NHS
Vale of York
Clinical Commissioning Group

INFORMATION GOVERNANCE STRATEGY
November 2018

Authorship :	Barry Jackson, Information Security & RA Team Manager, eMBED Pennie Furneaux Risk & Assurance Manager
Reviewing Committee :	Governance Committee
Date :	November 2018
Approval Body :	Executive Committee
Approved Date :	05 December 2018
Review Date :	November 2020
Equality Impact Assessment :	Yes
Sustainability Impact Assessment :	Yes
Related Policies :	IG01 Confidentiality Audit Policy IG02 Data Protection and Confidentiality Policy IG03 Internet, Email and Acceptable Use Policy IG04 Freedom of Information Act IG05 Information Security Policy IG06 Information Risk Policy IG07 Corporate Records Management Standards and Procedures IG08 Mobile Working Policy IG09 Subject Access Request Policy IG10 Safe Haven Policy 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 providing services to the CCG.
Policy Reference No. :	IG11
Version Number :	4.0

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

POLICY AMENDMENTS

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

New Version Number	Issued by	Nature of Amendment	Approved by and Date	Date on Internet
1.3	SMT	18/12/13: Initial draft 19/12/13: Update to reporting structure	SMT Dec 2013	Jan 2013
2.0	Information Governance Officer	23/02/2016: Update to include handling confidential information and HSCIC latest guidance	23/03/2016	10/03/2016
2.1	Risk and Assurance Manager	Inclusion of Strategy Statement Update to Job Titles, committees Replace IG Assurance Statement with HSCN Connection agreement requirement Remove reference to N3 due to termination of N3 at 31/3/17 Insertion of link to Information Governance legislation (s. 6.2) Reference to NHS Constitution and CCG Scheme of Reservation and Delegation (s. 6.6 & 6.7) Review of policy for inclusion of CCG patient services Changes in Steering Group arrangements Updates to reflect General Data Protection Requirement Insertion of eMBED IG Services	Circulated to EPBCIGSG October 2017	
2.2	IG Officer	Removal of training needs analysis		
3.0		Changes confirmed	CCG Exec. 15 November 2017 Audit Committee 30 November	08 December 2017
4.0	IG Specialist	Removal of IG Toolkit – replaced with Data Security & Protection toolkit Terms of reference added. Training Needs Analysis	Exec 05 December 2018	24 December 2018

CONTENTS

1. INTRODUCTION 4
2. STRATEGY STATEMENT 5
3. IMPACT ANALYSES 5
4. SCOPE 5
5. STRATEGY PURPOSE / AIMS AND FAILURE TO COMPLY 5
6. PRINCIPAL LEGISLATION AND COMPLIANCE WITH STANDARDS 6
7. ROLES / RESPONSIBILITIES / DUTIES 7
8. INFORMATION SECURITY 10
9. HANDLING CONFIDENTIAL INFORMATION 10
10. RISK MANAGEMENT 11
11. INCIDENT MANAGEMENT 12
12. INFORMATION GOVERNANCE FRAMEWORK STRUCTURE 12
13. POLICY IMPLEMENTATION 12
14. TRAINING AND AWARENESS 13
15. AUDIT 14
16. POLICY REVIEW 15
17. ASSOCIATED POLICIES 16
18. CONTACT DETAILS 16
19. APPENDIX A : LINKS TO THE CCG GOVERNANCE RISK ASSESSMENT AND ACTION PLAN 17
20. APPENDIX B : TERMS OF REFERENCE 19
21. APPENDIX C: DATA PROTECTION PRINCIPLES 23
22. APPENDIX D: THE CALDICOTT PRINCIPLES 24
23. APPENDIX E: TRAINING NEEDS ANALYSIS 25
24. APPENDIX F: EQUALITY IMPACT ANALYSIS FORM 28
26. APPENDIX G: SUSTAINABILITY IMPACT ASSESSMENT 32

1. INTRODUCTION

General

1.1. Information Governance provides a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information, allowing :

- Implementation of central advice and guidance;
- Compliance with the law;
- Year on year improvement plans.

1.2. Information Governance is about setting a high standard for the handling of information and giving organisations the tools to achieve that standard. The ultimate aim is to demonstrate that an organisation can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance standards and to be consistent in the way they handle personal and corporate information.

1.3. The Data Security and Protection Toolkit (DSPT) is an online tool that enables NHS organisations to measure their performance against the information governance requirements and compliance against the toolkit and provides assurance that organisations have established best practice in respect of handling information, and are actively promoting a culture of awareness and improvement to comply with legislation and other mandatory standards.

National Context

1.4. The NHS Information Governance Assurance Programme (IGAP) was established in February 2008 in response to the Cabinet Office Data Handling review. The Prime Minister commissioned the review following the high-profile data losses in 2007. IGAP developed a number of principles to support and strengthen the existing Information Governance agenda.

1.5. The principles are :

- All NHS organisations should be part of the same Information Governance Assurance Framework
- Information Governance should be as much as possible integrated into the broader governance of an organisation, and regarded as being as important as financial and clinical governance in organisational culture
- The Framework will provide assurance to the several audiences interested in the safe custody and use of sensitive personal information in healthcare. This involves greater transparency in organisational business processes around Information Governance
- IGAF to be built on the strong foundations of the existing Information Governance agenda and is the mechanism by which :
    - IG policies and standards are set
    - Regulators can check an organisation’s compliance
    - An organisation can be performance managed

2. STRATEGY STATEMENT

2.1. This strategy outlines the CCG plan to comply with Information Governance responsibilities and duties. The strategy has been developed from the standards outlined in the NHS Data Security and Protection Toolkit which are based on ISO27001 principles and practice.

