Vale of York
Clinical Commissioning Group

# INFORMATION SECURITY POLICY
# November 2018

| | |
|---|---|
| **Authorship :** | eMBED Information Governance Manager |
| **Reviewing Committee :** | Governance Committee |
| **Date :** | 29 January 2019 |
| **Approval Body :** | Executive Committee (Minor Amendments) |
| **Approved Date :** | 30 March 2019 |
| **Review Date :** | November 2020 |
| **Equality Impact Assessment :** | Complete |
| **Sustainability Impact Assessment :** | Complete |
| **Related Policies :** | • IG01 Confidentiality Audit Policy<br>• IG02 Data Protection and Confidentiality Policy<br>• IG03 Internet, Email and Acceptable Use Policy<br>• IG04 Freedom of Information Act<br>• IG06 Information Risk Policy<br>• IG07 Corporate Records Management Standards and Procedures<br>• IG08 Mobile Working Policy<br>• IG09 Subject Access Request Policy<br>• IG10 Safe Haven Policy<br>• IG11 Information Governance Strategy<br>• IG12 Clinical Records Keeping Standards Policy |
| **Target Audience :** | All NHS Vale of York CCG employees and persons working for the CCG; all members attending CCG committees and members of the governing body. All contractors / volunteers providing services to the CCG. |
| **Policy Reference No. :** | IG05 |
| **Version Number :** | 4.0 |

## 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 and Date | Date on Internet |
|---|---|---|---|---|
| 0.2 | Chris Wallace | First draft for comments | | |
| 1.0 | Barry Jackson | Approved version | | |
| 1.1 | Pennie Furneaux | CCG Specific Amendments | Senior Management Team – Feb 2014 | |
| 2.0 | C. Wallace | Addition of Encryption and Cloud Computing Regulations | Audit Committee – Feb 2015 | |
| 2.1<br><br>(3.0 when approved) | IG Officer<br><br>Risk and Assurance Manager | To update for changes in organisational relationships (CSU to eMBED)<br>To update for the requirements of the General Data Protection Regulation<br>Insert references to policy and procedures<br>Change in Accountable Officer title<br>Reference to eMBED assurance report<br>Reference to TNA<br>Reference Supporting Forms and Procedures | Exec Committee 05 November 2017 | 15 January 2018 |
| 4.0 | IG Specialist | Updates to:<br>Data Protection Act 2018<br>General Data Protection Regulation<br>Data Security and Protection Toolkit<br>Data Protection Impact Assessments<br>Data Protection Officer | Governance Committee 20 January 2019<br><br>CCG Exec. 20 March 2019 | 29 March 2019 |

To request this document in a different language or in a different format, please contact NHS Vale of York Clinical Commissioning Group :

**valeofyork.contactus@nhs.net or 01904 555 870**

**CONTENTS**

## 1. INTRODUCTION

1.1. The Information Security Policy provides a framework for a comprehensive and consistent approach to the secure management of information throughout the organisation, ensure continuous business capability, and minimise the likelihood of occurrence and the impacts of any information security incidents.

1.2. Information and information systems are important assets to every organisation and it is essential to take all the necessary steps to ensure that they are comprehensively protected, available and accurate to support the operation and continued success of the Vale of York Clinical Commissioning Group (hereafter called The CCG) at all times.

1.3. The CCG's Information Security Policy is supported by policies and procedures implemented by the eMBED Health Consortium that are designed to :

- provide a common framework for eMBED Health Consortium and its client CCG's in which security threats to Information Systems can be identified and managed;
- introduce formal procedures to minimise the risk of unauthorised modification, destruction or disclosure of information; and
- align the organisation to the NHS Information Governance aims and expectations described in the Information Security Management: Code of Practice for NHS Organisations.

1.4. **NOTE** : these objectives can only be achieved if every staff member observes the highest standards of personal, ethical and professional conduct in relation to the handling and management of information.

