NHS
Vale of York
Clinical Commissioning Group

INFORMATION RISK MANAGEMENT POLICY
November 2018

Authorship :	Pennie Furneaux – NHS Vale of York CCG Risk and Assurance Manager
Reviewing Committee :	Governance Committee
Date :	29 January 2019
Approval Body :	Executive Committee
Approved Date :	20 March 2019
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 • IG06 Information Risk Policy • IG07 Corporate Records Management Standards and Procedures • IG08 Mobile Working Policy • IG09 Subject Access Request Policy • IG10 Safe Haven Policy • IG11 Information Governance Strategy • IG12 Clinical Records Keeping Standards Policy
Target Audience:	All employees, members, committee and sub-committee members of the group and members of the governing body and its committees.
Policy Reference No:	IG06
Version Number:	2.0

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
1.0	Pennie Furneaux	First draft Approved	Management Team 18/02/14	Mar 2014
1.1	Risk and Assurance Manager	Reformatted standard CCG template Include related policies Changes in corporate responsibilities and organisational structures Revision of corporate Risk Management Policy and Strategy	Executive Committee 20.12.2017	15 January 2018
2.0	IG Specialist	Updates to : The Data Protection Act 2018 The General Data Protection Regulation Data Security and Protection Toolkit Data Protection Officer eMBED IG Specialist Fines for data breaches Definition of consent	Governance Committee 29 January 2019 Executive Committee 20 March 2019	03 April 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 4
2. POLICY STATEMENT 4
3. IMPACT ANALYSES 4
4. SCOPE 4
5. POLICY PURPOSE / AIMS AND FAILURE TO COMPLY 4
6. WHAT ARE INFORMATION ASSETS 5
7. MANAGEMENT OF INFORMATION RISKS 6
8. PRINCIPAL LEGISLATION AND COMPLIANCE WITH STANDARDS 8
9. ROLES / RESPONSIBILITIES / DUTIES 9
10. POLICY IMPLEMENTATION 11
11. TRAINING AND AWARENESS 11
12. MONITORING AND AUDIT 12
13. POLICY REVIEW 12
14. REFERENCES 12
15. ASSOCIATED POLICIES 12
16. CONTACT DETAILS 13
17. APPENDIX 1: EQUALITY IMPACT ANALYSIS FORM 14
19. APPENDIX 2: SUSTAINABILITY IMPACT ASSESSMENT 18
20. APPENDIX 3 : NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT 22
22. APPENDIX 4 : THE DATA PROTECTION ACT AND DIRECT MARKETING 24

1. INTRODUCTION

1.1 Information risk is a factor that exists in all areas where information of a personal or confidential nature are used and managed. Information risk management is a part of Information Governance (IG) and it is acknowledged that information governance, including the management of information risk should become part of the culture of the organisation, ensuring that staff are aware of, and work to, good Information Governance (and therefore information risk) practices.

2. POLICY STATEMENT

2.1 This policy 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 in relation to Information Governance and Information Risk.

3. IMPACT ANALYSES

Equality

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

3.2 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

3.3 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.

4. SCOPE

4.1 This policy covers all organisational areas including information risk associated with third party provision of services.

5. POLICY PURPOSE / AIMS AND FAILURE TO COMPLY

5.1 To provide a framework for the management of information risk within the Vale of York Clinical Commissioning Group. The management team is required to embed information risk management into key operational controls and approval processes for all major business processes and provide assurance that information risk is effectively managed.

5.2 Information risk is inherent in all administrative and business activities and everyone working for or on behalf of Vale of York CCG should consciously

manage information risk. There are legal and statutory requirements for the protection of information, both personal and confidential, and this policy sets out how the risks to that information will be managed in compliance with those requirements.

5.3 This policy specifically relates to risk associated with management information, records and data and lays the foundations for a formal information risk management programme by explicitly establishing responsibility for information risk identification and analysis, planning for information risk mitigation, and ensuring that systems are in place to manage and report risks. Highlighting information risk will allow risks to be properly addressed and managed in a way that is most appropriate and effective.

5.4 It should be noted that this policy complements and works on the same principle outlined in the organisation's Risk Management Strategy.