3. IMPACT ANALYSES

Equality

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

Sustainability

3.2. A Sustainability Impact Assessment has been undertaken. No positive or negative impacts were identified against the twelve sustainability themes. The results of the assessment are attached.

4. SCOPE

4.1. The organisation requires all employees to comply with the Policies, Procedures and Guidelines which are in place to implement this framework with the aim of ensuring that the Vale of York Clinical Commissioning Group maintains high quality Information Governance standards.

4.2. The Information Governance Strategy is linked to the organisation’s Risk and Assurance Framework, and the need to complete the Data Security and Protection Toolkit to a satisfactory standard.

5. STRATEGY PURPOSE / AIMS AND FAILURE TO COMPLY

5.1. The purpose of this strategy is to describe the management arrangements that will deliver Information Governance, (IG) assurance within the NHS Vale of York Clinical Commissioning Group, (the CCG) and to set out overall principles that will promote a culture of best practice around the processing of information and use of information systems. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner.

Data Security and Protection Toolkit (DSPT)

5.2. Completion of the DSPT is mandatory for all organisations that commission or provide health and social care services. All organisations are required to complete the toolkit to a satisfactory standard in order to demonstrate a satisfactory level of information governance practices. Annual plans will be developed year on year from the DSPT to achieve a satisfactory level in all requirements. As the DSPT is a publically available assessment the scores of partner organisations will be used to assess their suitability to share information and to conduct business with.

The Annual Governance Statement

5.3. The Information Governance Statement of Compliance, (IGSoC) is the process by which organisations enter into agreement with NHS Digital for access to its services. The terms and conditions of access are set out in the IG Assurance Statement. It is essential that every organisation meets the obligations of the DSP Toolkit, and complies with the IG Assurance Statement to the required standards to safeguard NHS Digital services and information for all.

HSCN Connection Agreement

5.4. From April 2017 the Connection Agreement replaces the N3 Information Governance Statement of Compliance (IGSoC) which separates the arrangements for being able to use HSCN from those relating to accessing data or systems available on HSCN.

5.5. Every organisation that wishes to use HSCN, i.e. send or receive data across HSCN; must complete a Connection Agreement. The HSCN Connection Agreement is organisation-centric. Each organisation is required to sign and submit only one Connection Agreement no matter how many locations or HSCN connections they have or use.

5.6. All organisations that handle patient data are required to meet the requirements of the DSPT and to provide evidence for this through an annual submission. This means that a current DSPT is required to access NHS Digital's National Applications such as NHS e-Referral Service (ERS), Personal Demographics Service (PDS) and Secondary Uses Service (SUS).

eMBED Health Consortium

5.7. The Vale of York Clinical Commissioning Group has a contract in place with eMBED Healthcare Consortium to support the CCG in developing its IG Framework and implementing appropriate policies and practices to meet its statutory IG Requirements.

6. PRINCIPAL LEGISLATION AND COMPLIANCE WITH STANDARDS

Statutory Instrument(s)

Data Protection Legislation

6.1. Data Protection Legislation is the most fundamental piece of legislation that underpins Information Governance. NHS Vale of York Clinical Commissioning Group is registered with the Information Commissioners Office and will fully comply with all legal requirements of this Legislation. A process will be adopted to ensure that a review of all of new systems is carried out and where requirements such as the need for Data Protection Impact Assessments are highlighted these will be completed.

The Data Protection Principles are detailed at Appendix C.

6.2. Other Legislation:

- Human Rights Act 1998 (Specifically Article 8)
- Access to Health Records Act 1990

- Section 251 of the NHS Act 2006
- General Data Protection Regulation

NHS / Department of Health Guidance

Caldicott Principles and Requirements

6.2. The original Caldicott Report on the Review of Patient-Identifiable Information 1997 and the subsequent Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013. These two reports have identified specific principles that are considered essential practice for the appropriate sharing and security of Patient Information.

6.3. Government response to the Report of the Caldicott 2 Report acknowledges the findings of this and promotes that everyone should understand how to protect and, where appropriate, share information about the people they care for, either directly or indirectly. The Caldicott Principles are detailed at Annex C.

6.4. This is further supported by the Everyone Counts: Planning for Patients 2014/15 to 2018/19 by detailing practical applications for information sharing.

The NHS Constitution

6.5. The NHS Constitution includes a number of personal rights in relation to respect, consent and confidentiality. These inform Information Governance requirements.

CCG Scheme of Reservation and Delegation

6.6. Approval of the arrangements for ensuring appropriate and safekeeping and confidentiality of records and for the storage, management and transfer of information and data is reserved to the Governing Body.

7. ROLES / RESPONSIBILITIES / DUTIES

NHS Vale of York Clinical Commissioning Group Governing Body

7.1. The Clinical Commissioning Group Governing Body is responsible for ensuring appropriate systems and policies are in place in respect of Information Governance, taking into account the statutory and NHS mandatory requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to deliver the Information Governance Agenda.

Accountable Officer

7.2. The CCG’s Accountable Officer has overall responsibility for Information Governance. The Accountable Officer is required to sign off the Information Governance Statement of Compliance, (IGSoC) before the final annual submission of the Data Security and Protection Toolkit.