## 2. REQUIREMENT FOR SECURITY POLICY

2.1. The CCG acknowledges that information is a valuable asset, therefore it is within its interest to ensure that the information it holds is suitably protected from any threat. By protecting its information the CCG is acting in the best interests of its employees and all third parties with whom information is shared whilst minimising key risks associated with information processing :

- legal action due to non-compliance with statutory and regulatory requirements
- loss of public confidence in the CCG
- contribution to clinical or corporate negligence

2.2. Key issues addressed by the Information Security Policy are :

- availability - information is delivered to the right person when it is needed
- confidentiality - data access is confined to those with specified authority to view the data;

- Integrity - all system assets are operating correctly according to specification and in the way the current user believes them to be operating

2.3. The CCG intends to achieve a standard of excellence in Information Governance by ensuring all information is dealt with legally, securely, efficiently and effectively in order to support the delivery of high quality patient care, service planning and operational management. For this to be achieved information processing must comply with legislation and best practice and the CCG will establish and implement policies and procedures to ensure appropriate standards are defined, implemented and maintained.

## 3. LEGAL COMPLIANCE

3.1. The CCG is bound by the provisions of a number of items of legislation affecting the stewardship and control of personal, patient and other information. The main relevant legislation is :

- Administrative Law;
- Common Law Duty of Confidentiality;
- The Data Protection Act 2018;
- General Data Protection Regulation
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- Access to Health Records Act, 1990 (where not superseded by the Data Protection Act, 1998);
- Computer Misuse Act, 1990;
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Crime and Disorder Act, 1998;
- The Human Rights Act 1998;
- Public Interest Disclosure Act 1998
- Audit and Internal Control Act 1987;
- Public Health (Code of Practice) 1984;
- National Health Service Act 2006;
- The Terrorism Act 2000;
- Road Traffic Act 1988
- Regulations under the Health and Safety at Work Act 1974;
- Regulations of Investigatory Powers Act 2000; and
- Freedom of Information 2000.

3.2. For further information regarding the organisation's Data Protection Obligations please refer to the Data Protection and Confidentiality Policy.

3.3. This policy describes the way in which information should be managed, in particular, the way in which personal or sensitive information should be protected.

3.4. Much of the legislation mentioned is available in electronic format, via the Internet (www.legislation.hmso.gov.uk). In addition, the CCG is bound by the Caldicott guidance on protection of patient information.

3.5. As part of, and in addition to, the above legislation the CCG is required to retain all records (health and administrative) for specified periods of time. For further information on this see the Records Management Policy.

## 4. ENGAGEMENT

4.1. This policy has been developed based on the knowledge and experience of the Information 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.

## 5. IMPACT ANALYSES

### Equality

5.1. An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

5.2. As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

### Sustainability

5.3. A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

## 6. SCOPE

6.1. This policy applies to :

- all users of the organisation's information
- all business functions within the organisation and all organisations providing a service on behalf of the organisation.
- information (manual and electronic), information systems, networks, physical environment and relevant people who support these functions.
- anyone having access to the organisation's IT network.

6.2. Any staff not employed by the CCG with a requirement to access information from the above organisation must have an honorary contract in place or sign a Non-Disclosure and Confidentiality Agreement.

6.3. Where systems are managed by third parties, it is the responsibility of the organisation to ensure that their information processing and systems are managed in line with the principles of this policy and associated legislation.

## 7. POLICY PURPOSE AND AIMS

7.1. It is the policy of the CCG to ensure compliance, in accordance with all the legislative obligations. The CCG also requires all employees, contractors and third parties to comply with this policy and supporting standards and procedures where appropriate.

## 8. INFORMATION SECURITY AWARENESS AND EDUCATION

8.1. It is the responsibility of all CCG employee's and third parties contractors providing services to or on behalf of the CCG to sustain excellent information security. To comply with this, the CCG requires all employees and contractors within scope to understand the importance of information security and be familiar with this document, and supporting documents where appropriate.

8.2. To facilitate this information governance training will be included in the staff induction process and as an annual requirement in order to ensure staff awareness is refreshed and updated as necessary.

### Contracts of Employment

8.3. Staff security requirements shall be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. In addition information security expectations of staff shall be included within appropriate job definitions.

## 9. EMAIL AND ELECTRONIC SYSTEMS

9.1. The CCG has clear standards relating to the use of e-mail, Internet and intranet and the deliberate or accidental misuse of electronic systems. The CCG has implemented policies that cover use of any systems used to store, retrieve, manipulate and communicate information (e.g. telephone, fax, e-mail, IT systems and the Internet. For further information see IG03 Internet, Email and Acceptable Use Policy). All employees and third parties are required to familiarise and adhere to them.