6. WHAT ARE INFORMATION ASSETS

6.1 An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

Examples of Information Assets

Personal Information Content	**Software**
• Databases and data files • Back-up and archive data • Audit data • Paper records (e.g. patient complaints, MP letters and personnel records) • Paper reports	• Applications and System Software • Data encryption utilities • Development and Maintenance tools
Other Information Content	**Hardware**
• Databases and data files • Research records • Back-up and archive data • Audit data • Paper records and reports	• Computing hardware including PCs, Laptops, PDA, communications devices e.g. blackberry and removable media
System/Process Documentation	**Miscellaneous**
• System information and documentation • Operations and support procedures • Manuals and training materials • Contracts and agreements • Business continuity plans	• Environmental services e.g. power and air-conditioning • People skills and experience • Shared service including Networks and Printers • Computer rooms and equipment • Records libraries

7. MANAGEMENT OF INFORMATION RISKS

7.1 It is necessary to ensure a consistent approach to information risk assessment and risk priority ratings so that all risks can be initially prioritised and ultimately agreed by the Finance and Performance Committee, (a formal sub-committee of the Governing Body). eMBED Health Consortium will provide the SIRO with regular reports of information risks. In line with the organisation's Risk Strategy all identified risks should be brought to the attention of immediate line managers.

7.2 A low or moderate risk (as per the organisation's risk matrix) can be regarded as acceptable. All high or significant risks (red and amber as per the risk matrix) should be escalated in line with the Risk Strategy. The Governing Body, through the Finance and Performance Committee will be informed of all significant information risks.

Local information risks

7.3 It is the IAO's responsibility to be aware of, and formally record, information risks in relation to the assets they manage. Many risks will be managed and resolved locally, but higher risks will need to be managed via IG in order to ensure the organisation is aware of those risks and can be assured that active and appropriate management of them is in place.

Information asset risk assessments

7.4 The organisation has implemented a structured information risk assessment process. As a minimum, all information assets listed in the information asset register will be subject to a high level information risk assessment as detailed and evidenced in the register. All assets identified in the register as "key" (i.e. fundamental and critical to the delivery of the organisation's business) will be subject to a more formal risk assessment and details of mitigating controls documented and their effectiveness tested.

7.5 The treatment options for information risk are :

- **Avoid** : not proceeding with activity likely to generate the risk;
- **Reduce** : reducing or controlling the likelihood and consequences of the occurrence;
- **Transfer** : arranging for another party to bear or share some part of the risk, through contracts, partnerships, joint ventures, etc.;
- **Accept** : some risks may be minimal and retention acceptable;

7.6 All identified risks should be scored using the organisation's risk matrix.

7.7 Information risks relating to sensitive personal data and confidential information in hard and soft format will be systematically evaluated by the eMBED IG Specialist and a report of risk profiles and assurances submitted to the SIRO for sign off.

The information asset register

7.8 The NHS Data Security and Protection Toolkit (DSPT) requires that organisations identify all key information assets and their details are included in an Information Asset Register. Information Asset Owners should be identified for each key information asset and that business critical systems have been identified.

7.9 The CCG will establish a programme to ensure that their information assets are identified, documented and assigned to an IAO. The SIRO will oversee a review of the organisation's asset register to ensure it is kept up to date, complete and robust. All critical IA's essential to the delivery of the organisation's services and business will be identified and included within the Information Asset Register. IAOs will ensure that risk reviews are carried out and regularly reviewed, as a minimum this should be annually. The frequency of review may be increased if incidents relating to the asset are reported or if a significant change occurs.

Data flow mapping

7.10 In the NHS, numerous urgent and routine transfers of patient and staff information take place each day for the purposes of healthcare and administration of healthcare services e.g. letters to service users, e-mails to job candidates, moving case notes. It has long been recognised that this information is more vulnerable to loss or compromise when outside the organisation i.e. being carried around or sent/copied from one location to another. The General Data Protection Regulation (GDPR) requires that all transfers of personal/sensitive or corporate confidential data shall be identified and arrangements implemented to protect personal/sensitive/confidential information in transit.

7.11 To ensure all transfers are identified, the CCG must determine where, why, how and with whom it exchanges information. This is known as Data Flow Mapping, (DFM) and the eMBED IG Specialist will assist the CCG in compiling a comprehensive register of information transfers so that these may be risk assessed and appropriate controls implemented to protect the information in transit. This will also allow any Information Sharing Agreements that should be in place to be identified.

