Vale of York
Clinical Commissioning Group

DATA PROTECTION AND CONFIDENTIALITY POLICY

November 2018

Authorship :	IG Team, eMBED Health Consortium
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 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 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. All contractors/volunteers providing services to the CCG.
Policy Reference No. :	IG02
Version Number:	5.1

POLICY AMENDMENTS

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

New Version Number	Issued by	Nature of Amendment	Approved by and Date	Date on Internet
0.1	Chris Wallace	First draft for comments	NR	
0.2	Barry Jackson	Small amendments	NR	
1.0	P. Furneaux	Update to Roles and Accountabilities Inclusion of: Information Sharing Protocols New Uses of PID Subject Access Requests Confidentiality Audit Procedures Non-Disclosure & Confidentiality Agreement Information Governance TNA	Feb 2014	
2.0	IG Team	Addition of regulations re Direct Marketing	Feb 2015 – Audit Committee	
3.0	Helen Sanderson	Addition of HSCIC Guidance and Caldicott 2 requirements	Approved by SMT February 2016	
4.0	Helen Sanderson	Addition of Related Policies Updates to Key IG Post Holders Responsibilities to make consistent with other IG Policies Addition of the Audit Confidentiality Requirements Removal of Training Needs Analysis in order to add it to the Information Governance Strategy.	Approved SMT December 2016	September 2017
5.0	IG Officer	Updated for Changes in Relationship to Embed Updates to reflect General Data Protection Requirement.	15 November 2017	08 December 2017
6.0	Hayley Gillingwater	Updated for changes in Data Protection Act 2018 and the General Data Protection Regulation		

To request this document in a different language or in a different format, please contact:
valeofyork.contactus@nhs.net or 01904 555 870

CONTENTS

1. INTRODUCTION

1.1. The NHS Vale of York Clinical Commissioning Group (from this point on known as the CCG) has a legal obligation to comply with all appropriate legislation in respect of data protection, confidentiality and information security. The organisation is also required to adhere to and comply with Department of Health, NHS England, Information Commissioners Office guidance and individuals are required to comply with guidance published by clinical / professional bodies.

1.2. The principle is that no individual or company working for or with the Vale of York Clinical Commissioning Group shall misuse any information being processed or that they come into contact with, or allow others to do so. It is also required that all individuals or companies working for or on behalf of the organisation implements appropriate information security to protect the information they process and hold in line with legal obligations and NHS requirements.

1.3. All staff and contractors working for the CCG are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within current Data Protection Legislation and, for health and other professionals, through their own professions Codes of Conduct.

1.4. The CCG places great emphasis on the need for the strictest confidentiality in respect of person identifiable and sensitive data. This applies to manual and computer records and conversations about service user's treatments. Everyone working for and on behalf of the CCG is under a legal duty to keep service user's information, held in whatever form, confidential. Service users who feel that confidence has been breached may issue a complaint under the CCG complaints procedure or they could take legal action.

1.5. Confidentiality should only be breached in exceptional circumstances and with appropriate justification and this must be fully documented.

1.6. The CCG is committed to the delivery of a first class confidential service. This means ensuring that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that the public can :

- Understand the reasons for processing personal information;
- Identify a legal basis for processing personal data;
- Give their consent for the disclosure and use of their personal information where necessary;
- Gain trust in the way the CCG handles information; and
- Understand their rights to access information held about them.

2. POLICY STATEMENT

2.1. This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and

policies which are considered as best practice and have been used across many public sector organisations.

3. IMPACT ANALYSES

Equality

3.1. An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1. (Section 15)

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. (Section 16) The assessment does not identify and benefits or negative effects of implementing this document.

4. SCOPE

4.1. This policy applies to all members of staff that are directly employed by the CCG and for whom the organisation has legal responsibility. The policy also applies to those staff covered by a letter of authority / honorary contract or work experience. All individuals working for or on behalf of the Vale of York Clinical Commissioning Group should familiarise themselves with the organisations policies and procedures.

