NHS
Hambleton, Richmondshire and Whitby
Clinical Commissioning Group

Data Protection and Confidentiality Policy

Authorship:	**Chris Wallace – Information Governance Manager**
Committee Approved:	
Approved date:	**11th March 2014**
Review Date:	**April 2016**
Equality Impact Assessment **Sustainability Impact Assessment** **Target Audience:**	**Screening** **Completed** **All staff**
Policy Reference No:	
Version Number:	**1.1**

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

POLICY AMENDMENTS

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

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Chris Wallace	First draft for comments	NR	
0.2	Barry Jackson	Small amendments	NR	
0.3	John Johnson	Addition of Privacy and Electronic communications regulations	December 2014	

CONTENTS

1 INTRODUCTION

1.1. The Hambleton Richmondshire and Whitby Clinical Commissioning Group (from this point on known as the CCG) as part of NHS England, a public body, has a statutory duty to safeguard the confidential information it holds. The principle of this policy is that no individual or company working for or with the CCG shall misuse any information it processes or comes 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 CCG implements appropriate information security to protect the information they process and hold in line with legal obligations and NHS requirements.

1.2. During the course of their day to day work, many individuals working within or for the CCG will often handle or be exposed to information which is deemed personal, sensitive or confidential, (including commercially confidential) information. It is a requirement that any individual, company and firm to which this policy applies shall not at any time during the period they work for or provide services to the CCG or at any time after its termination, disclose confidential information that is held or processed by or on behalf of the CCG.

1.3 All staff working in 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 the Data Protection Act 1998 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 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;
- 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 ENGAGEMENT

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

3.1 Equality

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

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 3. The assessment does not identify and benefits or negative effects of implementing this document.

4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG etc

4.1. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

4.2. For the purposes of this policy, confidential information shall include any confidential information relating to 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;
- ideas/programme plans/forecasts/risks/issues;
- finance/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.

5 POLICY PURPOSE & AIMS

The aims of this policy are:

- to safeguard all confidential information held and processed by the CCG;
- to provide guidelines in relation to direct marketing regulations
- 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;
- 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:
  - the common law duty of confidentiality;
  - Caldicott principles;
  - Human Rights Act 1998;
  - the Department of Health Publication: Confidentiality: NHS Code of Practice November 2003;
  - the Department of Health Publication Confidentiality: NHS Code of Practice – Supplementary Guidance: Public Interest Disclosures November 2010;
  - Data Protection Act 1998;
  - The Public Interest Disclosure Act 1998;
  - The Computer Misuse Act 1990;
  - Care Record Guarantee.
  - Privacy and Electronic Communications Regulations

It must also be recognised that under the Data Protection Act 1998 that individuals have the right to request access to their information, regardless of the media and format in which the information is held. The CCG must therefore put processes and procedures in place to respond to subject access requests in line with the Data Protection Act 1998.

5.1 Direct Marketing (Privacy & Electronic Communications Regulations)

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.

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 1.

5.2 Conduct

Individuals shall not be restrained from using or disclosing any confidential information which:

- they are authorised to use or disclose by the CCG; and/or
- has entered the public domain unless it enters the public domain as a result of an unauthorised disclosure by the individual; and/or
- has entered the public domain by an authorised disclosure for an authorised purpose by the individual or anyone else employed or engaged by the CCG; and/or
- they are required to disclose by law; and/or
- they are entitled to disclose under the Public Interest Disclosure Act 1998 provided that the disclosure is made in an appropriate way to an appropriate person having regard to the provisions of that Act.

All individuals must:

- 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 be secure when not in use;
- password protect all magnetic media
- passwords must not be disclosed to anyone including colleagues.
- Only use officially issued and fully encrypted mobile equipment in line with the mobile/agile working standard.
- Individuals must implement appropriate information security and safe haven procedures to protect the information they hold and process

All individuals will be required to comply with this policy whilst working within the CCG and thereafter for as long as the information remains confidential information. It is only when the information has entered the public domain that the information can be classed as no longer confidential.

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

5.3 The duty of confidence

- All NHS bodies and those carrying out functions on behalf of the NHS have a duty of confidence to service users and a duty to support professional ethical standards of confidentiality.
- Everyone working for or with the NHS records that handles, stores or otherwise comes across information that is capable of identifying individual service users has a personal duty of confidence to the service user and to his/her employer.
- The duty of confidence is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.
- Service users expect that information given by them to their doctors, nurses and other members of the healthcare team is treated in confidence and not passed to others without their permission. Similar considerations apply to personal information concerning other individuals, such as staff. Particular care must be taken to avoid inadvertent or accidental disclosure. The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised staff includes those who are not involved in either the clinical care of the service user or the associated administration processes.
- No personal information, given or received in confidence, may be passed to anyone else without the consent of the provider of the information. This is usually the service user but sometimes another person may be the source (e.g. relative or carer).
- 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.
- Service users are entitled to object to the use of their personal health data for purposes other than their immediate care.
- The duty of confidentiality owed to a deceased service user should be viewed as being consistent with the rights of living individuals.