Inclusion of information risk in risk registers

7.12 In line with the organisation's Risk Strategy, the risk register will document all information risks rated as significant or high. This Finance and Performance Committee is responsible for escalating high risks to the board and ensuring that where relevant they are admitted to the corporate risk register. Proactive planning will be undertaken for investigating and identifying risks through different scenarios, regular policy reviews, ICO recommendations and assessment of sources of legal weight and admissibility of evidence for reducing risks.

Information risk management training

7.13 All staff assigned information asset risk management responsibilities shall undertake appropriate training. The IG Training Tool is an online training tool

focused on all aspects of learning about IG. The aim of the tool is to develop and improve staff knowledge and skills. Staff are required to undertake the appropriate training modules as identified in the Information Governance Training Needs Assessment. SIRO and IAOs should undertake specific training for their roles:

Information asset accreditation

7.14 Accreditation is the method through which an NHS information asset can be risk assessed and assured that it complies with the Information Governance Security Policy, standards, legal requirements and expected good working practices. Accreditation processes will also allow essential and appropriate assurance to stakeholders including the Senior Information Risk Owner. Such accreditation assurances are :

- The information governance security risks to the information asset and its data have been considered and assessed on a regular basis;
- The required information governance security measures have been implemented correctly and cannot be bypassed; and
- The information governance security risks arising from use of the information asset are acceptable to its provider and other stakeholders.

8. PRINCIPAL LEGISLATION AND COMPLIANCE WITH STANDARDS

8.1 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.

9. ROLES / RESPONSIBILITIES / DUTIES

Accountable Officer

9.1 The Accountable Officer has overall responsibility for the organisation's risk management, including Information Risk Management. Operational responsibility for the organisation's information risk policy and management of information risk is delegated to the organisation's Senior Information Risk Owner.

Senior Information Risk Owner (SIRO)

9.2 The organisation has appointed a Senior Information Risk Owner who is responsible for the on-going development and day-to-day management of the organisation's risk management programme. The SIRO is a member of the Governing Body and is responsible for :

- Championing information risk;
- Ensuring that appropriate information risk policies are maintained;
- Implementing appropriate arrangements to manage information risk; and
- Briefing the Governing Body regarding information risk assurance.
- The SIRO will be supported by appropriately trained Information Asset Owners (IAO's).

Caldicott Guardian

9.3 The Caldicott Guardian is a senior person delegated with the responsibility for ensuring systems are in place to protect confidentiality of patient and service user information and enabling appropriate information sharing.

Data Protection Officer (DPO)

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

Information Assets Owners (IAO)

9.5 Information Asset Owners are responsible for :

- Undertaking appropriate information risk assessments for the assets under their control;
- Taking action to implement commensurate and effective processes and controls to manage the risks identified;

- Drafting, updating and maintaining IG accreditation documentation for the assets under their control;
- Effectively escalating risks as and when required in line with the organisation's policies and procedures;
- Help communicate good information governance practice to staff.
- Taking action in line with organisation policies and procedures;

9.6 Information Asset Owners are also responsible for providing the SIRO with an appropriate level of assurance regarding :

- The risks and threats to the information assets under their control;
- That information assets are fully used within the law for the public good, and
- That assurance regarding the security and use of their asset has been appropriately documented;

Executive Committee

9.7 The Executive Committee is responsible for receiving and approving updated policy and ensuring that appropriate resources are committed to embedding the policy into operational practice.

The Governance Committee

9.8 The Vale of York Clinical Commissioning Group Governance Committee, of which the SIRO and Caldicott Guardian are members; is responsible for monitoring plans and assurances concerning business continuity and information risk management. This Governance Committee will assist with the implementation of appropriate action at a local level to address specific risks arising from risk assessments and incidents as detailed in the action plan and approved by the SIRO.