Data Protection Officer

7.3. The General Data Protection Regulation (GDPR) makes it a mandatory requirement for all public bodies to appoint a Data Protection Officer who will be the cornerstone of accountability for Data Protection, facilitate compliance, inform the data controller and the organisation of their obligations, promote a data protection culture and monitor compliance with GDPR. This role must be :

- Easily accessible – contact details to be available to data subjects and the Information commissioner’s office (ICO)
- Have integrity and high professional ethics
- Be involved properly and in a timely manner in all issues relating to protection of personal data
- Be consulted when a data breach or incident occurs
- Be able to perform duties and tasks in an independent manner, must not be instructed, must be autonomous
- There should be no unfair termination of contract

Caldicott Guardian

7.4. The Caldicott Guardian for the Vale of York Clinical Commissioning Group is the Executive Director of Quality and Nursing.

7.5. The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

7.6. The Guardian plays a key role in ensuring that NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information.

7.7. Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

7.8. The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

Senior Information Risk Owner, (SIRO)

7.9. The SIRO for the Vale of York Clinical Commissioning Group is the Chief Finance Officer.

7.10. The SIRO is an Executive Director or Senior Management Board Member who will take overall ownership of the Organisation’s Information Risk Policy, act as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the Organisation’s Annual Governance Statement in regard to information risk.

7.11. The SIRO must understand how the strategic business goals of the Organisation and how other organisations’ business goals may be impacted by information risks, and how those risks may be managed. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the Organisation and advises the Board on the effectiveness of information risk management across the Organisation.

Information Governance Lead

7.12. The Information Governance Lead for the organisation is the Chief Finance Officer. The Risk and Assurance Manager supports the Chief Finance Officer in delivering Information Governance work programmes and agreed action plans to maintain organisational compliance with DSPT requirements.

7.13. eMBED Health Consortium is contracted to provide Information Governance services and advice to ensure appropriate systems are developed and implemented. The IG Lead is responsible for the co-ordination of and implementation of the IG agenda within the CCG. The IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG within the CCG. This role includes but is not limited to :

- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high level strategy document supported by corporate and/or directorate policies and procedures;
- Ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;
- Providing direction in formulating, establishing and promoting IG policies;
- Establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;
- Ensuring annual assessments and audits of IG policies and arrangements are carried out, documented and reported;
- Ensuring that the approach to information handling is communicated to all staff and made available to the public;
- Ensuring that appropriate training is made available to staff and completed as necessary to support their duties and for NHS organisations;
- Liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;
- Monitoring information handling activities to ensure compliance with law and guidance; and
- Providing a focal point for the resolution and/or discussion of IG issues.

Managers

7.14. Managers are responsible for ensuring that their staff, both permanent and temporary, are aware of :

- All information security policies and guidance and their responsibility to comply with them;
- Their personal responsibilities for information security;
- Where to access advice on matters relating to security and confidentiality; and
- The security of their physical environments where information is processed or stored.

Staff

7.15. Individual employees have a responsibility to ensure they are aware of all information security policies and guidance and comply with them. Staff must be aware of their personal responsibility for the security and confidentiality of information which they use. Staff are responsible for reporting any possible or potential issues whereby a breach of security may occur.

Information Governance Officer

7.16. The Vale of York Clinical Commissioning Group has in place an SLA agreement with eMBED to deliver a range of IG services to assist the CCG to deliver a satisfactory Data Security and Protection Toolkit submission.

8. INFORMATION SECURITY

8.1. With the increasing use of electronic data and ways of working which rely on the use of electronic information and communication systems to deliver services there is a need for professional advice and guidance on their use as well as the need to ensure that they are maintained and operated to the required standards in a safe and secure environment. (Detailed Information Security arrangements are provided in the CCG's Information Security Policy.)

9. HANDLING CONFIDENTIAL INFORMATION

9.1. When handling confidential information and especially where an individual can be identified from the information to be processed, the CCG must ensure that it has determined and documented a legal basis for processing that information. This must be recorded in the data flow mapping process to facilitate risk assessment.

9.2. In addition it must ensure that arrangements are in place to ensure:

- Ensuring data subjects are appropriately informed of all uses of their information
- The security of that information at all points of its lifecycle.
- Recognising and recording objections to the handling of confidential information and where circumstances under which an objection cannot be upheld.
- Ensuring that where objections are received where the proposed uses are not required by law the CCG should ensure they act in accordance with that objection.
- Implement procedures for recognising and responding to individuals requests for access to their personal information.
- Ensure appropriate information sharing arrangements are in place for the purposes of direct care.
- Ensure appropriate data processing agreements are in place to collect or obtain information for management purposes.

9.3. NHS Digital has issued two guidance documents in respect of appropriate information handling and confidentiality of that information :

- **Code of practice on confidential information** : This code of practice describes good practice for organisations handling confidential information concerning, or connected with, the provision of health services or adult social care.
- **A guide to confidentiality in health and social care** : A for those involved in the direct care of a patient on the appropriate handling of confidential information.

9.4. Other Guidance

- **NHS Information Governance*:*** Guidance on Legal and Professional Obligations.
- Report on the Review of Patient-Identifiable Information 1997 (Caldicott Report)
- **Report of the Caldicott2 Review - Information**: To share or not to share? The Information Governance Review 2013
- Government Response to Report of the Caldicott2 Review 2013.
- **NHS England: Everyone Counts:** Planning for Patients 2014/15 to 2018/19.
- **HSCIC**: A guide to confidentiality in health and social care: Treating confidential information with respect - September 2013
- **HSCIC**: A guide to confidentiality in health and social care: references - September 2013
- **National Information Board and DH**: Personalised Health and Care 2020
- **NHS England**: NHS Standard Contract
- **Information Commissioner**: Data Sharing Code of Practice
- **Information Commissioner**: Privacy Impact Assessment Code of Practice

9.5. Arrangements for secure information handling is provided in the following CCG policies :

- Data Protection and Confidentiality
- Records Management.