4.2. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

4.3. The policy covers all aspects of business relating to personal confidential information and commercially confidential information within the CCG and/or its agents, customers, prospective customers, service users, suppliers or any other third parties connected with the CCG and in particular shall include, without limitation :

- Service user information;
- Human Resources, including criminal bureau checks on staff;
- Occupational Health
- Ideas / programme plans/forecasts/risks/issues;
- Finance / payroll /budget planning / business cases;
- Sources of supply and costs of equipment and/or software;
- Prospective business opportunities in general;
- Computer programs and/or software adapted or used;
- Corporate or personnel information; and
- Contractual and confidential supplier information. This is irrespective of whether the material is marked as confidential or not.

4.4. The policy covers all methods of holding information, and all media used to store information, including :

- Manually stored paper data, e.g. card index files, medical records etc.;
- Computer referenced paper data, e.g. health records, personnel records, etc.;
- Computerised data held in computer applications, databases and backup media;
- Media used to record CCTV images;
- Data held offsite in archive storage;
- Data held on laptops, CDs, DVDs, flash drives/memory sticks, mobile phones, tablets, I-Pads, and other Personal Digital Assistants, (PDAs) and any other form of electronic media.

5. POLICY PURPOSE / AIMS AND FAILURE TO COMPLY

5.1. The Vale of York CCG Data Protection and Confidentiality Policy sets out the organisation's approach to compliance with Data Protection Legislation, Caldicott Guidance, Care Record Guarantee and other related legislation and mandatory NHS guidance.

5.2. The aims of this policy are to ensure that the organisation appropriately discharges its statutory responsibilities and common law duties of confidentiality in respect of the data it holds and processes as follows:

- To safeguard all confidential information held and processed by the CCG;
- to ensure the CCG has identified a legal basis for holding and processing personal identifiable information under Article 6 of the General Data Protection Regulation and for special categories an additional basis under Article 9 of the regulation and a condition under Schedule one of the Data Protection Act ;
- to complete data protection impact assessments on all new ways of processing personal identifiable information;
- to ensure appropriate information sharing agreements are in place for information sharing between multiple organisations;
- to provide guidelines for all individuals working within the organisation;
- to ensure a consistent approach to confidentiality across the CCG;
- to ensure all staff are aware of their responsibilities with regards to confidential information;

5.3. The aim is to provide all individuals working within the CCG access to the documents which set out the laws, codes of practice and procedures relating to confidentiality and which apply to them. These include :

- Data Protection Act 2018;
- General Data Protection Regulation 2018
- The common law duty of confidentiality;

- Caldicott principles;
- Human Rights Act 1998;
- The Department of Health Publication: Confidentiality: NHS Code of Practice November 2003;
- HSCIC: Code of Practice on confidential information;
- HSCIC: A guide to confidentiality in health and social care;
- the Department of Health Publication Confidentiality: NHS Code of Practice – Supplementary Guidance: Public Interest Disclosures November 2010;
- The Public Interest Disclosure Act 1998;
- The Computer Misuse Act 1990;
- Care Record Guarantee.

5.4. The Vale of York Clinical Commissioning Group shall ensure that all personal information is processed fairly, lawfully and as transparently as possible so that the public can:

- Understand the reasons for processing personal information;
- Give their consent for the disclosure and use of their personal information where necessary;
- Gain trust in the way the organisation handles information; and
- Understand their rights to access information held about them.

6. PRINCIPAL LEGISLATION AND COMPLIANCE WITH STANDARDS

Data Protection Legislation

6.1. Data Protection Legislation establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

6.2. Data Protection Legislation defines data as any information that:

- Is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- Is recorded with the intention that it should be processed by means of such equipment;
- Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or
- Forms part of an accessible record;
- Is recorded information held by a public body.

6.3. The following principles of the General Data Protection Regulation Article 5 state that personal data shall be::

- processed fairly and lawfully and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency');
- 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- 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 ('accuracy');
- 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In addition to the Article 5 principles:

- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Personal data shall not be transferred to a country or territory outside the European Economic Area without adequate protection

6.4. The Vale of York Clinical Commissioning Group is a Data Controller as defined by the Data Protection Act and has registered accordingly with the Information Commissioners Office. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act.

6.5. eMBED Healthcare Consortium provides Information Governance and data processing services on behalf of the CCG. eMBED is not a legal entity in its own right, but acts as a data processor under the terms of the Data Protection Legislation for Vale of York Clinical Commissioning Group. Data controllers remain responsible for ensuring their processing complies with the Act, whether they do it in-house or engage a data processor.