### Access to Information

9.2. Users will only be granted access to data and information that it is required as part of their job. Access is therefore granted on a 'need to know' basis.

9.3. Access authorisation should be regularly reviewed, particularly when staff roles and responsibilities change.

9.4. Staff must not access computer systems or data unless they have authority to do so. Access to files which are not in the course of the employee's duty will be considered a serious disciplinary offence. For example – accessing a friend or relative's, manual or electronic file. This may also be deemed a breach of the Computer Misuse Act 1990.

**Physical Security**

9.5. All staff are responsible for the physical security of assets, equipment and building used by the CCG. Appropriate physical security measures shall be put in place to secure information assets dependant on value and sensitivity to the organisation.

9.6. All staff are responsible for ensuring that buildings are left is a secure state when vacant.

9.7. Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

9.8. In addition each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

9.9. In order to minimise loss of, or damage to, assets equipment will be physically protected from threats and environmental hazards.

**Computer and Network Procedures**

9.10. Management of computers and networks shall be controlled by the eMBED Health Consortium on behalf of the CCG through standard documented procedures that have been authorised by the eMBED Health Consortium.

**Accreditation of Information Systems**

9.11. The eMBED Health Consortium oversee accreditation of all new information systems, applications and networks. A system level security policy should be documented and approved for all core systems and a Network security policy will be maintained by eMBED Health Consortium.

9.12. System Specific Security Policies (SSSPs) will be developed for systems under CCG control in order to allow granularity in the security management considerations and requirements of each. This may result in specific responsibilities being assigned and obligations communicated directly to those who use the system.

9.13. eMBED Health Consortium will advise and support the CCG during the procurement and implementation of all new information systems to ensure consideration of appropriate security management arrangements and development of relevant System Level Security Policies, (SLSPs). SLSPs

should detail appropriate security controls and business continuity arrangements for each system.

9.14. The Information Governance Specialist should review all SLSPs prior to implementation.

**Intellectual Property Rights**

9.15. eMBED Health Consortium shall ensure that all information products and assets belonging to the CCG or assets owned by the eMBED Health Consortium and used to provide services on behalf of the CCG are properly licensed and approved by eMBED's Head of IMT.

9.16. CCG Users shall not install software on the organisation's property without permission from eMBED Health Consortium Head of IMT. Users breaching this requirement may be subject to disciplinary action.

**System Change Control**

9.17. Changes to information systems, applications or networks under the control of eMBED Health Consortium shall be reviewed and approved by the eMBED Head of IM&T or authorised officer.

**New User Procedures**

9.18. All staff, agency staff, trainees, apprentices, staff on secondment and third party contractors who need access to CCG network resources and information systems will be required to sign a Non-Disclosure and Confidentiality Agreement as a pre-requirement to access.

9.19. The CCG Business Support Manager is responsible for notifying eMBED Health Consortium of new user account requirements. Access to networks and systems will only be provided on completion of a New Account form. All forms should be submitted to eMBED Health Consortium Service Desk on a timely basis to allow set up of new accounts. Line managers are responsible for timely notification of any leavers or changes in staff role that impact access permissions to enable termination/variation of access privileges.

**Remote Access to CCG Servers and Information Systems**

9.20. In order to support mobile working the CCG operates a secure link to a Remote Access Server.

**Home Computers**

9.21. The Organisation recognises that staff may use their own computers or portable devices and that this is of benefit both to the organisation and to the member of staff. However, due to legal constraints and risk to the organisation certain policy guidelines must apply.

9.22. Person identifiable and/or confidential data must not be processed on non-CCG provided equipment. Person identifiable information must only be accessed via organisation issued equipment and through the use of a VPN or equivalent remote access server (RAS) token if working remotely.

9.23. No person identifiable information or other corporate information of a sensitive or confidential nature must be stored on a computer not owned or assigned to the organisation (Data Protection Act 2018).

9.24. Staff using their own computers for business-related purposes do so at their own risk and the organisation does not accept any responsibility for any software or hardware failure.

9.25. Computer media that has been used in a home computer must not be used in on organisation equipment without being scanned for viruses first.

For further guidance see the CCG's Mobile Working Policy.