Staff

9.9 All staff will be aware of information risk management and understand the need for information risk to be a part of the culture of the organisation.

eMBED Healthcare Consortium

9.10 eMBED Healthcare Consortium is contracted to provide Information Governance Support Services for the NHS Vale of York CCG. In line with the Service Level Agreement, eMBED will support the CCG's Information Risk Programme in line with this policy and advise the SIRO in the discharge their duties. This will include :

- Supporting Information Asset Owners in performance of their duties;
- Reviewing Information Asset risk assessments to meet Data Security and Protection Toolkit requirements;
- Providing assurance regarding information risk assessments of information assets held and operated by eMBED Healthcare Consortium on behalf of the CCG;

- Providing appropriate reports and action plans to address identified risks within the scope of the Data Security and Protection Toolkit; and
- Providing specific assurances to the SIRO regarding arrangements to safeguard information in transit.
- Risk and Incident management relating to issues occurring as a result of Information Technology infrastructure incidents within the scope of the eMBED contract with the CCG;

9.11 eMBED will support the Vale of York CCG to appropriately discharge it's duties and responsibilities with regard to the Data Protection Act , the General Data Protection Regulation (GDPR) and Common Law duty of Confidentiality. In this respect eMBED shall :

- Develop and maintain appropriate policies and procedures;
- Support the Caldicott Guardian in developing and maintain a Caldicott Log and Action Plan;
- Provide support to the CCG's Data Protection Officer
- Provide advice and guidance regarding the duty of confidentiality and interpretation of and compliance with the Data Protection Act and the General Data Protection Regulation;
- Support and provide guidance and advice in dealing with subject access requests where necessary;
- Audit data protection compliance;
- Facilitate action in areas identified as being non-compliant; and
- Assist with complaints and incidents concerning data protection breaches.

10. POLICY IMPLEMENTATION

10.1 This policy will be made available to all staff. The policy will be made available to staff and others working under contract or agreement for the CCG and will be published on the CCG's website.

10.2 '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'.

11. TRAINING AND AWARENESS

11.1 Staff will be made aware of the policy through cascading the policy through team meetings; specific staff briefings and accessing the policy on the CCG website.

12. MONITORING AND AUDIT

12.1 Performance against the Data Security and Protection Toolkit will be reviewed by Internal Audit on an annual basis and used to inform the development of future procedural documents.

13. POLICY REVIEW

13.1 This policy will be reviewed on every two years, and in accordance with the following on an as and when required basis :

- Legislative changes;
- Good practice guidance;
- Case law;
- Significant incidents reported;
- New vulnerabilities; and
- Changes to organisational infrastructure.

14. REFERENCES

- Data Security and Protection Toolkit published by NHS Digital;
- The Data Protection Act 2018;
- The General Data Protection Regulation
- Computer Misuse Act, 1990;
- Crime and Disorder Act, 1998; and
- The Human Rights Act 1998.

15. ASSOCIATED POLICIES

- IG01 Confidentiality Audit Policy
- IG02 Data Protection and Confidentiality Policy
- IG03 Internet, Email and Acceptable Use Policy
- IG04 Freedom of Information Act
- IG06 Information Risk Policy
- IG07 Corporate Records Management Standards and Procedures
- IG08 Mobile Working Policy
- IG09 Subject Access Request Policy
- IG10 Safe Haven Policy
- IG11 Information Governance Strategy

- IG12 Clinical Records Keeping Standards Policy

16. CONTACT DETAILS

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

17. APPENDIX 1 : EQUALITY IMPACT ANALYSIS FORM

1.	**Title of policy/ programme/ service being analysed**
	Information Risk Management Policy
2.	**Please state the aims and objectives of this work.**
3.	**Who is likely to be affected? (e.g. staff, patients, service users)**
4.	**What sources of equality information have you used to inform your piece of work?**
5.	**What steps have been taken ensure that the organisation has paid <u>due regard</u> 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.
6.	**Who have you involved in the development of this piece of work?**
	Internal involvement: Senior Information Risk Owner Governance Committee representatives **Stakeholder involvement**: Consultation with eMBED Healthcare Consortium Information Governance Team **Patient / carer / public involvement**: This is an Internal policy aimed at staff employed by the CCG and contractors working for the CCG. The focus is on compliance with statutory duties and NHS mandated principals and practice. There are no particular equality implications.
7.	**What evidence do you have of any potential adverse or positive impact on groups with protected characteristics?** **Do you have any gaps in information?** **Include any supporting evidence e.g. research, data or feedback from engagement activities** **(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 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	
8.	**Action planning for improvement** Please outline what mitigating actions have been considered to eliminate any adverse impact? Please state if there are any opportunities to advance equality of opportunity and/ foster good relationships between different groups of people? An Equality Action Plan template is appended to assist in meeting the requirements of the general duty