5.4 What is personal information

- 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 or combination of data and other information, which can indirectly identify the person, will also fall into this definition.
- Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary.
- Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. Note however that even anonymised information can only be used for justified purposes.
- Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent.
- Confidential information may include personal information such as name, age, address, and personal circumstances, as well as sensitive personal information regarding race, health, sexuality, etc.
- Confidential information may be known, or stored on any medium. Photographs, videos, etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.

5.5 Disclosing information

- The NHS Confidentiality Code of Practice provides advice on using and disclosing confidential service user information and has models for confidentiality decisions and all staff should adhere to this guidance.
- Personal information may be disclosed on the basis of informed consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality.
- The CCG will inform service users, staff and any other data subject why, how and for what purpose personal information is collected, recorded and processed.
- Consent of the data subject will be required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.
- Under common law, personal information may be disclosed without consent for example:
    - in order to prevent abuse or serious harm to others
    - where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service.
- Where information is required by the police, this must be in line with the Data Protection Act section 29, and staff should consult the Information Governance, Security and Compliance Manager. Decisions on whether to disclose information or not must be recorded.

5.6 Personnel information

In keeping with good Human Resources practice, the CCG retains and processes personal data on its employees. In addition, the CCG may from time to time, retain and process "sensitive personal data" (as defined by the Data Protection Act 1998(DPA)), for example in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring for the prevention of fraud or other illegal activities.

The CCG may process such data and such data may be legitimately disclosed to appropriate employees and to the CCG professional advisors, in accordance with the principles of the DPA.

The CCG takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/ her is or may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with the Head of Human Resources.

5.7 Media enquiries

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.

5.8 Termination or expiry of a contract with the CCG

On leaving or termination of a contract with the CCG any copies of software, documents or correspondence, diaries, documents, plans, specifications or any other information relevant to the CCG (whether or not prepared or produced by the individual) must be returned to the CCG's possession and under no circumstances must the leaver take this information with them. All individuals that have left the CCG are bound by the Confidentiality Policy that was in publication at the time of their departure.

5.9 Awareness and compliance

It is important to the CCG to protect its legitimate business interests and in particular it's confidential information. Breaches of confidentiality, of any sort, including breach of this policy will be regarded as serious misconduct and may result in:

- dismissal;
- termination of secondment for secondees and a request for their employer to apply their internal disciplinary procedures;
- termination of contracts for interim resources, temporary workers, agency workers and/or contractors; and
- legal action being taken against the discloser and/or any other third party.

If an individual unintentionally divulges confidential information, or they are aware of any individual doing so, he or she must report it immediately to their line manager and/or to the CCG HR Directorate.

Everyone in the CCG must be aware of the importance of confidentiality. All staff need to be aware of their responsibilities for safeguarding service user confidentiality and keeping information secure.

The duty of confidentiality is written into employment contracts. Breaches of confidentiality are a serious matter. A breach of confidentiality of information gained, whether directly or indirectly, in the course of duty is a disciplinary offence which could result in dismissal and/ or prosecution. No employee shall knowingly misuse any information or allow others to do so.

It is a disciplinary offence to access records/ information that you have no legitimate reason to view this includes, records about yourself, your family, friends, neighbours, acquaintances. If you do not have a legitimate reason to access, do not browse. Remember all transactions are auditable.

6 ROLES / RESPONSIBILITIES / DUTIES

6.1. Overall accountability for procedural documents across the organisation lies with the Managing Director who has overall responsibility for establishing and maintaining an effective Information Governance Framework, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

6.2. Overall responsibility for the confidentiality policy lies with Information Governance, Security & Compliance manager who has delegated responsibility for managing the development and implementation of Confidentiality policy procedural documents.

6.3. The Caldicott Guardian is responsible for overseeing and advising on issues of service user confidentiality for the CCG.

6.4. 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 confidentiality and protecting information. They are also responsible for monitoring compliance with this guideline e.g. undertake ad hoc audits to check for inappropriate disclosures, records left out, abuse of passwords etc.

6.5. Staff are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment with the CCG and this extends after they have left the employ of the CCG.

6.6. Individual staff members are personally responsible for any decision to pass on information that they may make.

6.7. All staff are responsible for adhering to the Caldicott principles, the Data Protection Act, and the Confidentiality Code of Conduct.