**User Media**

9.26. The eMBED Health Consortium uses port control software to control the use of removable media. Access to USB mass storage devices and other portable devices will be restricted to approved users only.

9.27. All removable media received from external sources or that has been used on computers systems not assigned to the CCG will require scanning using anti-virus software before its use.

9.28. All removable media that holds CCG Personal confidential data must be encrypted. Failure to do this may result in disciplinary action.

**Encryption**

9.29. Following Department of Health requirements all mobile computing equipment will be encrypted to ensure data security. This ensures if the device is lost or stolen only pre-approved user will be able to access and content stored locally.

9.30. To ensure data security on other media types, along with port controls described above, only encrypted removable media will be sanctioned for use. Any USB removable media will be required to meet UK eGovernment Interoperability Framework standards for encryption.

9.31. Where data of a personal confidential nature is to be written to CD or DVD media then this will also require encryption. The eMBED Health Consortium will ensure software is made available to use that allows the encryption of data before it is copied to the disk.

**Online or Cloud Storage**

9.32. The use of online or cloud storage is prohibited and staff should not use any service that has not been provided through the eMBED Health Consortium IMT department. Some device manufactories provide cloud based storage options with their products. If you setup your work supplied device or use your own device you will be responsible for ensuring that any data on the device does not synchronise with the cloud.

**Classification of Sensitive Information**

9.33. The CCG will implement information classifications controls, based upon the results of formal risk assessment and guidance contained within the Data Protection and Security Toolkit to secure their NHS information assets. The status of information classification will be listed in the CCG's information asset register. Information Asset Owners should check and verify the classification assigned to the information assets under their control. Further details of the classifications controls can be found in the CCG's Corporate Records Management Policy.

## 10. PREVENTION OF MISUSE

10.1. Any use of IM&T facilities for non-business or unauthorised uses without management approval will be regarded as inappropriate usage.

10.2. The Computer Misuse Act 1990 introduced three criminal offences. Staff must remember that the following offences can be enforced in a court of law :

- unauthorised access
- unauthorised access with intent to commit further serious offence
- unauthorised modification of computer material

## 11. FORENSIC READINESS

11.1. Forensic readiness provides the organisation with the capability to use digital evidence in a forensic investigation.

11.2. If digital evidence is to be recovered and analysed as part of an investigation then it should be done in a manner that is systematic, standardised and legal in order to ensure the admissibility of that evidence in case it has to be produced in a legal case or disciplinary hearing to :

- protect the organisation, its staff and its patients through the availability of reliable digital evidence gathered from its systems and processes.
- Allow consistent, rapid investigation of major events or incidents with minimum disruption to the organisational business.
- enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required.
- demonstrate due diligence and good governance of the organisation's information assets.

11.3. Digital evidence may feature in a wide range of investigations or disputes involving NHS organisations including (but not confined to) :

- confidentiality breaches, complaints requiring investigation and privacy issues; identity theft, invasions of privacy, compliance with the Data Protection Act and other relevant legislation;

- security incidents; unauthorised access to, tampering with or use of IT systems, electronic attack, including denial of service and malicious software ('malware') attacks (viruses, worms, Trojan);
- criminal activities such as fraud, deception, money laundering, threats, blackmail, extortion, harassment, stalking;
- commercial disputes; intellectual property rights; and
- disciplinary issues; accidents, negligence, malpractice, abuse of Acceptable Use Policy, or grievance procedures.

11.4. eMBED will provide support for the Senior Information Risk Owner (SIRO) in coordinating any forensic investigation for the organisation.

11.5. eMBED Information Asset Owners (IAOs) are responsible for ensuring that forensic readiness planning is adequately considered and documented for all information assets where they have been assigned 'ownership.'

**Protection from Malicious Software**

11.6. The eMBED Health Consortium will use software countermeasures and management procedures to protect against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users will not install software on the eMBED Health Consortium s hosted infrastructure without formal permission from the eMBED Health Consortium IMT Services. Users breaching this requirement may be subject to disciplinary action.

## 12. BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS

12.1. All designated sensitive and critical information and systems must have a disaster recovery plan which includes back up of electronic systems. This is required to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

12.2. eMBED Health Consortium will ensure that appropriate backup arrangements are in place for all systems under their management and control; stored in approved locations and that restore of back-ups should be tested regularly.