Caldicott Principles

- **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.

- **Don’t 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).

- 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

- **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.

- **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.

- **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.

- **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.

6.6. These principles should underpin information governance across the health and social care services.

Definition and Use of Personal Information

6.7. Person-identifiable information is anything that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number, National Insurance number etc. Any data, combination of data and other information, which can directly or indirectly identify an individual, will also fall into this definition. Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary.

6.8. Information that directly identifies individuals must be regarded as confidential, and should not be used without legal justification.

6.9. Whenever possible, anonymised data, that is data where all personal details have been removed and therefore cannot identify the individual, should be used. The CCG is not authorised to hold patient identifiable data. Data protection law does not apply to data rendered anonymous in such a way that the data subject is no

longer identifiable. Fewer legal restrictions apply to anonymised data. Anonymisation also supports data protection law's general data minimisation approach.

Disclosure of Personal/Corporate Confidential Information

6.10. It is the responsibility of each individual to ensure that information is shared appropriately and securely. Care must be taken to check that there is a firm legal basis in place and a record of the information shared and the reason for sharing is documented accordingly.

6.11. It is essential to consider how much confidential information is required and ensure that the minimal amount necessary is disclosed.

6.12. Information can be disclosed :

- When effectively anonymised.
- When the information is required by law or under a court order, which may include the detection and prevention of serious crime. In this situation staff must discuss with their Line Manager or the Information Governance Team before disclosing, they will then inform and obtain approval of the Caldicott Guardian.
- In identifiable form, with the individual's written consent or with support from NHS England who will apply for the necessary approval from the appropriate authority for example, the Confidentiality Advisory Group (CAG) within the Health Research Authority.
- In potential safeguarding situations or when it is deemed in the public interest. Before disclosure takes place, staff should contact their line manager and the Information Governance Team, who will then inform and obtain approval from the CCG Caldicott Guardian.

6.13. The NHS Confidentiality Code of Practice provides further advice on the use and disclosure of confidential information.

6.14. The CCG will inform service users, staff and other data subjects why, how and for what purpose personal confidential information is collected, recorded and processed by means of a privacy policy posted on the internet and the registration with the Information Commissioners Office.

6.15. **NB** : Disclosures should be in accordance with a relevant information sharing agreement, unless the disclosure is required by law, including under the Public Interest Disclosure Act 1998. The HSCIC have published a Code of Practice on confidential information and A Guide to Confidentiality in Health and Social Care which give comprehensive guidance in handling and sharing confidential information for different purposes.

Information Sharing Protocols

6.16. When necessary Information Sharing Protocol, Data Re-Use or Data Transfer Agreements should have been completed before any information is transferred. The agreement will set out any conditions for use and identify the mode of transfer.

For further information on Information Sharing Protocol contact the eMBED Information Governance Team.

New Uses of Person Identifiable Data

6.17. The use of Data Protection Impact Assessments is required to help the CCG to comply with Privacy by Design principles and should be considered for all new projects and proposals affecting the management of personal data.

Media Enquiries

6.18. All requests for information by the media, other than those made under the Freedom of Information (FOI) Act, must be referred to the Communications Team or the Freedom of Information Team as appropriate for proper management of the response.

Subject Access Requests

6.19. Individuals whose information is held within the CCG have rights of access to it (subject to certain exemptions) regardless of the media on which the information may be held. Individuals also have a right to complain if they believe that the CCG is not complying with the requirements of the Data Protection Legislation.

6.20. Subject Access Requests will be handled in accordance with the CCG's Subject Access Request Procedures. Subject Access Requests for Vale of York Clinical Commissioning Group are supported by eMBED Healthcare Consortium Information Governance Team. .

Staff information

6.21. In keeping with good Human Resources practices, the CCG retains and processes personal data in respect of its employees. In addition, the CCG may from time to time, retain and process 'sensitive personal data' (defined in the Data Protection Act 2018(DPA) and the General Data Protection Regulation (GDPR), for example in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring or for the prevention of fraud or other illegal activities.

