Durham Dales, Easington
and Sedgefield
Clinical Commissioning Group

Policy Type		Policy Name
Information Governance		**CO17 Security Policy**
Corporate	X	
Standard Operating Procedure		
Human Resources		

Status	Final
Committee approved by	Executive Committee
Date Approved	December 2017
Equality Impact Assessment undertaken	Completed
Distribution	All CCG staff
Planned Review Date	December 2019

Document History

Version	Date	Significant Changes
1	3/2013	Policy provided to Clinical Commissioning Group (CCG) as part of policy suite
2	08.05.2015	Re-styled to CCG policy standard Review of duties and responsibilities
3	10/2017	Reviewed in line with expiration date. Minimal amendments. No changes to legislation.

POLICY VALIDITY STATEMENT

This policy is due for review on the latest date shown above. After this date, policy and process documents may become invalid.

Policy users should ensure that they are consulting the currently valid version of the documentation.

Approval

Role	Name	Date
Approval (1)	Policy Group	2013
Approval (2)	Executive In Common	29/09/2017
Approval (3)	Executive Committee	December 2017

Review

This policy is due for review on the latest date shown above. After this date, policy and process documents may become invalid.

Table of Contents

1. Introduction

For the purposes of this policy NHS Durham Dales, Easington and Sedgefield Clinical Commissioning Group will be referred to as ‘the CCG’.

The Clinical Commissioning Group (CCG) aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients, their carers, public, staff, stakeholders and the use of public resources.

The CCG 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 the security of their property, buildings and equipment are safeguarded. Whilst the CCG recognises that it would 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.

1.1 Purpose and scope

The CCG is committed to promoting and improving the security of its premises/assets and the safety of staff and visitors to the CCG. The CCG will do its utmost to safeguard against crime and against loss or damage to property and equipment.

The CCG recognises and accepts its responsibility to provide a safe and healthy workplace and working environment for all employees and for those using its premises as required by the Health and Safety at Work etc. Act 1974.

Security is the responsibility of all staff in not only safeguarding their own wellbeing and personal property but also that of visitors and CCG property. The primary objectives of security management are:

- the prevention of violent or aggressive behaviour towards CCG staff, clients and visitors
- the protection of life from malicious criminal activity or other hazards
- the protection of premises and assets against fraud, theft and damage
- the detection and reporting of suspected offenders committing offences against patients, clients, staff, property or private property within CCG premises
- the education of all staff in proactive security and general security awareness

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 the business activity of the CCG.

Effective security management is linked to other policy areas, including but not limited to counter fraud, the management of violence and aggression, lone working.

2. Definitions

The following terms are used in this document:

- CCG – Clinical Commissioning Group
- NHS – National Health Service
- LSMS – Local Security Management Specialist

2.1 Designated Manager for Security

The Designated Manager for Security within the CCG is the Chief Finance Officer.

3. Security Policy

3.1 CCG Premises

Following risk assessment, managers are responsible for developing any local procedures required to ensure security of premises, for example explicit 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, key codes
- Lone working/ personal safety.
- Relevant arrangements for contractors to access premises as required.

3.2 Access Fobs

Where used, access fobs will be given to staff when joining the CCG. When staff leave CCG employment, all fobs should be returned to the Manager and deactivated.

Fobs should not be swapped or given to unauthorised personnel at any time. Lost or missing fobs should be reported immediately via the CCG incident reporting system.

3.3 Identification Badges

ID Badges are issued to all staff on commencement of employment. 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.

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.

3.4 Visitors / Contractors

All visitors/contractors are to be signed in and out of CCG premises and issued with a visitor pass, which must be displayed at all times whilst on CCG premises. For security reasons all visitors must be escorted to and from their destination within CCG buildings.

3.5 CCG Property/assets

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. Managers should review CCG property held by their department on a regular basis to ensure that all items are securely managed.

All managers and staff should take all reasonable steps to safeguard CCG property whilst it is in their care. It is an offence for members of staff to remove property belonging to 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.

3.6 Personal Property

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. Where storage has been provided for personal use, the individual to whom it is allocated will be responsible for ensuring it is locked.

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 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 reference number assigned should also be recorded on the incident log.

3.7 Security of Information - Confidentiality

All safeguards should be taken by staff that handle, receive and use confidential patient/personal information. It is essential that all staff taking up employment with the CCG understand and follow the CCG's confidentiality policy. The relevant CCG information governance policies should be referred to.

3.8 Security of Motor Vehicles

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.

3.9 Lease Cars

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.