12.3. CCG Information Asset Owners and Information Asset Administrators for information assets under the local control of the CCG should ensure that appropriate business continuity and disaster recovery plans for their information assets. These plans should ensure :

- integrity and availability of data,
- backups of systems and information,
- timely input of data and its validation,
- control of internal processing

12.4. Vale of York Clinical Commissioning Group commission IM&T infrastructure and support services from the eMBED Health Consortium. eMBED Health Consortium are responsible for the network infrastructure and the associated

business continuity plans including daily back-ups of the network drives. eMBED Health Consortium shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

**Reporting**

12.5. eMBED Health Consortium will keep the CCG informed of the information security status of the organisation by means of regular reports and presentations as required.

## 13. POLICY AUDIT

13.1. This policy will be subject to regular independent audit and annual assessment in line with the completion of the Data Security and Protection Toolkit by internal and external audit.

## 14. INFORMATION SECURITY EVENTS AND WEAKNESSES

14.1. All information security events and suspected weaknesses must be reported via the CCGs Incident Management process to the CCG's Risk and Assurance Manager and eMBED's assigned Information Governance Specialist.

14.2. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

## 15. INCIDENT REPORTING

15.1. It is the responsibility of all staff to ensure that the potential for security breaches does not occur as a result of their actions. All staff must report instances of security breaches, near misses or weaknesses through the CCG's incident reporting procedures.

15.2. Both the CCG organisational policy and the Data Security and Protection Toolkit (DSPT) procedures for the management of Serious Incidents must be followed.

15.3. Information security or potential data loss incidents will be reported to the SIRO, through the Line Manager and Information Governance Lead and any incidents relating to person-identifiable data will also be reported to the Caldicott Guardian.

15.4. All suspected / actual security breaches will be investigated by the organisation and reported to the appropriate bodies.

15.5. The organisation will be responsible for collating and reporting the number of breaches and ensuring actions have been taken.

15.6. The eMBED Health Consortium IM&T in conjunction with CCG staff carry out audits on security and confidentiality compliance of the IT network across organisations.

15.7. It is a condition of employment with the CCG that compliance should be maintained where appropriate with the information security management policy, and supporting policies and procedures.

15.8. Any breach to this policy will be treated as security incidents, and reported in accordance with the CCGs incident reporting procedure. Failure to comply with this policy, or supporting procedures, could result in disciplinary action.

## 16. RISK MANAGEMENT

16.1. Information risk is part of overall corporate risk. Appropriate security measures must be viewed as necessary for protection against a risk of an event occurring or to reduce the impact of such an event. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address :

- the threat of something damaging the confidentiality, integrity or availability of information held on systems or manual records.
- the impact that such a threat would have if it occurred.
- the chance that such a threat would occur.

16.2. All staff must consider the risks associated with the computers and the information that is held on them as well as information that is held in manual records.

16.3. For further information regarding information risk management refer to the CCG Information Risk Management Policy.

### Information Risk Assessment

16.4. All critical information assets should be subject to periodic risk assessments and independent assurance by internal/external audit services. Risk assessments must consider arrangements in place to appropriately protect information. All risks identified must be reported in line with the corporate Risk Management Strategy and added to the appropriate risk register.

16.5. Once identified, information security risks shall be managed on a formal basis. Risks recorded within the Information Asset Register shall be either accepted or appropriate action plans put in place to effectively manage identified risks.

16.6. The Information Asset Register and all associated action plans shall be reviewed quarterly by Information Asset Owners. Any implemented information security arrangements shall also be regularly reviewed and will be included in the eMBED Health Consortium's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have

arisen since the last review was completed. Risk assessments completed by IAOs or the IG Team must be forwarded to the CCG SIRO for approval and acceptance.

## 17. PROCUREMENT, CONTRACTING, PROJECTS AND PROCESSES – MANAGING RISKS AT IMPLEMENTATION

17.1. When planning for, and during procurement of, new systems, it is the responsibility of the Project Manager to ensure that appropriate system security features are included within the system. eMBED Health Consortium should be consulted and their advice sought.

17.2. Any procurement or development of services, projects and process where systems which process person-identifiable information must be risk assessed for any Information Governance Security issues and a Data Protection Impact Assessment performed.