10. RISK MANAGEMENT

10.1. The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. The eMBED IG Team will be responsible for completion of the risk assessments for any IG related issue, and have a specific remit to risk assess new technologies and recommend controls where necessary.

Awareness and Advice

10.2. The eMBED IG Team will provide advice on any IG related issue. They will be responsible for the production of newsletters and staff e-mails to provide information to staff on IG issues.

11. INCIDENT MANAGEMENT

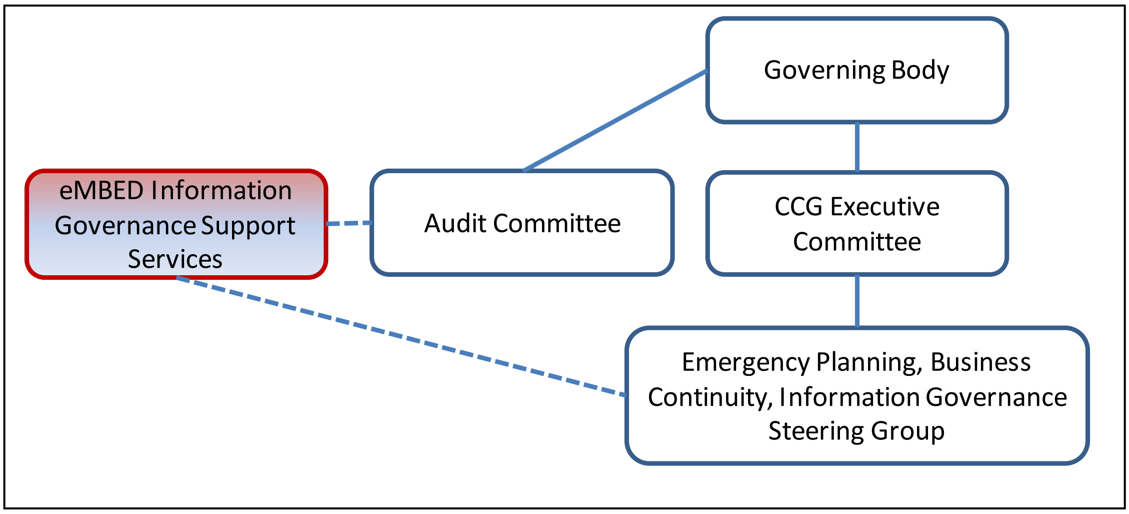
Incident Reporting

11.1. Incidents must be reported and managed through the local incident management process. The eMBED IG Team will have an active involvement in all IG related incidents and IG related service desk calls to ensure compliance with IG principles. Significant issues will be subject to full investigation and reporting action. Incidents relating to personal information will be highlighted to the Caldicott Guardian whilst those of a more technical nature will be reported to the SIRO.

Incident Investigation

11.2. The eMBED IG Team will be have an active involvement in IG issues reported. This may include but is not limited to, breaches of policy, breaches of confidentiality and issues related to IT Security. The CCG must maintain policy and procedure for the appropriate investigation of all incidents reported and promote staff to report all incidents identified.

12. INFORMATION GOVERNANCE FRAMEWORK STRUCTURE


Governing Body
eMBED Information Governance Support Services
Audit Committee
CCG Executive Committee
Emergency Planning, Business Continuity, Information Governance Steering Group

CCG Emergency Planning, Business Continuity and Information Governance Steering Group (Governance Committee)

12.1. The organisation has implemented an Information Governance Steering Group that reports to the Audit Committee. The Emergency Planning, Business Continuity and Information Governance Steering Group will be the organisation's forum with delegated authority to oversee Information Governance issues, assurance and work plans. See Annex B for the Terms of Reference for this group.

13. POLICY IMPLEMENTATION

13.1. Following approval by the policy will be sent to :

- The Communications Manager who will disseminate to all staff via the team newsletter process

- The Chairs of the Governing Body, the Council of Members and all other committees and sub committees for dissemination to members and attendees.
- The Practice Managers of all member practices for information, (if appropriate).

14. TRAINING AND AWARENESS

14.1. The CCG will implement and maintain an approved Information Governance Training Needs Analysis that details the training appropriate for each staff group. The Emergency Planning, Business Continuity and Information Governance Steering Group is responsible for reviewing the Training Needs Analysis. (Appendix E).

14.2. All staff working for the CCG are mandated to undertake Information Governance training as outlined in the following paragraphs. This involves completing the appropriate Data Security and Awareness Training module available on the e-Learning portal.

New Starters

14.3. Staff should complete the Information Governance Training for their role within 4 weeks of commencement of employment. Ideally before they are given access to any systems containing personal data.

Temporary Staff

14.4. **ALL** temporary staff and short-term staff must complete the mandated Information Governance training within a week of commencing employment, (ideally on the first day) this includes volunteers, students, agency and bank staff, and those on short-term contracts (These will be referred to as temporary staff hereafter.)

Annual Refresher Training

14.5. Staff are required to renew their Information Governance Training annually on an on-going basis.

Additional Training Requirements

14.6. In addition to the induction and mandatory annual refresher training there are certain posts/ job roles, which may require a more in depth knowledge of specific aspects of the Information Governance in order fulfil their duties, for example; Caldicott Guardians, Senior Information Risk Owners, Information Asset Owners and Administrators; staff handling patient identifiable data; those with records management responsibilities, those with responsibility for responding to Subject Access Requests, and agile workers who carry and use mobile equipment, e.g. laptops and smart phones.
NB : this is not an exhaustive list. These are disciplines which require specific knowledge and/or clear awareness of certain guidelines, therefore specific information governance training tool modules should be completed.