6.22. The CCG may process this data, which may also be legitimately disclosed to appropriate employees and to the CCG professional advisors, in accordance with the principles of the DPA and GDPR.

6.23. The CCG will take all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that the data held on him/her is or may be inaccurate, or he/she wishes to have access to such data, they should contact the head of Human Resources in the eMBED Health Consortium.

Contracts of Employment

6.24. Staff contracts of employment are produced and monitored by the eMBED Human Resources department. All contracts of employment include a clause on data

protection and general confidentiality. Agency and non-contract staff working on behalf of NHS must be subject to the same rules via a confidentiality agreement.

6.25. All CCG employees will be made aware of their responsibilities in connection with the Data Protection Legislation, General Data Protection Regulation and Code of Confidentiality.

Confidentiality Audit Procedures

6.26. Good practice requires that all organisations that handle personal confidential data put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated in conjunction with the eMBED Information Governance Team through a programme of audits. A Schedule of Audits which can be undertaken is detailed at Appendix 5 (Section 19)

Disclosure of information outside the European Economic Area (EEA)

6.27. No personal data should be disclosed or transferred outside of the EEA to a country or territory which does not ensure an adequate level of protection unless certain exemptions apply or adequate protective measures are taken.

6.28. In the event that there is a need to process personal information outside of the United Kingdom, the eMBED Information Governance Team must be consulted prior to any agreement to transfer or process the information.

Direct Marketing (Privacy & Electronic Communications Regulations)

6.29. The Privacy and Electronic Communications Regulations (PECR) set out detailed rules and legal requirements in a number of areas that apply to direct marketing of services and products. The marketing rules apply if you are sending marketing and advertising by electronic means, such as by telephone, fax, email, text, picture or video message, or by using an automated calling system.

6.30. The relationship between PECR and the Data Protection Act is a complex one and staff who intend to carry out marketing activities on behalf of the organisation need to be aware of these regulations. Guidance on this is attached with a link to the Information Commissioner's Office and the regulations. See Privacy and Electronic Communications Regulations attached at Appendix 4(Section 18) .

7. ROLES / RESPONSIBILITIES / DUTIES

The Accountable Officer

7.1. The Accountable Officer has overall responsibility for establishing and maintaining an effective Information Governance Framework within the CCG, including data protection and confidentiality requirements, which meets all statutory requirements and adhering to guidance issued in respect of procedural documents.

The Caldicott Guardian

7.2. 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. The Caldicott Guardian is also responsible for monitoring incidents and complaints in relation to confidentiality breaches within the CCG. The Caldicott Guardian will receive reports of potential or actual incidents identified during the audits undertaken in order to monitor investigations as appropriate and ensure appropriate corrective action taken.

The Senior Information Risk Owner

7.3. The SIRO has overall responsibility for the review and implementation of this policy and ensuring that the organisation appropriately discharges its statutory duties and mandated responsibilities. The SIRO is also responsible for monitoring risks in relation to information security and should receive reports of audit results to monitor weaknesses identified and ensure corrective action is implemented

IG Lead

7.4. The CCG Information Governance Lead will co-ordinate with the eMBED Information Governance Team to ensure a system of CCG departmental audits on an annual basis. These audits may involve some or all of the audit mechanisms detailed in Appendix 5 (Section 19)

The Information Governance Steering Group

7.5. The CCG has convened an Information Governance Steering Group which has operational responsibility for :

- Cascading national guidance and advice;
- Leading on local implementation of guidance and advice;
- Receiving and acting on reports received from the eMBED Healthcare Consortium ;
- Receiving and reviewing 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; and
- Taking forward lessons learned resulting from information governance incidents.

Line Managers

7.6. Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to information confidentiality and data protection. They are also responsible for monitoring compliance with this policy e.g. undertake ad hoc audits to check for inappropriate disclosures, records left out, abuse of passwords etc.

Staff

7.7. All staff are responsible for adhering to the Caldicott principles, Data Protection Legislation, the General Data Protection Regulation and the Confidentiality Code of Conduct. Staff will receive instruction and direction regarding these standards from a number of sources:

- Standard / strategy and procedure manuals;
- Line manager;
- Specific training course;
- Other communication methods (e.g. team brief / team meetings);
- Staff Intranet / CCG website.