17.3. eMBED Health Consortium will manage all software applications, upgrades and amendments. These will be developed in a controlled manner, documented and thoroughly tested before implementation.

17.4. Proof of ownership of software licences will be maintained and master copies held in a secure environment in the event of necessary re-install.

## 18. ROLES / RESPONSIBILITIES / DUTIES

### Information Security Responsibilities

18.1. Robust information security management and assurance arrangements are needed to ensure that the organisation complies with information security obligations and keeps the Governing Body informed of changes and performance issues which need to be considered and addressed. Information security responsibilities apply to all staff and should be identified and documented in employment contracts and job descriptions.

### Accountable Officer

18.2. The Accountable Officer has overall responsibility for this policy. The Accountable Officer has responsibility for ensuring that appropriate management and accountability arrangements are in place to effectively discharge information security responsibilities

### Senior Information Risk Owner

18.3. The SIRO is responsible for the identification, scoping definition and implementation of an information security risk programme the security and confidentiality of information within the organisation and has lead responsibility to ensure organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist. The SIRO for the CCG is supported by the eMBED Health Consortium Information Governance team.

**Caldicott Guardian**

18.4. The Caldicott Guardian is a senior person with delegated responsibility for protecting the confidentiality of a patient and service-user information and enabling appropriate information-sharing.

18.5. **Data Protection Officer**

The Data Protection Officer (DPO) is a senior person with delegated responsibility for monitoring compliance with the GDPR and other data protection laws, and with the CCG's data protection polices, including managing internal data protection activities.

**Information Assets Owners (IAO)**

18.6. Information Asset Owners are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets including electronic systems that they are responsible for.

**Information Asset Administrators (IAA)**

18.7. Information Asset Administrators may be appointed to support Information Asset Owners, to ensure that information governance policies and procedures are followed, assist in identifying actual or potential security incidents, and ensure that information asset registers are accurate and up to date.

**Senior Managers**

18.8. Senior Managers are responsible for implementing and maintaining the policy in their area of management, including ensuring that procedures are in place and staff adequately trained.

**Staff**

18.9. All staff will comply with information security policies and procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

18.10. Each member of staff will be responsible for the operational security of the information systems they use.

18.11. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

18.12. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

## 19. eMBED HEALTH CONSORTIUM

19.1. eMBED Health Consortium manages IM&T and Information Governance Services on behalf of the CCG. eMBED Health Consortium will ensure that

the security of information systems is reviewed on a regular basis. The eMBED Health Consortium will ensure that appropriate infrastructure and information security arrangements are in place in line with NHS Information Governance standards which will be subject to internal audit. The eMBED Health Consortium is responsible for advising, supporting and reporting the outcomes of information Security reviews to the CCG in line with agreed SLA arrangements.

## 20. IMPLEMENTATION

20.1. The policy will be disseminated by being made available on the intranet and highlighted to staff through newsletters, team briefings and by managers.

20.2. 'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

## 21. TRAINING AND AWARENESS

21.1. Staff will be made aware of the policy via the internet and will undertake appropriate training as identified in the CCG's Training Needs Analysis.

## 22. MONITORING AND AUDIT

### Monitoring System Access and Use

22.1. An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

22.2. CCG Staff should be aware that the CSU has in place routines to regularly audit compliance with this and other policies. In addition the CCG reserves the right monitor activity where it suspects that there has been a breach of policy.

22.3. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons :

- establishing the existence of facts
- investigating or detecting unauthorised use of the system
- preventing or detecting crime
- ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- in the interests of national security
- ascertaining compliance with regulatory or self-regulatory practices or procedures
- ensuring the effective operation of the system

- any monitoring will be undertaken in accordance with the above act and the Human Rights Act

## 23. POLICY REVIEW

23.1 This policy will be reviewed in two years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

## 24. REFERENCES

- The Data Protection Act (2018)
- The General Data Protection Regulation
- The Data Protection (Processing of Sensitive Personal Data) Order (2000).
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health & Social Care Act (2012)

## 25. SUPPORTING DOCUMENTS AND PROCEDURES

The following documents are in support of the Information Security Policy :

- Incident Reporting Procedure
- System Level Security Policy Template
- Privacy Impact Assessment Guidance
- Information Asset Register