14.7. The CCG will develop and maintain an IG Training Needs Analysis in order to guide managers in identifying the training that is appropriate to their staff. Managers should consider which modules are appropriate to the job role of the individual members of staff. These do not need to be completed annually but managers may wish to request staff to complete certain additional modules between appraisals. These modules can be completed over a number of years as deemed appropriate by the manager.

14.8. This strategy will be published on the CCG's website.

14.9. The strategy and related policies will be brought to the attention of all new employees as part of the induction process. Further advice and guidance is available from the Risk and Assurance Manager.

14.10. In accordance with the requirement to achieve a satisfactory level on the DSP Toolkit all staff must complete an Induction session when they first start employment which will include Information Governance. In subsequent years all staff are required to complete further Information Governance training as set out in the on line IG Training Tool.

14.11. Within the DSPT there is a requirement for Caldicott, SIRO and IG staff to complete the modules relevant to their roles.

14.12. Staff access IG mandatory training through their ESR Employee Self-service (ESS) Account.

14.13. Staff awareness of IG may be assessed by questions in the annual staff survey or through internal audit survey in order to provide assurance that the training is sufficient.

Third Party Contracts

14.14. The CCG will ensure that contracts with third parties providing services to and on behalf of the CCG include appropriate, detailed and explicit requirements regarding confidentiality and data protection to ensure that Contractors are aware of their IG obligations.

Awareness and Advice

14.15. eMBED IG Team will provide advice on any IG related issue. They will be responsible for the production of newsletters and all staff emails to provide information to staff on IG issues.

15. AUDIT

15.1. Internal audit will provide an independent and objective opinion on Information Governance risk management, control and governance arrangements by measuring and evaluating their effectiveness. The Head of Internal Audit will provide an annual opinion on the effectiveness of the whole system of internal control.

15.2. The opinion will be based on a systematic review and evaluation of risk management, control and governance which comprises the policies, procedures and operations in place to :

- Establish and monitor the achievement of the organisations strategic and operational objectives;
- Identify, assess and manage strategic and operational risks to achieving the organisations objectives;

- Identify the extent of compliance with, and the financial effect of, the relevant established policies, plans and procedures;
- Identify the adequacy and application of financial and other related management controls;
- Ensure the integrity and reliability of information, accounts and data, including internal and external reporting and accountability processes; and
- Identify the extent to which the NHS Vale of York CCGs assets and interests are accounted for and safeguarded from loss of any kind, arising from:
  - fraud and other offences;
  - waste, extravagance, inefficient administration;
  - poor value for money; or
  - other causes.

15.3. Internal Audit shall also independently verify the assurance framework statements detailed in the CCG Annual Report in accordance with NHS guidance.

15.4. The Head of Internal Audit will make suitable provision to form an opinion on key systems operated on behalf of other organisations, and key systems being operated by other organisations, either by deriving the opinions themselves or by relying on the opinions provided by other auditors/review bodies.

15.5. Whenever any matter arises which involves, or is thought to involve, irregularities concerning cash, stores, or other property or any suspected irregularity of a pecuniary nature, the Chief Financial Officer must be notified immediately.

15.6. The Head of Internal Audit normally attends Audit Committee meetings and has a right of access to all Audit Committee members, the Chair and Accountable Officer of the NHS Vale of York CCG.

15.7. The Head of Internal Audit shall be accountable to the Chief Financial Officer. The reporting system for internal audit shall be agreed between the Chief Financial Officer, the Audit Committee and the Head of Internal Audit. The agreement shall be in writing and shall comply with guidance on reporting contained in the Government Internal Audit Standards. The reporting system shall be reviewed at least every three years.

External Audit

15.8. Under the Health and Social Care Act 2012, NHS England will arrange for the Audit Commission to appoint External Auditors for the CCG.

16. POLICY REVIEW

16.1. This strategy will be reviewed every three years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation / guidance.

17. ASSOCIATED POLICIES

17.1. The organisation will implement a number of Information Governance Policies which will be published on the organisation’s intranet and internet sites. Key policies relate to :

- Overarching Information Governance arrangements
- Confidentiality and data protection;
- Information security and risk;
- Information lifecycle management including records management and information quality; and
- Corporate governance including Freedom of Information

17.2. In addition the organisation will implement a number of supporting standards and procedures which also be published and made accessible to staff.

18. CONTACT DETAILS

NHS Vale of York Clinical Commissioning Group
The Governance team
NHS Vale of York Clinical Commissioning Group
West Offices
Station Rise
York, Y01 6GA

Telephone: 01904 55778   Email: valeofyork.contactus@nhs.net

19. APPENDIX A : LINKS TO THE CCG GOVERNANCE RISK ASSESSMENT AND ACTION PLAN

Potential Risk : The CCG may fail to implement effective policies/operational systems and procedures to meet statutory duties and maintain adequate compliance with mandated Information Governance principles.