Sign off
Name and signature of person / team who carried out this analysis Risk and Assurance Manager
Date analysis completed December 2017
Name and signature of responsible Director Chief Finance Officer (SIRO)
Date analysis was approved by responsible Director

18. APPENDIX 2 : SUSTAINABILITY IMPACT ASSESSMENT

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

Title of the document	Information Risk Management Policy
What is the main purpose of the document	CCG policy document to implement arrangements to comply with statutory duties
Date completed	15 January 2018
Completed by	Rachael Simmons

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		
	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		

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?
Workforce	Will it provide employment opportunities for local people?	N/A		
	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		

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 provide sympathetic and appropriate landscaping around new development?	N/A		
	Will it improve access to the built environment?	N/A		
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		

19. APPENDIX 3 : NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

All persons working for or carrying out duties on behalf of Vale of York Clinical Commissioning Group are required to sign a non-disclosure and confidentiality undertaking as detailed below.

STAFF / AGENCY
STAFF / TRAINEES / APPRENTICES / STAFF ON SECONDMENT
THIRD PARTY RESPONSIBILITIES

You are subject directly or indirectly to the requirements of the Data Protection Act 2018, the General Data Protection Regulation (GDPR), the Human Rights Act 1998, the 'common law duty of confidentiality' and the Freedom of Information Act 2000.

You are also subject to the NHS Code of Practice 2003 which sets out the standards of practice concerning confidentiality and patients' consent to use their health records. These rules apply to any party who works within or is under contract to an NHS organisation.

1. The following terms apply where an organisation or its staff may gain access to, or have provided to it, personal identifiable information (defined within the terms of the Data Protection Act 2018 and the General Data Protection Regulation) when working for, or with Vale of York Clinical Commissioning Group ('the data controller'). They also apply where you have access to commercially sensitive information, security related information and any intellectual property of the contracting organisation.

2. **Information containing a unique number** (e.g. NHS, NI or organisational) or a combination of items from the following list is personal identifiable data: **Name, Address, Postcode, Date of Birth, Other Dates** (i.e. death, diagnosis), **Sex, Ethnic Group or Occupation.**

3. The access referred to in clause 1 above may include access to or sharing of information held in any electronic format or on paper and information that is part of verbal discussions. You are personally liable to respect and protect the confidentiality of the information you collect, process and encounter and should not discuss this information or disclose it to any unauthorised person or company during the course of your work or after termination of your employment.

4. Any information (personal or organisational) will only be used for purposes agreed between the organisations. Anyone who discloses personal information, intentionally or otherwise may be personally liable in damages by the individual affected and may also be subject to disciplinary procedures. In addition, the employing organisation may be liable for financial penalties of up to €20 million, or 4% of the total worldwide annual turnover, whichever is higher.

5. Any work done involving access to personal identifiable information will be done by formally authorised staff of the organisation (except as provided in clause 7 below). The organisation shall keep a record of such authorisations.

6. An NHS mail account must be used to send and receive personally identifiable data which may only be sent to email accounts with a specified level of security, e.g. **gsi.gov.uk; gsx.gov.uk; gse.gov.uk; scn.gov.uk; pnn.police.uk; cjsm.net; Nhs.net** You are responsible for ensuring that all personal and corporate information is stored, used, transported and accessed appropriately and for compliance with the organisation's Information Governance Policies.

7. Where the organisation sub- contracts any work it is doing, this agreement will be an explicit part of that sub- contract.

8. Any breach of the terms of this agreement may result in termination of arrangements (including formal contracts) and legal action may be taken.

DECLARATION

9. I confirm that by signing this agreement I have read and understand the statements made and the statutory rules and NHS policies contained within it.

Signed ……..

Name …….

Job Title ……

Dated …….

Witnessed ……

This document must be signed, dated and retained within Personnel Files.

20. APPENDIX 4 : THE DATA PROTECTION ACT AND DIRECT MARKETING

This Annex is to give an overview of the subject of direct marketing in data protection from guidance published by The Information Commissioner's Office (ICO).

