Data Protection and Confidentiality Policy

November 2020

Authorship:	Senior Information Governance Specialist
Committee Approved:	NHS North Yorkshire CCG Audit Committee
Approved date:	November 2020
Review Date:	November 2024
Equality Impact Assessment:	Yes
Sustainability Impact Assessment:	Yes
Target Audience:	Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	NY-108
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	Senior Information Governance Specialist	First Draft	IGSG (Nov 2020)	
0.2	Senior Information Governance Specialist	Second Draft revised for amendments from IG Steering Group		
1.0	Senior Information Governance Specialist		Approved by NHS North Yorkshire CCG Audit Committee (Nov 2020)	December 20
1.1	Senior Information Governance Specialist	Requirement for new starters to complete Data Security training within first week of starting employment	IGSG (May 2021)	May 2021

Contents

1.0 Introduction

The North Yorkshire 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.

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.

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 Data Protection Legislation and, for health and other professionals, through their own professions Codes of Conduct.

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.

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

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. These are detailed at Appendix B

2.0 Purpose

The aims of this policy are:

- 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, this includes new services, systems and projects;
- to ensure appropriate information sharing agreements are in place for information sharing between multiple agencies;
- 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.

It must also be recognised that under Data Protection Legislation 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 current Data Protection Legislation, the CCG has documented and published a policy for dealing with subject access requests

3.0 Definitions / Explanation of Terms

3.1 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, pseudonymised data, biometric and genetic data, and online identifiers and location data, etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition. 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.

Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary. The appropriate legal basis under Article 6 of the General Data Protection Regulation must be identified and recorded in the CCG Information Asset Register to be able to legally process personal identifiable information.

3.2 Special Category Data

Special category data includes, Health Data, Trade Union membership, Political opinions, Religious or philosophical beliefs, Racial or Ethnic Origin, Sex life and sexual orientation, Biometric Data and Genetic Data.

In addition to having identified a legal basis under Article 6 of the General Data Protection Regulation to legally process personal identifiable information, to legally process special category information the CCG must identify the condition under Schedule 1 of the current Data Protection Act and the legal basis under Article 9(2) and record these on the information asset register.

4.0 Scope of the Policy

The policy applies to NHS North Yorkshire CCG and all its employees and must be followed by all those who work for the organisation, including the Governing Body, those on temporary or honorary contracts, secondments, pool staff, contractors and students.

It is important that the CCG protects 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, they must report it immediately to their line manager, the CCG Information Governance Lead and/or to the CCG SIRO or Caldicott Guardian.

The duty of confidentiality is written into employment contracts. Breaches of confidentiality are a serious matter. 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.

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.

5.0 Duties, Accountabilities and Responsibilities

5.1 Accountable Officer

Overall accountability for procedural documents across the organisation lies with the Accountable Officer 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.

5.2 SIRO

The CCG's SIRO is responsible for overseeing the implementation of appropriate processes and procedures to ensure that individuals information can be processed and held securely.

5.3 Caldicott Guardian

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

5.4 Corporate Services Manager

Responsibility for the Data Protection and Confidentiality policy lies with the Corporate Services Manager who has responsibility for the management, development and implementation of policy procedural documents.

5.5 Line Manager

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.

5.6 All Staff

All 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.

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

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

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;

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.

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 Data Security and Protection Toolkit to a satisfactory level.

5.7 Responsibilities for Approval

Audit Committee is responsible for the review and approval of this policy

6.0 Policy Procedural Requirements

6.1 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 Legislation 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 at: https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/

6.2 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.

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 Health and Social Care Information Centre(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.

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;
- passwords must not be disclosed to anyone including colleagues.
- Only use officially issued and fully encrypted mobile equipment and electronic media 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.

6.3 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.

6.4 Disclosing Information

The HSCIC Code of Practice on Confidential Information and The Guide to Confidentiality in Health and Social Care Services provide advice on using and disclosing confidential service user information and have 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 by means of a privacy notice on the CCG website and where necessary service user information leaflets.

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. This consent must be recorded. Where service users personal information is to be shared on a regular basis in order to provide services or comply with statutory duties of the CCG then an information sharing agreement must be put in place in line with the North Yorkshire Multi-agency information sharing protocol.

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 provided in line with Data Protection Legislation and staff should consult the Information Governance Team before disclosing such information. Decisions on whether to disclose information or not must be recorded.