3.10 Prevention of violence to staff

The CCG has a duty to provide a safe and secure environment for all employees and visitors as well as delivering care and treatment to patients 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.

Please refer to the relevant Violence, Aggression and Abuse Policy.

3.11 Bomb Threats and the law

The vast majority of bomb threats are hoaxes. Making such malicious calls is an offence contrary to S*ection 51 of the Criminal Law Act 1977* 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.

3.12 Reporting of Security Incidents

All staff have a responsibility to report all crimes and breaches of security and should refer to the relevant Incident Reporting and Management Policy.

Reporting falls into the following categories:

- **Assault or abuse of a staff member or visitor:** All incidents of assault or abuse must be reported through the CCG incident reporting system and should be reported as soon as practical after the incident. Staff incidents should be dealt with in line with NHS protocols regarding violence and aggression against staff. All physical assaults to staff should be reported by the Manager through the electronic risk management system. Visitors, patients and staff should always be asked if they wish the police to be involved.

- Where a **security incident or crime is in progress** it should be reported immediately to the Police and the senior manager on site. An incident must be logged onto the Incident reporting system as soon as possible after the incident and passed on as per CCG incident reporting policy.

- Where a **criminal incident is discovered after the fact** and the time of the offence is not known, the incident should be reported on the CCG system as soon as the crime is discovered and then passed on as per the incident reporting policy. The manager should ensure the police are involved, e.g. it may be necessary to obtain a police reference number for insurance purposes.

- Where a security incident involved the **theft of patient identifiable information** this must immediately be reported to the Caldicott Guardian; SIRO and Corporate Governance and Risk Officer. Any theft or loss of data storage e.g. computer, laptop, disks, CDs, tapes should all be reported in this way as well as via the incident reporting form. Also incidents where systems are suspected of being compromised should be reported to the Corporate Governance and Risk Officer. Staff should refer to relevant CCG policy.

- All cases of **suspected fraud or corruption** should be notified immediately to the Chief Finance Officer who will then give advice or arrange investigation of the incident, in accordance with the CCG Prime Financial Policies.

4. Duties and Responsibilities

Executive Committee	The Executive Committee is responsible for formal review and approval of organisational process documents.
Chief Officer	The Chief Officer, as Accountable Officer, has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements.
Management responsibility	All Executives, Managers and Supervisory Staff are responsible for the adherence and monitoring compliance with this policy. All managers in the CCG are responsible for security within their work area. Managers are required to assess security risks as part of the general assessments for their department/service, develop action plans and implement security measures. In particular they shall ensure: • Arrangements are in place to ensure the security of premises and assets and the safety of staff, patients and visitors taking all preventative measures to safeguard people and property (including occupied but not owned by the CCG). • That risk assessments are in place and where significant security risks exist local procedures are in place to minimise or reduce the impact. • That staff are aware of local and CCG security procedures and the results of risk assessments by effective training and communication. • Security arrangements are reviewed following incidents and ensure necessary changes in procedures are implemented. • Disciplinary procedures are initiated for staff who breach security arrangements. • That all criminal activities are reported to the Police and that all security incidents are reported and safeguards are completed. • That all staff are briefed with regard to their own personal security and local procedures, and where appropriate, are supported to attend security training. • That all staff are issued with staff identification badges (ID badges). • That work areas under their control are operated in accordance with this policy and any associated procedures. • That all breaches of security arrangements are investigated and reported immediately in accordance with laid down procedures.

	• That all staff on leaving the CCG return their ID badges, uniforms, keys and electronic passes. • That rules with regard to confidential paperwork are adhered to. • That advice is sought, as appropriate, from the LSMS and others where there is any doubt as to the standards that are to be applied in adhering to this policy. • That arrangements are in place to summon the Chief Officer or appointed deputy directly in the event of any serious incident occurring in the area under their control. • That official visitors/contractors are issued with the relevant visitor badge and this is monitored to ensure they are carried at all times when on CCG premises. • That all security incidents are recorded using the CCG's incident reporting system. • That any suspicion of fraud is reported to the local counter fraud service. • That a response is made at the earliest opportunity to any request from employees for advice on security concerns. • That appropriate support is given to staff involved in any security related incident.
Employees' responsibility	All employees have a duty to co-operate with the implementation of this policy. All CCG employees, whether permanent, temporary or working through an agency or other third party, are responsible for acquainting themselves with this policy, following the guidance contained in it and complying with all security measures in their department. In particular it should be ensured: • That they are vigilant and responsible in the workplace, bringing to the attention of their immediate manager, as appropriate, any suspicious activity they observe on CCG premises. • That they attend, or carry out any appropriate security training or education. • That they co-operate with managers to achieve the aims of the security policy, highlighting any identified risks. • That they complete incident report forms for all security related incidents. • That they wear their staff identification badges at all times. • That they report immediately to their departmental manager any loss of or malicious damage to their own patients.