## 26. CONTACT DETAILS

**The Governance Team**
VOYCCG.Governance@nhs.net
NHS Vale of York Clinical Commissioning Group
West Offices
Station Rise
York, YO1 6GA

## 27. APPENDIX 1: EQUALITY IMPACT ASSESSMENT

| | |
|---|---|
| **1.** | **Title of policy/ programme/ service being analysed** |
| | **Information Security Policy** |
| **2.** | **Please state the aims and objectives of this work.** |
| | This policy provides guidance on the CCG's expectations for the use of the internet and email. |
| **3.** | **Who is likely to be affected? (e.g. staff, patients, service users)** |
| | Staff need to comply with the principles and practices outlined in this policy. |
| **4.** | **What sources of equality information have you used to inform your piece of work?** |
| | NHS England guidance |
| **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** |
| | The analysis of equalities is embedded within the terms of reference of the CCG's committees and project management framework. |
| **6.** | **Who have you involved in the development of this piece of work?** |
| | **Internal involvement :** SIRO/Caldicott Guardian, review by Steering Group membership<br>**Stakeholder involvement** : Consultation with eMBED Healthcare Consortium<br>**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 principles 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?**<br>**Do you have any gaps in information?**<br>**Include any supporting evidence e.g. research, data or feedback from engagement activities**<br><br>**(Refer to** Error! Reference source not found. if your piece of work relates to commissioning activity to gather the evidence uring all stages of the commissioning cycle) |

| | |
|---|---|
| **Disability**<br>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**<br>Men and Women | Consider gender preference in key worker, single sex accommodation etc. |
| N/A | |
| **Race or nationality**<br>People of different ethnic backgrounds, including Roma Gypsies and Travellers | Consider cultural traditions, food requirements, communication styles, language needs etc. |
| N/A | |
| **Age**<br>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**<br>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**<br>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**<br>Includes religions, beliefs or no religion or belief | Consider holiday scheduling, appointment timing, dietary considerations, prayer space etc. |
| N/A | |
| **Marriage and Civil Partnership**<br>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**<br>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**<br>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**<br>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**<br>Please outline what mitigating actions have been considered to eliminate any adverse impact?<br>No adverse equality impact has been identified.<br>Please state if there are any opportunities to advance equality of opportunity and/ foster good relationships between different groups of people?<br>An Equality Action Plan template is appended to assist in meeting the requirements of the general duty |

| **Sign off** |
|---|
| Name and signature of person / team who carried out this analysis<br>Business Support Manager |
| Date analysis completed<br>13 September 2017 |
| Name and signature of responsible Director<br>Rachel Potts Executive Director of Governance and Planning |
| Date analysis was approved by responsible Director |

## 28. 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 | Email, Internet and Acceptable Use Policy |
| What is the main purpose of the document | This policy provides guidance on the CCG's expectations for the use of the internet and email. |
| Date completed | 13 September 2017 |
| Completed by | Business Support Manager |

| Domain | Objectives | Impact of activity<br>Negative = -1<br>Neutral = 0<br>Positive = 1<br>Unknown = ?<br>Not applicable = N/A | Brief description of impact | If negative, how can it be mitigated?<br>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 | | |

| Domain | Objectives | Impact of activity<br>Negative = -1<br>Neutral = 0<br>Positive = 1<br>Unknown = ?<br>Not applicable = N/A | Brief description of impact | If negative, how can it be mitigated?<br>If positive, how can it be enhanced? |
|---|---|---|---|---|
| | 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 | | |
| | 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 | 0 | | |
| Facilities Management | Will it reduce the amount of waste produced or increase the amount of waste recycled?<br>Will it reduce water consumption? | 0 | | |

| Domain | Objectives | Impact of activity<br>Negative = -1<br>Neutral = 0<br>Positive = 1<br>Unknown = ?<br>Not applicable = N/A | Brief description of impact | If negative, how can it be mitigated?<br>If positive, how can it be enhanced? |
|---|---|---|---|---|
| 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)? | 0 | | |
| | 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 | | |
| | 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 | | |

| Domain | Objectives | Impact of activity<br>Negative = -1<br>Neutral = 0<br>Positive = 1<br>Unknown = ?<br>Not applicable = N/A | Brief description of impact | If negative, how can it be mitigated?<br>If positive, how can it be enhanced? |
|---|---|---|---|---|
| | 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 | | |