Action		Assurance Provided By:
1	To establish a robust information governance framework that conforms to Department of Health standards that provides appropriate assurance regarding the efficient, effective, secure and legal processing of all information.	Annual review and sign off of an organisational Information Governance Strategy
2	Maintain a clear outline of responsibilities and reporting structure for all information governance functions.	Implementation of the organisation's and operation of the approved Information Governance Strategy.
3	To ensure that the Governing Body and relevant sub-committees are apprised of the Information Governance agenda, receives periodic assurance that management and accountability arrangements are adequate and assurance that the CCG is fulfilling their obligations.	Annual report to the Governing Body and ad hoc reporting during the year as required. Reporting to the Audit Committee as detailed in the annual work plan for that committee.
4	To use the Data Security and Protection Toolkit as the driver for the main Information Governance work programme reflecting the business needs of the CCG and any other national requirements such as Informatics Planning, or special directives issued by the Department of Health.	Adherence to the Data Security and Protection Toolkit reporting and submission agenda Provision of adequate evidence to support compliance statements.
5	To ensure that there is a suite of policies that encompasses all the elements of information processing that comply with legal and ethical requirements and best practice.	Implementation of CCG Information Governance Policies and related and standard Operating procedures
6	To ensure that there are clearly defined processes in place to support the policies.	Vale of York CCG Information Governance Steering Group Standard Operating Procedures
7	To ensure that organisational information systems, procedures and working practices conform to Information Governance standards	Implementation of Information Governance Policies and related Standards System Level Security Policies
8	To ensure that clear advice and guidance is available for staff and to ensure that they understand and apply Information Governance in their daily working practice	Publication of up to date Information Governance documentation on the organisation's intranet Staff newsletters and briefing documents
9	To ensure that measures are in place to ensure that information is of the highest possible quality.	SLA and reports from the eMBED Business Intelligence Unit assurance. CCG Clinical Record Keeping Standards Policy

Action		Assurance Provided By:
10	To ensure that appropriate and adequate information security controls are in place to protect patient confidential data.	CCG Information Security Policy. Information Security Controls for Commissioning Data. IG assurance is embedded in system/services procurement processes. IG clauses in contracts
11	To undertake regular reviews and audits on the various aspects of information processing. To ensure that such reviews and audits are used to identify good practice and opportunities for improvement.	Outcomes of Internal Audit Information Governance and other related reviews.
12	To ensure that all policies and procedures are monitored and reviewed regularly to ensure that they are adhered to and are effective.	Outcomes from the programme of reviews and monitoring arrangements agreed with the eMBED Health Consortium.
13	To ensure that all staff, service users and the general public will have confidence in the way that we process their information.	Annual review and publication of a Privacy Notice. Up to date guidance published on the organisation’s web site.
14	To ensure that clear advice is given to all data subjects about how their personal information is processed, and to ensure that there is a mechanism to deal with all enquiries.	
15	To ensure that when service developments or modifications are undertaken, that a review is undertaken of all aspects of information governance Arrangements to ensure that they are robust and effective.	Application of the Data Protection Impact Assessment guidance and procedures.
16	To continuously improve the information governance culture across the CCG through training and awareness campaigns.	Approved Information Governance work plan.
17	To ensure that there is a comprehensive proactive information risk management programme.	Report of outcomes of Information Risk Assessments to the SIRO
18	To ensure that all information governance incidents or near misses are notified, investigated and actioned appropriately in accordance with the Data Security and Protection Toolkit and Data Protection Act requirements and CCG policies and procedures.	Report of information governance incidents, complaints and audits are monitored by the Information Governance Steering Group
19	To strive for year-on-year improvements in compliance with the Data Security and Protection Toolkit standards across the CCG.	CCG Information Governance work plan.
20	To ensure that independent contractors comply with Information Governance principles.	Use of approved Information Governance clauses in contracts
21	To support the commitments of the NHS Care Record Guarantee and the NHS Constitution and associated pledges	Data Security and Protection Toolkit submitted to a satisfactory standard.

20. APPENDIX B : TERMS OF REFERENCE

Governance Committee

Terms of Reference

1. Introduction

The Information Governance Steering Group will oversee and monitor the implementation of the Clinical Commissioning Group's (CCG's) Information Governance Framework, including identifying lines of accountability ensuring that information governance practices and procedures are embedded throughout the CCG.

The areas of work within the remit of the Steering Group are :

- Confidentiality and Consent;
- Data Protection;
- Data Quality;
- Information Management;
- Information Disclosure and Sharing;
- Information Security;
- Records Management;
- Registration Authority and access control;
- Information Governance Incident Reporting and investigation; and
- Freedom of Information.

2. Accountability and Reporting

Accountable to:
The Audit Committee of Vale of York Clinical Commissioning Group

Reporting:
The Chair/Vice Chair of the Information Governance Steering Group will provide quarterly reports to the Audit Committee.

3. Membership

The core membership of the Steering Group will be as follows:

- Chief Finance Officer - Senior Information Risk Officer
- Director of Quality and Nursing / Executive Nurse - Caldicott Guardian
- Head of Legal and Governance
- Corporate Governance & Organisational Development Lead
- eMBED Senior Information Governance Specialist

Where a member is unable to attend, a deputy or nominated representative should attend in their place.

4. Attendance

Staff may be requested to attend the meeting in relation to specific topics or the requirement to ensure implementation of appropriate information governance practices and procedures. These may include staff from Contracting, Finance, Improvement and innovation, Integrated Governance and Nursing, Quality and Patient Safety, and any others as required. There may also at times be a requirement for representatives from other Embed Healthcare Consortium departments, e.g. Business Intelligence or IMT.
The CCG's Data Protection Officer should also be informed of dates and time of all these meeting and may attend as and when required.

