy and Medicine's Management
- AD Localities
- Head of IM&T
- Health and Safety Adviser

5. CONTENT

5.1 Premises Security

The Head of Corporate Support in conjunction with the Office Manager will be responsible for developing any local procedures required to ensure the security of the premises where they are based – for example explicit arrangements for the items listed below (although this list is not exhaustive and other issues may be identified)

- Access to CCG premises including staff identification badges, key code, access fobs or swipe cards, unlocking and locking of premises
- Security of CCG, patient and staff property, providing appropriate secure storage facilities
- Relevant arrangements for contractors to access premises as required
- Security arrangements are reviewed following incidents and necessary changes to procedures are implemented;

CCG staff will comply with all local requirements for the securing of the premises that they are based within.

It is essential that access is tightly controlled throughout CCG premises. Where possible all access to CCG areas should be restricted. Visitors should not be allowed to wander through premises, but should be asked to either report to a reception area or be met by the person who has invited them.

Outside of normal working hours, CCG premises/facilities are to be secured. Local close down/lock-up procedures should be developed where this is deemed appropriate.

Some access doors have keypad entry systems and codes for these are only to be issued to staff working in the area. The codes should never be given to staff not working in that area or be given to patients or visitors and doors with coded entry systems should never be latched or wedged open. Staff should also not just release any electrical door entry without first checking the identity of the person seeking entry. Staff should also be aware of other persons "tailgating" them in order to gain access to a restricted area. If the person is not recognised as a member of staff, or authorised visitor, he/she should be asked to:

- Wait at the door or in a designated area
- Give details of the person with whom they have an appointment
- Await the arrival of an identified member of staff to escort him/her into the controlled access area
- At the end of the appointment/meeting, the visitor should be escorted out of the controlled access area

Where entry to a working area is by coded access, these codes must be changed on a regular basis. This is the responsibility of the Head of Corporate Support and / or Office Manager.

All members of staff should ensure that their work areas are secured at the end of the working day (where applicable) and that any departmental keys are held in a secure place at all times.

The loss of any key(s) must be reported to the line manager and the Office Manager or Designated Person. It is important to avoid delay so as to ensure premises can be secured.

5.2 Identification Badges

ID badges will be issued to all staff on commencement of employment by the Corporate Support team. Staff should wear their ID badge at all times whilst on CCG premises or when representing the CCG. Persons not wearing an ID badge on CCG premises should be challenged and asked to identify themselves.

Managers must ensure that any member of staff, permanent or temporary, hand their ID badge to the Office Manager or Designated Person on their last day of employment.

The loss of an ID badge must be reported immediately to the Office Manager or Designated Person. An incident form must be completed.

5.3 Personal Safety & Lone Working

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

The CCG Lone Worker policy must be complied with.

5.4 Security of Motor Vehicles

All motor vehicles used by employees, service users, visitors and other outside agencies must park in authorised parking area, where these have been provided. The security of motor vehicles owned by employees, service users and visitors is the responsibility of the owner of the vehicle. Providers of parking facilities will not accept liability for any theft or damage to motor vehicles or their contents when they are parked on their sites.

CCG property should not be left unattended in vehicles, particularly in view. However, where it is essential that confidential documents are transported in staff cars, they must be stored in the boot of the car and remain out of sight.

5.5 Verbal and Physical Assault or Anti-Social Behaviour

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. Violent or abusive behaviour will not be tolerated and decisive action will be taken by the CCG to protect staff, patients and visitors. Please refer to the Zero Tolerance Behavioural Policy.

5.6 Staff Property

Secure storage is provided on different sites in a variety of forms. Therefore, staff should be aware that the CCG cannot accept liability for loss or damage to staff property brought onto its premises. Staff are advised to take adequate precautions to ensure the safety of their possessions and not bring valuables to work.

Staff must report any loss or damage to their belongings and co-operate in any consequent enquiry. If private property has been stolen, then it is the owner's and not the CCG's responsibility to report the matter to the police. This should be after notifying a line manager and reporting the incident. Any crime reference number assigned should also be recorded on the incident log.

5.7 Visitors

All visitors and contractors should be asked to wait in the reception area until they can be escorted to their destination.

5.8 CCG Property/Assets

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

Where appropriate, CCG assets should be placed on the asset register. Managers should review the property held by their department on a regular basis to ensure that all items are securely managed.

5.9 Receipt of Goods

Any member of staff who signs for goods on behalf of the CCG is accountable for any discrepancies which may occur. All packages delivered must be identified and counted; the delivery note must not be signed unless they are sure that all items have been accounted for and any discrepancies noted. Any discrepancies outstanding must be recorded accurately along with the name and signature of the person delivering. Packages must not be left in a position where they create a safety/fire risk.