6.5 Personal 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 Legislation), 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 Data Protection Legislation.

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.

6.6 Media and Freedom of Information Enquiries

All requests for information by the media must be referred to and dealt with by the Communications Team to ensure they are dealt with appropriately.

Similarly all Freedom of Information (FOI) applications must be passed to the officer responsible for managing FOI applications in the CCG as these must be recorded and dealt with in accordance with FOI Legislation.

6.7 Termination or expiry of a contract with the CCG

On leaving or termination of a contract with the CCG any hardware, 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.

Line managers need to ensure that leavers e-mail accounts are closed when someone leave, this may be removing their access under the CCG Organisation and allowing their account to follow them to a new NHS organisation. However if an individual receives confidential information as part of their role i.e. safeguarding staff or legal correspondence, consideration should be given to closing that individual's e-mail account completely and not transferred to another NHS organisation to prevent confidential information being sent to them inappropriately.

6.8 Confidentiality Audit

It is essential that the CCG implement appropriate systems to ensure that personal confidential information and commercially sensitive information is held and processed in a confidential and secure manner. In order to ensure that appropriate controls are maintained the CCG must implement a regular system of reviews and audits to assess controls in place and compliance to these controls. Mechanisms to achieve this are detailed at Appendix C.

6.9 Secure Handling of Information (Safe Haven Checklist)

Secure and appropriate handling of information is essential to maintain confidentiality of both personal identifiable information and corporately sensitive information. Therefore a checklist for appropriate methods of handling, processing and transferring information has been developed to guide staff. See Appendix D

6.10 Broken and old equipment

Broken and old equipment, including mobile phones should always be returned to the CCG to be disposed of securely.

7.0 Public Sector Equality Duty

In developing this policy an Equality Impact Analysis (EIA) has been undertaken. As a result of 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.

NHS North Yorkshire District CCG aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

8.0 Consultation

This Policy has been reviewed by Information Governance Steering Group prior to approval by the Audit Committee.

9.0 Training

Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test, this must be completed by new employees within one week of commencement of employment. Further specific training may be required in line with job roles delegated to staff.

10.0 Monitoring Compliance with the Document

The CCG will monitor compliance with the policy throughout the year via:

- Monitoring and investigating incidents resulting in a breach of confidentiality. Guidance will be sort from the NECS IG Team as appropriate
- Lessons learnt from incidents will be reflected in policies and procedures as required and communicated to staff via the CCG newsletter.

Audit Committee is responsible for monitoring compliance against policy. This is done via updates provided from the IGSG.

11.0 Arrangements for Review

This policy will be reviewed every three 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.

12.0 Dissemination

Staff will be made aware of the policy via the Intranet. Awareness of reviewed and amended policies will be through the CCG staff newsletter.

13.0 Associated Documentation

- Information Governance Framework and Strategy.
- Confidentiality: Code of Conduct
- Subject Access Request Policy
- 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
- HSCIC: Code of Practice on confidential information;
- HSCIC: A guide to confidentiality in health and social care;

14.0 References

This policy was developed in line with the following practices and legislation:

- Data Protection Act 2018;
- Human Rights Act 1998;
- General Data Protection Regulation 2016
- The Public Interest Disclosure Act 1998;
- Health and Social Care Act 2012 and HSC (Safety and Quality) Act 2015.
- The Computer Misuse Act 1990;
- the common law duty of confidentiality;
- National Data Guardian Standards;
- Caldicott principles;
- Information Commissioners Data Sharing Code of Practice

15.0 Appendices

- Appendix A: Data Protection Principles
- Appendix B: Individuals Rights
- Appendix C: Mechanisms for Auditing Information Security Controls
- Appendix D: Safe Haven Checklist

16.0 Appendix A - Data Protection Principles

The GDPR requires that data controllers ensure personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The implementation of the Regulation completed by 25 May 2018.

17.0 Appendix B - Individuals Rights

- Fair Processing (Privacy) notices, to explain how individuals information is used.
- Right of portability, to be able to move their information from one organisation to another.
- Right of erasure.
- Right of rectification.
- Subject Access requests.
- Right to object and restrict processing.

NB/ Not all rights apply to all types of records and exemptions may apply from some of the rights detailed above.

18.0 Appendix C - Mechanisms for Auditing Information Security Controls

The Information Governance Team 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 Checklist (Appendix D)

It is essential that all departments have appropriate information security controls in place to protect Personal information at all times. The security and transmission of personal and confidential information includes an audit checklist to enable Information Asset Owners 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, Shared Mailbox and individual systems access.