All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.

5. Implementation

5.1 This policy will be available to all Staff for use in the circumstances described on the title page.

5.2 All managers are responsible for ensuring that relevant staff within the CCG have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

6. Training Implications

It has been determined that there are no specific training requirements associated with this policy/procedure.

7. Related Documents

7.1 Other related policy documents

- Violence, Aggression and Abuse Policy

7.2 Legislation and statutory requirements

- Health and Safety Executive (1974) *Health and Safety at Work etc Act 1974*. London HSE.

8. Monitoring, Review and Archiving

8.1 Monitoring

The Chief Officer will oversee, on behalf of the Governing Body, a method for monitoring the dissemination and implementation of this policy.

8.2 Review

8.2.1 The Governing Body will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

8.2.2 Staff who become aware of any change, including legislative changes, which may affect a policy should advise their line manager as soon as possible. The Governing Body will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

8.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the ‘version control’ table on the second page of this document.

8.3 Archiving

The Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with Records Management: NHS Code of Practice 2016.

9. Equality Impact Assessment

Introduction - Equality Impact Assessment

An Equality Impact Assessment (EIA) is a process of analysing a new or existing service, policy or process. The aim is to identify what is the (likely) effect of implementation for different groups within the community (including patients, public and staff).

We need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010
- Advance equality of opportunity between people who share a protected characteristic and those who do not
- Foster good relations between people who share a protected characteristic and those who do not

This is the law. In simple terms it means thinking about how some people might be excluded from what we are offering.

The way in which we organise things, or the assumptions we make, may mean that they cannot join in or if they do, it will not really work for them.

It's good practice to think of all reasons why people may be excluded, not just the ones covered by the law. Think about people who may be suffering from socio-economic deprivation or the challenges facing carers for example.

This will not only ensure legal compliance, but also help to ensure that services best support the healthcare needs of the local population.

Think of it as simply providing great customer service to everyone.

As a manager or someone who is involved in a service, policy, or process development, you are required to complete an Equality Impact Assessment using this toolkit.

Policy	A written statement of intent describing the broad approach or course of action the Trust is taking with a particular service or issue.
Service	A system or organisation that provides for a public need.
Process	Any of a group of related actions contributing to a larger action.

STEP 1 - EVIDENCE GATHERING

Name of person completing EIA:	**Lee Crowe**
Title of service/policy/process:	**Security Policy**

Existing: □ **New/proposed:** √ **Changed:** □

What are the intended outcomes of this policy/service/process? Include outline of objectives and aims

The aim of the policy is to ensure CCG considers Health and Safety along with its other business objectives and to ensure that the CCG follows the details stipulated within H&S Regulations.

Who will be affected by this policy/service /process? (please tick)

□ **Consultants** □ **Nurses** □ **Doctors** √ **Staff members** □ **Patients** □ **Public**
□ **Other**

If other please state:

What is your source of feedback/existing evidence? (please tick)

□ **National Reports** □ **Internal Audits**
□ **Patient Surveys** □ **Staff Surveys** □ **Complaints/Incidents**
□ **Focus Groups** □ **Stakeholder groups** □**Previous EIAs**
√ **Other**

If other please state:

- Health and Safety at Work Act
- Management of Health and Safety at Work Regulations
- Health and Safety Guidance HSG65
- Feedback from CCG staff and regular service line meetings between NECS/CCG.

Evidence	**What does it tell me? (about the existing service/policy/process? Is there anything suggest there may be challenges when designing something new?)**
National Reports	Not applicable
Patient Surveys	Policy has no impact on patients
Staff Surveys	Staff Survey's to include questions around H&S
Complaints and Incidents	This policy will ensure that systems are in place should there be any complaints received or Incidents regarding Health and Safety and that the CCG has robust systems in place around H&S Management
Results of consultations with different stakeholder groups – staff/local community groups	Only applicable to staff within CCG
Focus Groups	Only applicable to staff within CCG
Other evidence (please describe)	