5.10 Counter Fraud

It is the responsibility of all employees to be alert to the possibility of fraud being perpetrated against the CCG. Fraud can best be defined as obtaining a financial benefit by deceit. Typical examples of fraud within the NHS are as follows:

<u>Contractors</u>

- Claiming for goods/services not provided

<u>Staff</u>

- Working elsewhere while on sick leave
- Claiming for work not done (timesheet fraud)
- Claiming for travel/other expenses not incurred

This list is not exhaustive but if any member of staff has any suspicion that fraud may be occurring against the CCG they should contact one of the following:

- Chief Finance Officer
- Local Counter Fraud Specialist (LCFS)

The LCFS can be contacted on: 01908 687800 / 07815 433361 **(**www.rsmuk.com)

5.11 IT Security

All staff are required to comply with relevant IM&T security policies.

5.12 Security of Information

It is essential that all CCG staff understand and follow the CCG's Information Governance policies (including Information Risk and Information Security policies)

5.13 Reporting and Investigations

All security incidents must be reported via the CCG's incident reporting procedures as quickly as possible so that an internal investigation may be initiated. When a criminal offence is committed or alleged to have been committed on CCG premises by any person, staff should inform their line manager and also contact the police without delay.

The Head of Corporate Support will liaise with the police, affected staff and the line manager regarding any investigation of offence. They will also conduct an internal investigation into any significant security breaches.

6. MONITORING COMPLIANCE

The Head of Corporate Support will be responsible for the review of this policy on a bi-annual basis, or following any significant security incidents or changes to current legislation.

An Incident Report should be completed in relation to any security incident in line with the HVCCG Incident Reporting Policy and Procedure, so that compliance can be easily monitored. The investigation of such incidents will be used as a tool to identify common cause, prevent reoccurrence and assess the effectiveness of policy controls and risk assessments.

7. EDUCATION AND TRAINING

Health and Safety training is a statutory requirement of legislation and therefore mandatory for all staff of the CCG. This can be carried out through e-learning. Additional Health & Safety training will be delivered for line managers through face to face sessions.

All staff are also mandated to complete Conflict Resolution training

8. REFERENCES

- Health and Safety at Work etc. Act 1974
- Management of Health and Safety at Work Regulations 1999
- Workplace Health, Safety and Welfare Regulations 1992
- Data Protection Act 1998

9. ASSOCIATED DOCUMENTATION

- HVCCG Whistleblowing policy
- HVCCG Standards of Business Conduct
- HVCCG Data Protection Confidentiality policy
- HVCCG Email and Internet policy
- HVCCG Forensic Readiness policy
- HVCCG Health and Safety policy and strategy
- HVCCG Incident Reporting policy & procedure
- HVCCG Information Governance policy
- HVCCG Information Risk policy
- HVCCG Information Lifecycle Management policy, procedure and strategy
- HVCCG Information Security policy
- HVCCG Information Sharing policy
- HVCCG Lone Workers policy
- HVCCG Risk Management strategy and policy
- HVCCG Safe Haven policy
- HVCCG Suspect Package and Substances plan
- HVCCG Zero Tolerance Behavioural policy
- HVCCG Telecommunications Policy

APPENDIX A – GLOSSARY

CCG	Clinical Commissioning Group
HVCCG	Herts Valleys CCG
ID	Identification
IM&T	Information Management and Technology
IT	Information Technology
NHS	National Health Service

Appendix B - HVCCG Equality Impact Screening Form

Name of policy / service	Security policy
What is it that is being proposed?	Herts Valleys Clinical Commissioning Group (HVCCG) is committed to promoting and improving security for all of its staff, patients and visitors. The CCG aims to provide and maintain a calm, pleasant and secure working environment where patients, visitors and staff are confident of their personal safety and security of their property, buildings and equipment are safeguarded.
What are the intended outcome(s) of the proposal	The purpose of this policy is to detail the responsibility of HVCCG for the effective management of security in relation to staff, patients, visitors and property. The CCG will do its utmost to safeguard against crime and against loss or damage to property or equipment. The main aim of the policy is to minimise potential losses by strict control, as well as preventing violent or aggressive behaviour towards staff, but it also aims to: • Protect the safety, security and welfare of staff, patient, contractors and the general public while on CCG property • Provide safe systems and safeguard against crime, fraud, loss, damage or theft of property, equipment or other CCG assets • Ensure the detection and reporting of suspected offenders committing offences against patients, staff or property within CCG premises • Educate staff in proactive and general security awareness
Explain why you think a full Equality Impact Assessment is not needed	This policy will not assist with any of the aims of the Equality Act or have any specific impact on the characteristic groups
On what evidence/information have you based your decision?	H&S Legislation
How will you monitor the impact of policy or service?	Please see section 5 of the policy "Monitoring Compliance"
How will you report your findings?	Via annual H&S audit

Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full Equality Impact Assessment is

not required.	
Assessors Name and Job title	Amanda Yeates
Date	October 2017