Access of staff to network folders and shared mailboxes 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 within 24 hours and must be monitored and investigated, advice and assistance should be obtained from 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.

19.0 Appendix D Safe Haven Checklist

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
General Security					
1	The area should be separated from the general public and unauthorised personnel by appropriate access controls when unmanned, e.g. locked doors and all personal and corporate confidential information should be locked away. In the event visitors require access to office areas they should be requested to sign in, and then be met and escorted as appropriate.				
2	The area should be protected by appropriate alarm and security systems				
3	Personal Confidential Data (PCD) and Corporate Confidential Information should be secured away when not in use, in a formal secure filing system i.e. Clear desk policy				
4	Staff should be aware that the area must be secured if it is to be left unattended.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
5	Where keypad locks are in place the codes should be changed on a regular basis, e.g. quarterly.				
Security of Manual Records					
1	Access to information must be restricted on a need to know basis appropriate to the staff members job role, this applies to all formats e.g. written records, photos, etc.				
2	All types of files containing (PCD) should be held securely when not in use, e.g. filing cabinets / drawers and computers are locked.				
3	Records should be filed in a structured manner. In addition manual records placed in a file should be secured within that file to prevent accidental loss of pages.				
4	A comprehensive tracking / tracing and monitoring system for all records and files should be place. This applies to all stages of transit, including where handovers during transit have taken place.				
5	As far as possible PCD should not be visible through any file covers.				
Security of Electronic Records					

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
1	Monitors and other screens should be placed in such a manner as to avoid the information displayed on them being over looked, e.g. through a window or in an open reception area				
2	Electronic information should only be stored on the main server and not a local computer.				
3	Proper system access controls should be in place i.e. passwords and access levels for each user. Staff should be made aware of their responsibilities in respect the management and security of passwords and smartcards, e.g. passwords and smartcards must not be shared or left unattended.				
4	Staff should be aware that PC's, laptops etc, should be locked or switched off when leaving it unattended				
5	Personal Information or other confidential information should not be copied to any personal PC or media that do not belong to the organisation or is not approved by the organisation.				
Working from Home via VPN					