5. Support to the Committee

The Steering Group will be supported by the Director of Quality as Caldicott Guardian who will be responsible for supporting the Chair in the management of the Group's business and for drawing the Group's attention to best practice, national guidance and other relevant documents, as appropriate.

6. Quorum

A minimum of three members will constitute a quorum. This must include either The Senior Information Risk Owner Officer or the Caldicott Guardian, the IG Lead (or their designated representatives), or the Corporate Governance Lead and one member of the Embed Information Governance Team

7. Frequency of Meetings

The Information Governance Steering Group will meet bi-monthly, a minimum of six times a year.

8. Remit and responsibilities

The Governance Committee is the organisation's forum with delegated authority to oversee the implementation of Information Governance practices, resolution of issues, development and implementation of appropriate work plans, in order to provide appropriate assurance on behalf of the CCG.

The group will liaise closely with the eMBED Health Consortium Information Governance Team who co-ordinate operational Information Governance services on behalf of the organisation.

Overall Purpose

The group's purpose is to support and embed the broader information governance agenda within the CCG and provide the Governing Body with assurance that effective information governance is in place within the organisation.

The Group is tasked with :

- ensuring organisation-wide engagement in the Information Governance Agenda in line with Data Security and Protection Toolkit;

- ensuring that the Information Governance Assurance Framework is documented and embedded across the organisation;
- providing a local forum for Information Governance team leads, disseminating national guidance and best practice; and
- receiving concerns, issues and problems with a view to determining appropriate resolutions.

Specific Responsibilities

Specific Responsibilities are as follows :

- cascade national guidance and advice;
- lead on local implementation of guidance and advice;
- receive and action Information Governance performance reports produced by the Embed Health Consortium Information Governance Team;
- receive and review Information Governance policies and procedures;
- ensuring that agreed information governance strategies, policies and procedures are embedded within the culture and practice of the organisation and adhered to;
- ensuring that local operational leads are assigned for specific areas of the information governance agenda as appropriate, who will be responsible for providing evidence to support Data Security and Protection Toolkit compliance and reviewing and approving toolkit scores in their designated area(s);
- receive reports of information governance incidents and take forward lessons learned resulting from the investigation of those incidents; and
- monitoring compliance of statutory and mandatory training in respect of Information Governance
- Monitoring RA, FOI and SAR compliance, and the completion of Data Flow Mapping and risk assessment.
- Monitoring implementation of IG requirements within the Contracting Process.
- Monitoring the completion of Privacy Impact Assessments for new projects and services and actions required from the risk assessments.
- Monitoring of the implementation of the requirements of the General Data Protection Regulation.

9. Review of terms of reference

The Committee shall review its terms of reference at least annually and any changes recommended will be put to the Audit Committee for approval.

Administration

- The agenda will be managed by the Information Governance Team and circulated to members at least three working days prior to the meeting along with relevant papers;

- Agreed actions will be documented and circulated to all members within five working days of the meeting;

- Any queries regarding the action notes should be referred to the Information Governance Team.

10. Links Maintained by the Committee

Internal

- Accountable Officer and Senior Management Team
- Audit Committee
- Risk Management and Incident Reporting process
- Service managers and staff

External

- Data Protection Officer
- eMBED Health Consortium, (Informatics, HR, ICT, Information Governance)
- Commissioned Acute, Mental Health, Foundation and other NHS Trusts
- Commissioned Any Qualified Providers of Healthcare services
- Commissioned Any Qualified Providers of non-Healthcare services
- Health and Social Care Information Centre
- Information Commissioner’s Office
- NHS England

21. APPENDIX C : DATA PROTECTION PRINCIPLES

GENERAL DATA PROTECTION PRINCIPLES

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individual.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

22. APPENDIX D : THE CALDICOTT PRINCIPLES

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Do not use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

(Extracted From The Caldicott Manual March 2017)

23. APPENDIX E : TRAINING NEEDS ANALYSIS

Staff Group	Training Objective/Aim	Module/Course Name	Method of Delivery	Frequency of Training
New starters	Data Security Standard 3 in the Caldicott Review requires that all staff undertake appropriate annual data security training and pass a mandatory test.	**Data Security Awareness training Level 1**	E-learning	Once – within seven days of starting in role
All Staff	Data Security Standard 3 in the Caldicott Review requires that all staff undertake appropriate annual data security training and pass a mandatory test.	**Data Security Awareness Level 1**	E-learning or classroom based session*	Annually
Records Management staff	To enable understanding of the importance of good records management.	**Awaiting module on** https://nhsdigital.e-lfh.org.uk	E-learning or classroom based session	3 yearly
Staff handling Subject Access Requests	Advice on dealing with requests for access to patient records, both from the patient themselves and their friends and family.	**Awaiting module on** https://nhsdigital.e-lfh.org.uk	Classroom or individual session	3 yearly
Staff Commissioning Services And Project Managers	Data Protection Impact Assessment Training – understanding when DPIAs are required and successful completion.	**DPIA Training is available via the eMBED IG Team**	Classroom or individual sessions*	3 yearly or as required.
Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs)	Describes key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties.	**Awaiting module on** https://nhsdigital.e-lfh.org.uk **Classroom sessions are also available via eMBED IG Team.**	E-learning or Classroom or individual session*	3 yearly
SIRO	To assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in	**Online module withdrawn. Completion of previous module presentation and**	E-learning or classroom/ individual	Yearly