7.8. All staff are responsible for maintaining the confidentiality of all personal and corporate information accessed during their employment and this extends after they have left employment.

7.9. All persons working for or carrying out duties on behalf of Vale of York Clinical Commissioning Group shall :

- Exercise all due care and diligence to prevent unauthorised disclosure of confidential information;
- Ensure the physical security of all confidential documents and/or media, including storage of files on PCs and any mobile equipment. Confidential information must never be left unattended and should always be secured when not in use;
- Ensure that system level security policies are adhered to;
- Not disclose or share their passwords with anyone including colleagues;
- Only use officially issued and fully encrypted mobile equipment in line with the Mobile Working Policy.
- Implement appropriate information security and safe haven procedures to protect the information they hold and process;
- Complete a Non-Disclosure and Confidentiality Agreement on commencing working for the organisation as detailed at Appendix 3 (Section 17).

7.10. No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information.

7.11. If an individual is unclear as to whether information should be classed as confidential, they must discuss the issue with their manager who will offer advice.

eMBED Healthcare Consortium

7.12. Operational responsibilities to support CCG compliance with the Data Protection Legislation are provided under Contract by eMBED Healthcare Consortium. eMBED provides the following services to the Vale of York CCG and are required to implement appropriate processes and procedures to comply with Data

Protection Legislation requirements and other statutory requirements and NHS mandatory and advisory standards :

- Business Intelligence services;
- Workforce services, including training and development, recruitment and occupational health; and
- IM&T Services which includes Information Governance.

7.13. eMBED will support the Vale of York Clinical Commissioning Group to appropriately discharge it's duties and responsibilities with regard to the Data Protection Legislation, General Data Protection Regulation and Common Law duty of Confidentiality and maintain the CCG's ICO DPA registration. In this respect eMBED shall :

- Act as initial point of contact for Data Protection issues which may arise within the CCG;
- Develop and maintain appropriate policies and procedures;
- Support the Caldicott Guardian in developing and maintain a Caldicott Log and Action Plan;
- Provide advice and guidance regarding the duty of confidentiality and interpretation of and compliance with the Data Protection Legislation ;
- Support and provide guidance and advice in dealing with subject access requests;
- Audit data protection compliance;
- Facilitate action in areas identified as being non-compliant; and
- Assist with complaints and incidents concerning data protection breaches.

8. POLICY IMPLEMENTATION

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

8.2. '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'.

9. TRAINING AND AWARENESS

9.1. Staff will be made aware of the policy via the Intranet and Team Briefs.

9.2. Information Governance training is mandatory and all new starters must receive IG training as part of their corporate induction. All staff members are required to undertake mandated annual refresher training and other accredited Information Governance training as appropriate to their role. The CCG training needs analysis, (TNA) has been developed to advise staff of the Information Governance Training Toolkit modules that they should undertake. (See The Information Governance Strategy for the Training Needs Analysis.)

10. MONITORING AND AUDIT

10.1. The eMBED Information Governance Team, in conjunction with the CCG Policy and Assurance Manager; will lead in monitoring the effectiveness of the policy.

10.2. Adherence to this policy will be monitored though both the programme of confidentiality audits as detailed at Appendix 5 and through the reporting and investigation of breaches of the Data Protection Legislation, General Data Protection Regulation and Common Law Duty of Confidentiality.

10.3. A breach of the Data Protection Legislation, the General Data Protection Regulation or the Common Law Duty of Confidentiality requirements could result in a member of staff facing disciplinary action. All staff must adhere to CCG policies and procedures relating to the processing and protection of personal information

11. POLICY REVIEW

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

12. REFERENCES

- A set of procedural document manuals will be available via the CCG staff intranet.
- Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff intranet.
- All documents in the CCG Policies and Procedures Register are relevant.