The ICO has received a large number of complaints about unwanted marketing calls and texts. Their focus is on reducing the number of complaints by taking systematic enforcement action.

The subject of direct marketing and how it relates to data protection is complex, therefore this guidance cannot cover the subject in its entirety or great detail enough to ensure compliance. Staff should use the link provided at the end of this document to access the guidance published by the Information Commissioner's Office on direct marketing for the more comprehensive information about marketing & legal requirements.

Direct Marketing Definition

The Data Protection Act 2018 (DPA) defines direct marketing as:

"The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".

The above definition applies to the Privacy & Electronic Communications Regulations (PECR). This is because although direct marketing is not specifically defined in PECR, regulation 2 of PECR states that any expressions that are not defined in PECR will have the same meaning as defined in DPA.

This definition covers **any** advertising or marketing material, not just commercial marketing. All promotional material falls within this definition, including material promoting the aims of not-for-profit organisations, even if that is not the main purpose of the material published.

The definition also covers **any** means of communication, it is not limited to traditional forms of marketing such as telesales or mailshots, and can extend to online marketing, social networking or other emerging channels of communication.

The key element of the definition is that the material must be directed to particular individuals. Indiscriminate blanket marketing – for example, leaflets delivered to every house in an area, magazine inserts, or adverts shown to every person who views a website – will not therefore fall within this definition of direct marketing.

Legal Framework for Direct Marketing

The Data Protection Act (DPA) and Privacy & Electronic Communications Regulations (PECR) both restrict the way organisations can carry out unsolicited direct marketing (that is, direct marketing that has not specifically been asked for by the intended recipient).

Data Protection Act (DPA)

If direct marketing involves the processing of personal data (in simple terms, if the organisation knows the name of the person it is contacting), it must comply with the principles set out in the DPA. The most relevant principles here are :

- **The first principle**: organisations must process personal data fairly and lawfully. In particular, they will need to tell the individuals concerned who the organisation is and that they plan to use those details for marketing purposes. Organisations will also need to tell people if they plan to pass those details on to anyone else, and are likely to need their consent to do so. Organisations must not do anything that people would not reasonably expect or which would cause them unjustified harm.
- **The second principle**: organisations must only collect personal data for specified purposes, and cannot later decide to use it for other 'incompatible' purposes. So they cannot use people's details for marketing purposes if they originally collected them for an entirely different purpose, e.g. to provide health care.
- **The fourth principle**: organisations must ensure that personal data is accurate and, where necessary, kept up to date. So a marketing list which is out of date, or which does not accurately record people's marketing preferences, could breach the DPA.

The DPA also gives individuals the right to prevent their personal data being processed for direct marketing. An individual can, at any time, give written notice to stop (or not to begin) using their details for direct marketing.

Privacy and Electronic Privacy Regulations (PECR)

PECR has been designed to complement the Data Protection Act and set out more detailed privacy rules in relation to the developing area of electronic communications. Regulation 4 of PECR states that nothing contained in those regulations relieves a person from their obligations under the DPA in terms of processing personal data.

Market Research

If an organisation contacts customers to conduct genuine market research (or contracts a research firm to do so), this will not involve the communication of advertising or marketing material, and so the direct marketing rules will not apply. However, organisations conducting market research will still need to comply with other provisions of the DPA, and in particular ensure they process any individually identifiable research data fairly, securely and only for research purposes.

However, an organisation cannot avoid the direct marketing rules by labelling its message as a survey or market research if it is actually trying to sell goods or services, or to collect data to help it (or others) to contact people for marketing purposes at a later date.

If an organisation claims it is simply conducting a survey when its real purpose (or one of its purposes) is to sell goods or services, generate leads, or collect data for marketing purposes, it will be breaching the DPA when it processes the data.

Solicited and unsolicited marketing

There is no restriction on sending solicited marketing – that is, marketing material that the person has specifically requested. PECR rules only apply to 'unsolicited' marketing messages, and the DPA will not prevent an organisation providing information which someone has asked for. So, if someone specifically asks an organisation to send them particular marketing material, it can do so.

If the marketing has not been specifically requested, it will be unsolicited and the PECR rules apply. This is true even if the customer has 'opted in' to receiving marketing from that organisation.