STEP 2 - IMPACT ASSESSMENT

What impact will the new policy/system/process have on the following: (Please refer to the 'EIA Impact Questions to Ask' document for reference)
Age A person belonging to a particular age
The Policy will ensure that individuals of all ages are considered in relation to Health and Safety tasks.
Disability A person who has a physical or mental impairment, which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities
This Policy has a positive impact on any staff who have a physical/Mental impairment by considering their needs regarding H&S and the subsequent policies and procedures that underpin the Health and Safety Strategy.
Gender reassignment (including transgender) Medical term for what transgender people often call gender-confirmation surgery; surgery to bring the primary and secondary sex characteristics of a transgender person's body into alignment with his or her internal self perception.
As far as we are aware there are no members of staff to whom this applies. Should there be a member of staff undergoing gender reassignment/transgender the content within the policy does not include vocabulary that should cause offense.
Marriage and civil partnership Marriage is defined as a union of a man and a woman (or, in some jurisdictions, two people of the same sex) as partners in a relationship. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'. Civil partners must be treated the same as married couples on a wide range of legal matters
The Policy has no impact on marriage or civil partnership.
Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context.
The Policy can be accessed by all staff via intranet and policies/procedures are in place which underpin the policy's aims. The CCG also has New and Expectant mothers risk assessment documentation in place to ensure all risks are considered.
Race It refers to a group of people defined by their race, colour, and nationality, ethnic or national origins, including travelling communities.
There are no requirements for translation within the current staff group should the staff group characteristics change then versions and signage within the CCG in other languages can be obtained.
Religion or belief Religion is defined as a particular system of faith and worship but belief includes religious and philosophical beliefs including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition.
Risk assessments and training can be arranged for staff unavailable due to religious or other reasons.
Sex/Gender A man or a woman.
There is no discriminations between males and females within the policy
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes
Policy uses appropriate language no additional considerations are required.
Carers_A family member or paid helper who regularly looks after a child or a sick, elderly, or disabled person
Risk assessments and training can be arranged for those staff that have caring responsibilities and there is also online training which can be accessed whilst working within the CCG or at home.
Other identified groups such as deprived socio-economic groups, substance/alcohol abuse and sex workers
Other groups have been considered however as the Policy is for staff there are no additional impacts on health inequalities.

STEP 3 - ENGAGEMENT AND INVOLVEMENT

How have you engaged stakeholders in testing the policy or process proposals including the impact on protected characteristics?
Please list the stakeholders engaged:
Shared policy with Governance Colleagues within CCG. Regular service line meetings with CCG to discuss any H&S issues that arise.

STEP 4 - METHODS OF COMMUNICATION

What methods of communication do you plan to use to inform service users of the policy?

√ Verbal – stakeholder groups/meetings √ Verbal - Telephone
□ Written – Letter □ Written – Leaflets/guidance booklets
√ Email □ Internet □ Other

If other please state:

ACCESSIBLE INFORMATION STANDARD

The Accessible Information Standard directs and defines a specific, consistent approach to identifying, recording, flagging, sharing and meeting the information and communication support needs of service users.

Tick to confirm you have you considered an agreed process for:

□ Sending out correspondence in alternative formats.
□ Sending out correspondence in alternative languages.
□ Producing / obtaining information in alternative formats.
□ Arranging / booking professional communication support.
□ Booking / arranging longer appointments for patients / service users with communication needs.

If any of the above have not been considered, please state the reason:
As this is a staff policy needs have been considered internally and appropriate recommendations made.

STEP 5 **- SUMMARY OF POTENTIAL CHALLENGES**

Having considered the potential impact on the people accessing the service, policy or process please summarise the areas have been identified as needing action to avoid discrimination.

Potential Challenge	What problems/issues may this cause?
1 Workforce Characteristics	May require other formats such as braille, size of font etc. May also need to consider if face to face training takes place that accessibility of training venues is sufficient.

STEP 6- ACTION PLAN

Ref no.	Potential Challenge/ Negative Impact	Protected Group Impacted (Age, Race etc)	Action(s) required	Expected Outcome	Owner	Timescale/ Completion date
1	Staff unable to access Strategy	Age, Disability	Alternative formats provided if required, font size adjustment. As part of reasonable adjustments on appointment.	All staff can access the policy for reference	CCG/ NECS H&S	On receipt of individual request

Ref no.	Who have you consulted with for a solution? (users, other services, etc)	Person/ People to inform	How will you monitor and review whether the action is effective?
1	CCG Governance Colleagues	NECS Health and Safety Team	Regular Service Line Meetings

SIGN OFF

Completed by:	**Lee Crowe**
Date:	**December 2017**
Signed:	
Presented to: (appropriate committee)	**Executive Committee**
Publication date:	**December 2017**