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
1	The organisation allows authorised access via a VPN, in order to provide those members of staff with a legitimate business need to have access to their authorised section of the organisation network, when working away from organisational premises. VPN access should only be used in association with equipment that has been encrypted and issued by the IM&T department for work purposes.				
2	Staff should be aware that all of the guidance set out in this document must also be applied when working from home.				
Portable Media and Encryption					
1	Only equipment that has been encrypted and issued by the IM&T department should be used for work purposes.				
Transferring Information					
1	Staff should be aware of and have access to the NHS Confidentiality, Code of Practice, HSCIC Code of Practice on Confidential Information and HSCIC: A Guide to Confidentiality in Health and Social Care and Data Protection Policy & Standard.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
2	Transfers and receipt of PCD should only be undertaken by appropriately trained and authorised personnel. Where PCD is sent in password protected documents via NHS Mail the password to the document must be communicated separately preferably via a phone call directly to the person authorised to receive that information. Staff must also be aware of HSCIC: Sending an encrypted email from NHSmail to a non-secure email address				
3	Where necessary consent is obtained from the data subject for any transfers of PCD this must be recorded in the data appropriate record and be in line with documented information sharing agreement for that servicewhere applicable Where consent is not the basis for the transfer, then a legal justification must be identified and documented.				
4	Secure methods of transfer appropriate to the information being transferred have been determined and implemented.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
5	Routine transfers of PCD, to and from the organisation, by whatever method, should be recorded on a data mapping spreadsheet, to ensure appropriate controls of the data at all times. An Information sharing agreement should be documented and agreed by all parties to the information sharing				
6	If information is to be transferred by means of DVD or memory stick these must be encrypted and the encryption password communicated separately, preferably via a phone call directly to the person authorised to receive that information. The DVD or memory stick should be sent via tracked mail.				
Removing Information from secure storage point, including sending to archiving					
1	Staff who are required to remove PCD from organisational premises should be approved to do so and the approval recorded? All staff approved should have signed to say they have read and understand the associated policies. e.g. mobile working, safe haven, code of confidentiality, etc.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
2	A record made of information to be taken from its storage point should be made in the tracking systems in place. NB/ This tracking system should be completed every time information is removed from its storage point, even if it remains in the office. Should records be transferred between members of staff both inside and outside the office a record of this must be made within the tracking system This should be monitored to ensure records are returned.				
3	Only the minimum PCD required for the purpose should be taken when taking records off site. These records should never be left unattended.				
4	Appropriate transportation methods should be implemented, e.g. carried in a locked container or via encrypted electronic methodology.				
5	Staff should be aware that when records are to be transported this must be out of sight i.e. in the boot of the car and that they should not be left in vehicles for long periods, e.g. over night. Where records are to be left in car boots for necessary operational reasons then this should be signed off as agreed by the appropriate governing body.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
6	In situations where staff have been authorised to take records home it must be evidenced that they are aware that the records must be kept securely and not accessible to other members of the household or visitors and records must be returned to their secure storage point ASAP.				
Incoming Mail					
1	Staff should be aware that letters marked private and confidential should opened by the addressee or appropriate nominee only and opened away from public areas				
Outgoing Mail					
1	Confirm from verifiable records the correct name, department, and address are being used, for the intended recipient of the correspondence. A record of information being sent should be maintained on the project or patient file, including when, to whom and by what method When necessary ask the recipient to confirm the receipt of the package. If acknowledgment is not received then it must be followed up as this may be the first indication of a potential breach.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
2	Staff should ensure packages are addressed correctly, and marked appropriately e.g. **private and confidential** where necessary. Return addresses should be annotated on all outgoing mail, to enable recipients to return incorrectly received correspondence without opening it.				
3	Staff should be aware of the correct packaging methods for PCD being sent out and a standard procedure should include a check that the contents being placed in the package are for the addressee of the package.				
4	Staff should be aware of the correct method for sending PCD e.g. courier, post, tracked /special delivery, etc. Nb. Sending an item via special delivery needs to be balanced against the risk of any confidentiality breach and practical and cost issues of using special delivery				
General Transmission by Fax					
1	It should be ensured that fax machines are situated in a secure area at both ends of the transmission and accessible / visible only to authorised staff.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
2	Where Personal Information is to be transferred to another party all methods are considered before the use of fax, e.g. scanning and sending via NHS Mail. All staff should be aware of the HSCIC: Safe Haven Briefing: secure transfer of personal identifiable information by fax **NB**/ Fax should only be used as a last resort or in emergency situations.				
Incoming Faxes					
1	Incoming Faxes need to be collected regularly by authorised staff.				
2	Where possible the fax machine should locked overnight/out of hours.				
3	Where faxes have been incorrectly received, the sender should be contacted to inform them and to agree that the document will be securely destroyed or securely returned for destruction.				
Outgoing Faxes					