An opt-in means that the customer is happy to receive further marketing in future, and is likely to mean the unsolicited marketing is lawful (see the next section on consent). But it is still unsolicited marketing, which means the PECR rules apply.

Consent

Consent is defined in DPA, and therefore applies to PECR, as:

"a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data."

Consent is central to the rules on direct marketing. Organisations will generally need an individual's consent before they can send marketing texts, emails or faxes, make calls to a number registered with the TPS, or make any automated marketing calls under PECR. They will also usually need consent to pass customer details on to another organisation under the first data protection principle. If they cannot demonstrate that they had valid consent, they may be subject to enforcement action.

To be valid, consent must be knowingly given, clear and specific, as defined above. Organisations should keep clear records of what an individual has consented to, and when and how this consent was obtained, so that they can demonstrate compliance in the event of a complaint.

Marketing calls

General rule : screen live calls against the Telephone Preference Service (TPS)

Organisations can make live unsolicited marketing calls, but must not call any number registered with the TPS unless the subscriber (i.e. the person who gets the telephone bill) has specifically told them that they do not object to their calls. In effect, TPS registration acts as a general opt-out of receiving any marketing calls.

In practice, this means that to comply with PECR, organisations should screen the list of numbers they intend to call against the TPS.

Business-to-business calls

The same rules apply to marketing calls made to businesses, sole traders and partnerships may register their numbers with the TPS in the same way as individual consumers, while companies and other corporate bodies register with the Corporate Telephone Preference Service (CTPS). So organisations making business-to-business marketing calls will need to screen against both the TPS and CTPS registers.

Marketing texts and emails

General rule : only with consent

Organisations can generally only send marketing texts or emails to individuals (including sole traders and some partnerships) if that person has specifically consented to receiving them. Indirect consent (i.e. consent originally given to a third party) is unlikely to be sufficient. Refer to guidance on consenting considerations.
The same rule applies to any marketing sent by 'electronic mail', which is defined in PECR as:

"any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service".

In other words, the same rules will apply to any electronically stored messages, including email, text, picture, video, voicemail, answerphone and some social networking messages. The rules also still apply to viral marketing – organisations will still need consent even if they do not send the messages themselves, but instead instigate others to send or forward them. Organisations must not disguise or conceal their identity in any marketing texts or emails, and must provide a valid contact address for individuals to opt out or unsubscribe (which would mean consent was withdrawn). It is good practice to allow individuals to reply directly to the message and opt out that way, to provide a clear and operational unsubscribe link in emails or at least to provide a Freephone number.

Existing customers : the 'soft opt-in'

Although organisations can generally only send marketing texts and emails with specific consent, there is an exception to this rule for existing customers, known as the 'soft opt-in'. This means organisations can send marketing texts or emails if:

- they have obtained the contact details in the course of a sale (or negotiations for a sale) of a product or service to that person;

- they are only marketing their own similar products or services; **and**

- they gave the person a simple opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that.

The texts or emails must be marketing products or services, which means that the soft opt-in exception can only apply to commercial marketing. Charities, political parties or other not for-profit bodies will not be able to rely on the soft opt-in when sending campaigning texts or emails, even to existing supporters. In other words, texts or emails promoting the aims or ideals of an organisation can only be sent with specific consent.

The right to opt out

Organisations must not send marketing texts or emails to an individual who has said they do not want to receive them. Individuals have a right to opt out of receiving marketing at any time. Organisations must comply with any written objections promptly to comply with the DPA – but even if there is no written objection, as soon as an individual says they don't want the texts or emails, this will override any existing consent or soft opt-in under PECR and they must stop.

You must not make it difficult to opt out, for example by asking customers to complete a form or confirm in writing. It is good practice to allow the individual to respond directly to the message – in other words, to use the same simple method as required for the soft opt-in. In any event, as soon as a customer has clearly said that they don't want the texts or emails, the organisation must stop, even if the customer hasn't used its preferred method of communication.

Business-to-business texts and emails

These rules on consent, the soft opt-in and the right to opt out do not apply to emails sent to companies and other corporate bodies (e.g. limited liability partnerships, Scottish partnerships, and government bodies). The only requirement is that the sender must identify itself and provide contact details.