6.8. Staff will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods (e.g. team brief/team meetings);
- staff Intranet;

6.9. All staff are mandated to undertake Information Governance training on an annual basis. This training should be provided within the first year of employment and then updated as appropriate in accordance with the Statutory and Mandatory Training Standard and Information Governance Training Needs Analysis.

6.10. The CCG must ensure that all contractors and supporting organisations are working to documented contracts or service level agreements that detail their responsibilities in respect of information governance and security, and confidentiality and data protection. This includes the completion of the Information Governance Toolkit to a minimum of level 2 compliance.

7 IMPLEMENTATION

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

'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'.

8 TRAINING & AWARENESS

Staff will be made aware of the policy via the Intranet.

9 MONITORING & AUDIT

9.1. Performance against the Information Governance Toolkit will be reviewed on an annual basis and used to inform the development of future procedural documents.

9.2. 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.

9.3. Equality Impact Assessment

9.3.1. The CCG aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, service users and the public have been reviewed in line with the CCG's Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, service users and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/ belief.

9.3.2. The Equality Impact Assessment has been completed and has identified impact or potential impact as "no impact"

9.4. Records Management, Retention and Disposal

9.4.1. A records management system must be implemented to ensure that all records are maintained in accordance with the Data Protection Act and Caldicott Principles (See Annexes A&B), and the NHS Records Management, Code of Practice.

9.4.2 The records management systems must include appropriate controls to protect information from unauthorised access, theft or loss, and inappropriate disclosure of person identifiable or corporately confidential information.

9.4.3 A system of timely housekeeping must be implemented and include secure methods of destruction for records that have reached their retention period and been assessed as not to be retained for permanent preservation.

9.5. Complaints

9.5.1 The CCG will implement a complaints procedure to deal with complaints in connection with the Data Protection Act and breaches of confidentiality. If the complainant is not satisfied with the investigation and outcome of their complaint they should be advised of their right to contact the Information Commissioners Office.

10 POLICY REVIEW

This policy will be reviewed in 2 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.

11 REFERENCES

11.1. A set of procedural document manuals will be available via the CCG staff intranet.

11.2. Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff intranet.

11.3. All documents in the CCG Policies and Procedures Register are relevant.

Appendix 1

The Data Protection Act and Direct Marketing

This Appendix 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 1998 (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 & 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:

"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

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 (ie 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 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). 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 (eg 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 (ie 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

Appendix 2

1. Equality Impact Analysis	
Policy / Project / Function:	Data Protection and Confidentiality policy
Date of Analysis:	13/01/14
This Equality Impact Analysis was completed by: **(Name and Department)**	C Wallace - IG Manager – CSU IG Team
What are the aims and intended effects of this policy, project or function ?	This policy sets out the CCG's responsibilities under the Data Protection act and provides guidance on how information held by the organisation should be treated and were necessary kept confidential.
Please list any other policies that are related to or referred to as part of this analysis?	
Who does the policy, project or function affect ? Please Tick ✔	Employees ☒ Service Users ☐ Members of the Public ☐ Other (List Below) ☐

2. **Equality Impact Analysis: Screening**					
	Could this policy have a positive impact on…		Could this policy have a negative impact on…		Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact
	Yes	No	Yes	No	
Race	☐	☒	☐	☒	
Age	☐	☒	☐	☒	
Sexual Orientation	☐	☒	☐	☒	
Disabled People	☐	☒	☐	☒	
Gender	☐	☒	☐	☒	
Transgender People	☐	☒	☐	☒	
Pregnancy and Maternity	☐	☒	☐	☒	
Marital Status	☐	☒	☐	☒	
Religion and Belief	☐	☒	☐	☒	
Reasoning					
If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7					

Appendix 3

SUSTAINABILITY IMPACT ASSESSMENT

Policy / Report / Service Plan / Project Title:				
Theme (Potential impacts of the activity)	**Positive Impact**	**Negative Impact**	**No specific impact**	**What will the impact be? If the impact is negative, how can it be mitigated? (action)**
Reduce Carbon Emission from buildings by 12.5% by 2010-11 then 30% by 2020			X	
New builds and refurbishments over £2million (capital costs) comply with BREEAM Healthcare requirements.			x	
Reduce the risk of pollution and avoid any breaches in legislation.			x	
Goods and services are procured more sustainability.			x	
Reduce carbon emissions from road vehicles.			x	
Reduce water consumption by 25% by 2020.			x	
Ensure legal compliance with waste legislation.			x	
Reduce the amount of waste produced by 5% by 2010 and by 25% by 2020			x	
Increase the amount of waste being recycled to 40%.			x	
Sustainability training and communications for employees.			x	
Partnership working with local groups and organisations to support sustainable development.			x	
Financial aspects of sustainable development are considered in line with policy requirements and commitments.			x	