Staff Group	Training Objective/Aim	Module/Course Name	Method of Delivery	Frequency of Training
	understanding and fulfilling their duties.	**workbook to be signed off.** **OR classroom sessions are available from:** https://www.staycompliant.training/ https://www.actnow.org.uk/ https://www.advent-im.co.uk/training/public-sector-senior-information-risk-owner-siro/ **OR any other accredited provider.**	session	
Caldicott Guardian	To learn about the role of the Caldicott Guardian	**Awaiting module on** https://nhsdigital.e-lfh.org.uk **Classroom sessions are available from:** http://www.healthcareconferencesuk.co.uk/courses/caldicott-guardian-training.html https://www.dilysjones.co.uk/training/open-courses OR any other accredited provider.	E-learning or classroom/ individual session	3 yearly
Information Governance	In depth understanding of the Data Protection Act, General Data Protection Regulation (and	British Computer Society (BCS) Data Protection and Information	Specialist courses	Once only

Staff Group	Training Objective/Aim	Module/Course Name	Method of Delivery	Frequency of Training
Support*	associated legislation) and information security	Security courses.	providers	

*IG service delivered by eMBED Health Consortium

24. APPENDIX F: EQUALITY IMPACT ANALYSIS FORM

	Title of policy/ programme/ service being analysed
	Information Governance Strategy (IG11)
	Please state the aims and objectives of this work.
	This document provides justification and defines guidance for the transfer of personal confidential data in a secure way.
	Who is likely to be affected? (e.g. staff, patients, service users)
	Staff
	What sources of equality information have you used to inform your piece of work?
	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 CCG's Committee Terms of Reference and project management framework.
	Who have you involved in the development of this piece of work?
	Internal involvement: Senior Management team Stakeholder involvement: Consultation with Senior Managers Patient / carer / public involvement: This is an Internal policy aimed at staff employed by the CCG and contractors working for the CCG. The focus is on compliance with statutory duties and NHS mandated principals and practice. There are no particular equality implications.
	What evidence do you have of any potential adverse or positive impact on groups with protected characteristics? Do you have any gaps in information? Include any supporting evidence e.g. research, data or feedback from engagement activities **(Refer to** Error! Reference source not found. if your piece of work relates to commissioning activity to gather the vidence during all stages of the commissioning cycle)

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

Marriage and Civil Partnership Refers to legally recognised partnerships (employment policies only)	Consider whether civil partners are included in benefit and leave policies etc.
N/A	
Pregnancy and maternity Refers to the pregnancy period and the first year after birth	Consider impact on working arrangements, part-time working, infant caring responsibilities etc.
N/A	
Carers This relates to general caring responsibilities for someone of any age.	Consider impact on part-time working, shift-patterns, options for flexi working etc.
N/A	
Other disadvantaged groups This relates to groups experiencing health inequalities such as people living in deprived areas, new migrants, people who are homeless, ex-offenders, people with HIV.	Consider ease of access, location of service, historic take-up of service etc.
N/A	
	Action planning for improvement Please outline what mitigating actions have been considered to eliminate any adverse impact? Please state if there are any opportunities to advance equality of opportunity and/ foster good relationships between different groups of people? An Equality Action Plan template is appended to assist in meeting the requirements of the general duty

Sign off
Name and signature of person / team who carried out this analysis Rachael Simmons, Corporate Services Manager
Date analysis completed 08 December 2017
Name and signature of responsible Director
Date analysis was approved by responsible Director

26. APPENDIX G: 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	Policy Name
What is the main purpose of the document	
Date completed	
Completed by	

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

Travel	Will it provide / improve / promote alternatives to car based transport?	N/A		
	Will it support more efficient use of cars (car sharing, low emission vehicles, environmentally friendly fuels and technologies)?	N/A		
	Will it reduce ‘care miles’ (telecare, care closer) to home?	N/A		
	Will it promote active travel (cycling, walking)?	N/A		
	Will it improve access to opportunities and facilities for all groups?	N/A		

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

	Will it specify social, economic and environmental outcomes to be accounted for in procurement and delivery?	N/A		
Procurement	Will it stimulate innovation among providers of services related to the delivery of the organisations' social, economic and environmental objectives?	N/A		
	Will it promote ethical purchasing of goods or services?	N/A		
Procurement	Will it promote greater efficiency of resource use?	N/A		
	Will it obtain maximum value from pharmaceuticals and technologies (medicines management, prescribing, and supply chain)?	N/A		
	Will it support local or regional supply chains?	N/A		
	Will it promote access to local services (care closer to home)?	N/A		
	Will it make current activities more efficient or alter service delivery models	N/A		
Facilities Management	Will it reduce the amount of waste produced or increase the amount of waste recycled? Will it reduce water consumption?	N/A		
Workforce	Will it provide employment opportunities for local people?	N/A		

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

	Will it promote or support equal employment opportunities?	N/A		
	Will it promote healthy working lives (including health and safety at work, work-life/home-life balance and family friendly policies)?	N/A		
	Will it offer employment opportunities to disadvantaged groups?	N/A		
Community Engagement	Will it promote health and sustainable development?	N/A		
	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)?	N/A		
	Will it increase safety and security in new buildings and developments?	N/A		
	Will it reduce greenhouse gas emissions from transport (choice of mode of transport, reducing need to travel)?	N/A		
	Will it provide sympathetic and appropriate landscaping around new development?	N/A		
	Will it improve access to the built environment?	N/A		

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

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)?	N/A		
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?	N/A		
	Will it promote prevention and self-management?	N/A		
	Will it provide evidence-based, personalised care that achieves the best possible outcomes with the resources available?	N/A		
	Will it deliver integrated care, that co-ordinate different elements of care more effectively and remove duplication and redundancy from care pathways?	N/A		