However, it serves little purpose to send unsolicited marketing messages to those who have gone to the trouble of saying they do not want to receive them. In addition sole traders and some partnerships do in fact have the same protection as individual customers. If an organisation does not know whether a business customer is a corporate body or not, it cannot be sure which rules apply. Therefore we strongly recommend that organisations respect requests from any business not to email them.

In addition, many employees have personal corporate email addresses to which marketing messages could be sent (e.g. firstname.lastname@org.co.uk), and individual employees will have a right under the DPA to stop any marketing being sent to that type of email address.

Other Types of Direct Marketing

The focus of the ICO guidance is on marketing calls and texts (and by extension, emails and other forms of electronic mail). However, PECR also specifically regulate marketing by fax, and the DPA can apply to any other type of direct marketing. These are also covered in more detail in the ICO guidance but in brief, these include:

Marketing Faxes

Organisations must not send marketing faxes to individuals (including sole traders and some partnerships) without their specific consent. See the section above on what counts as consent.

Organisations can send marketing faxes to companies (or other corporate bodies) without consent, but must not fax any number listed on the Fax Preference Service (FPS) unless that company has specifically said that they do not object to those faxes. This means that to comply with PECR, organisations will need to screen the list of numbers they intend to fax against the FPS register.

Marketing Online

Organisations must comply with the DPA if they are targeting online adverts at individual users using their personal data – which might apply if, for example, they display personalised adverts based on browsing history, purchase history, or log-in information.

Marketing Mail

PECR does not cover marketing by mail, but organisations sending marketing mail to named individuals must comply with the DPA. If an organisation knows the name of the person it is mailing, it cannot avoid DPA obligations by simply addressing the mail to ‘the occupier’, as it is still processing that individual’s personal data behind the scenes.

In essence, the DPA requires that an individual is aware that an organisation has their contact details, and intends to use them for marketing purposes. The organisation must have obtained the address fairly and lawfully. It cannot send marketing mail if the address was originally collected for an entirely different purpose.

Lead Generation and Marketing Lists

Marketing lists can be compiled in different ways, and vary widely in quality. A good marketing list will be up to date, accurate, and reliably record specific consent for marketing. A list like this can be used in compliance with the law and should generate few – if any – complaints. However, other lists may be out of date, inaccurate, and contain details of people who have not consented to their information being used or disclosed for marketing purposes. Using such a list is likely to result in a breach of both the DPA and PECR.

A list might contain data compiled in-house from customer contacts. Or it might be a bought-in list of people an organisation has never dealt with directly. Or it could be a mixture of the two. This is an important distinction, because a list compiled in-house should be more accurate and up to date – and easier to check. Quality issues are harder to identify if lists are bought in. And, for certain types of marketing, the law works differently if people's details were not obtained directly.

Generating Leads

There are a wide range of sources for marketing leads. These might include public directories, previous customers and people who have sent an email, registered on a website, subscribed to offers or alerts, downloaded a mobile app, entered a competition, used a price-comparison site to get a quote, or provided their details in any other way. An organisation may be able to legitimately use these sources, but must ensure that it complies with the DPA – and in particular that it acts fairly and lawfully – whenever and however it collects personal data.

If collecting contact details directly from individuals, an organisation should provide a privacy notice explaining clearly that it intends to use those details for marketing purposes. This should not be hidden away in a dense or lengthy privacy policy or in small print. Organisations must not conceal or misrepresent their purpose (e.g. as a survey or competition entry) if they also intend to use the details for marketing purposes. And if they intend to sell or disclose the details to other organisations, the privacy notice should make this very clear, and get the person's specific consent for this.

Buying a Marketing List

Organisations buying or renting a marketing list from a list broker or other third party must make rigorous checks to satisfy themselves that the third party obtained the personal data fairly and lawfully, that the individuals understood their details would be passed on for marketing purposes, and that they have the necessary consent.

Organisations should take extra care if using a bought-in list to send marketing texts, emails or automated calls. They must have very specific consent for this type of marketing, and indirect consent (i.e. consent originally given to another organisation) will not always be enough. Remember also that the 'soft opt-in' exception for email or text marketing cannot apply to contacts on a bought-in list.

ICO PECR guidance can be found at -:
http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/direct-marketing-guidance.pdf