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
1	When considering faxing correspondence to another organisation first consider whether NHS Mail can be used instead. NB/ NHSMail has a facility which facilitates the secure transmission of personal confidential information to none NHS Mail account holders. Please see HSCIC: Sending an encrypted email from NHSmail to a non-secure email address				
2	Where the correspondence is to be faxed then staff should be aware that checks must be undertaken to ensure that the fax number to be used is the correct and valid number for the destination				
3	Staff should make the intended recipient aware of the transmission of a fax before sending and request acknowledgement of receipt. If acknowledgment is not received then it must be followed up as this may be the first indication of a potential breach.				
4	Use a fax cover sheet marked **PRIVATE AND CONFIDENTIAL**, indicate the number of sheets being sent, and ensure the intended recipient is verified and named on the cover sheet. Include contact details of the sender.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
5	Staff should request a report sheet from the fax machine to check and confirm transmission was successful.				
Secure Email					
1	Staff should be aware that only NHS Mail and associated secure government email systems are to be used for the transmission of Personal Information. Also that only the minimum Personal Information required for the purpose should be communicated.				
2	All secure email addresses should be checked to ensure the correct email recipient has been selected. Delivery and read receipt options should be selected to verify the message has been successfully sent and the recipient has read it.				
3	Recipients of email correspondence should be checked to ensure that it is appropriate for them to receive the PCD for the intended purpose(s) **NB**/ Only recipients with a genuine need to know should receive the PCD this includes CC's and BCC's				
4	Secure emails containing PCD should be marked confidential.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
5	The organisational standard disclaimer has been placed on all emails stating 'this email is confidential and is intended for the named recipient(s) only. If you have received this email in error please delete it and notify the sender accordingly. Unauthorised copying and or use of this email if you are not the intended recipient may result in legal action being taken.'				
6	Personal Information sent or received via email should be safely stored and archived, as well being incorporated into the appropriate record, including an audit trail of actions.				
Telephone Conversations					
1	Staff should be aware that all telephone conversations regarding PCD should be kept to a minimum and take place in a private area where they cannot be over heard by unauthorised personnel				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
2	When speaking to service users, carers and others, staff should confirm the caller's identity and their authority to receive the information requested, if in doubt check with a manager. Where applicable job title, department and organisation of the caller should be taken, and then called back using a known verifiable number. It is important to guard against people seeking information by deception this is particularly risky when using mobile telephone numbers. This can be waived where a caller is known to you.				
3	Staff should be aware to use the secrecy (mute) button when putting callers on hold.				
4	Where telephone messages containing PCD are received, they should preferably be emailed via NHS Mail to the intended recipient. If this is not possible the message should be placed in an envelope, sealed and addressed to the intended recipient, marked private and confidential.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
5	In the event of requests for information by telephone, staff should confirm the identity of the requestor and their authorisation to receive the information. If in doubt staff should be aware to check with a senior manager. This could mean calling the enquirer back via a main switch board. **NB/ DO NOT** use direct lines for verification purpose as number given by callers may not be genuine.				
Incoming Voicemail and Answerphone messages					
1	When checking messages on an answer phone staff should ensure they cannot be overheard by unauthorised personnel.				
2	Where message books are used is it essential that these are held securely and access to them is on a need to know basis, as appropriate to their staff member's job role. **NB/** Messages should not contain PCD but should refer readers to proper records.				
Answerphones Outwards					
1	Staff should be aware that should they need to leave an answer phone message that they should only leave a name and phone number for call back. Do not indicate the reason for the call.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
Verbal Transfer of Information					
1	Staff should be aware that whenever they are transferring information verbally they must ensure they cannot be overheard by unauthorised personnel.				
2	Where service users register at reception it should be ensured that any personal details they need to give cannot be overheard.				
3	Where discussions include PCD they must not take place in a communal areas, e.g. shared offices, or anywhere else where you can be overheard by unauthorised personnel.				
4	Where message books are used they should be held securely and access limited on a need to know basis. **NB**/ Messages should not contain PCD but should refer readers to proper records.				
Information Sharing					
1	Staff should be aware of their responsibilities in respect of information sharing and documented protocols put in place where information sharing forms a routine part of the service provision.				
2	Staff should be aware of guidance available e.g. The Confidentiality NHS Code of Practice.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
3	Responsibility for making Information sharing decisions should be delegated to appropriate senior personnel.				
Subject Access Requests					
1	Staff should be made aware of their responsibilities in respect subject access requests received and appropriate staff identified and trained to deal with these requests. All subjects access requests must be processed in line with the Subject Access Request Policy				
2	Staff should be able to advise individuals on how to apply for a copy of their information.				
3	Records are reviewed by a clinician or senior manager as appropriate to ensure no exempt information is sent out and that the correct records are being sent to the correct recipient in response to the request.				
Disposal of Information					
1	Secure methods of disposing of Personal Information, whatever format it may be in, should be identified and implemented. This must be done in compliance with the NHS Code of Practice for Records Management.				

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
2	A register of records destroyed must be maintained. This must be done in compliance with the NHS Code of Practice for Records Management.				
Reporting Incidents					
1	Staff should be aware that all breaches of confidentiality and information security must be reported within 24 hours on the CCG reporting system, including near misses. Staff should trained in the corporate incident reporting system.				
Highlighting Security Weaknesses					
1	Staff should be aware that they are responsible for reporting security weaknesses identified to their manager for corrective action				
Training					
1	All staff have been briefed and are aware of information handling, transferring, sharing and security requirements. Data Security and Awareness Statutory and Mandatory Training must be been completed annually				
Documented Procedures					

No.	Guidance	Current departmental process	Adequate YES/NO	Corrective action identified (Where Applicable)	Action Date and officer nominated
1	Controls and procedures put in place, in line with this standard, have been documented, made available to staff and staff trained appropriately				
Residual Risks					
1	All risks identified in this audit which cannot be mitigated must be reported to and approved by the appropriate governing body and recorded on the risk register.				

Note this list is not exhaustive other controls can be implemented if thought required