13. ASSOCIATED POLICIES

- IG01 Confidentiality Audit 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
- IG11 Information Governance Strategy
- IG12 Clinical Records Keeping Standards Policy

14. CONTACT DETAILS

NHS Vale of York Clinical Commissioning Group
Telephone : 01904 555870
Email : valeofyork.contactus@nhs.net
Address : West Offices, Station Rise, York. Y01 6GA

15. APPENDIX 1: EQUALITY IMPACT ANALYSIS FORM

1.	**Title of policy/ programme/ service being analysed**
	Data Protection and Confidentiality Policy
2.	**Please state the aims and objectives of this work.**
	To Provide guidance and policy on the use and handling of confidentiality information in compliance with the Data Protection Act 2018 and the General Data Protection Regulation
3.	**Who is likely to be affected? (e.g. staff, patients, service users)**
	N/A
4.	**What sources of equality information have you used to inform your piece of work?**
	N/A this is for compliance with the Data Protection Legislation
5.	**What steps have been taken ensure that the organisation has paid due regard to the need to eliminate discrimination, advance equal opportunities and foster good relations between people with protected characteristics**
	The analysis of equalities is embedded within the 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: Caldicott Guardian, Senior Information Risk Owner, EPBCIG Steering Group Members **Stakeholder involvement**: eMBED Healthcare Consortium **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 he evidence 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	

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 October 2017
Name and signature of responsible Director Michele Carrington, Executive Director of Quality and Nursing(Caldicott Guardian)
Date analysis was approved by responsible Director

16. 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	Data Protection and Confidentiality Policy
What is the main purpose of the document	CCG policy document to implement arrangements to comply with statutory duties
Date completed	November 2016 (November 2017, no change)
Completed by	Helena Nowell

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		

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 improve access to opportunities and facilities for all groups?	N/A		
	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?	1	Compliance with the Data Protection Legislation	
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		

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 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		
	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?	0		
	Have you sought the views of our communities in relation to the impact on sustainable development for this activity?	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?
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		
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		

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 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		

16. APPENDIX 3 : NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

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
3RD PARTY RESPONSIBILITIES

You are subject directly or indirectly to the requirements of the Data Protection Legislation, the General Data Protection Regulation, 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 Legislation) 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.

18. 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 and legal requirements.

Direct Marketing Definition

The Data Protection Act 2018 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 & 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.

An organisation cannot, however, 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. 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 and the GDPR – 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 section 11 of 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). PECR, however, 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. Other lists may, however, 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 the GDPR– 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

17. APPENDIX 5 : MECHANISMS FOR AUDITING INFORMATION SECURITY CONTROLS

The Information Governance Team in conjunction with the CCG will develop an audit plan to co-ordinate work as appropriate to ensure the following are undertaken as necessary.

A General Information Security/ safe Haven Procedures

- It is essential that all departments have appropriate information security controls in place to protect PCD at all times. The security and transmission of confidential information/ safe haven standard includes an audit checklist to enable IAO's and department heads to record the assessment of controls in place.

B Review of Information Asset Register and associated Data Flow Maps

- Information asset owners must on a regular basis review their information asset register to ensure that all information assets are recorded and the associated information flow maps have been documented and risk assessed.

C Review of Network Folders and individual systems access.

- Access of staff to network folders should be reviewed on a regular basis, to ensure that leavers have been removed and access allocated is appropriate to the job role. This will require reports of access levels to be produced via the IM&T department and departmental managers/team levels to review access levels set.

- This process also needs to be undertaken for specific systems, to ensure that access is allocated to staff on a need to know basis and that all live users are current employees.

D Failed Log-ins

- Periodically and upon the suspicion of attempted unauthorised access to network folders or an individual system, checks should be made to assess whether unauthorised access has been attempted or obtained. The IM&T Department would need to assist in the production of reports enable these assessments to be undertaken.

E Monitoring Incidents

- All Information Security and Confidentiality incidents reported must be monitored and investigated by the Information Governance Team this includes potential and actual incidents identified as a result of any audit work undertaken.

Audit Reporting and Follow-up

A formal report will be produced detailing the outcome of the audit, recommendations, corrective action and completion timescales agreed.

These reports must be provided to both the Caldicott Guardian and the SIRO for monitoring purposes.

Arrangements should be made to follow-up corrective action agreed to ensure appropriate implementation and that where necessary system documentation and procedures are amended accordingly.

All risks identified must be reported as appropriate on the corporate risk register until such a time as appropriate corrective action is complete. All residual risks must remain on the corporate risk register for management consideration.

Audit Closure

Once the corrective action has been implemented and checked the audit can be formally closed.