Confidentiality Code of Conduct	
Author	Narissa Leyland, Head of Information Governance & Data Protection Officer (Former) Simon Boycott, Head of Development and Governance
Corporate Lead	Jim Barwick, Chief Executive
Document Version	1.1
Document Status	FINAL
Date approved by Quality Committee	5th July 2022
Date issued	5th July 2022
Review date	July 2023

Executive summary

It is necessary that the organisation has a set of standards which detail the importance in relation to keeping information safe and secure once it is the possession of Leeds GP Confederation.

Therefore all staff need to be aware of the requirement to ensure that they treat information which comes into their possession in a confidential manner and in line with the requirements of the Data Protection Act 2018. The consequences of not adhering to this policy are reputational damage and potential monetary penalties from the Information Commissioners Office.

This document must be read in conjunction with the Information Governance Policy and Framework and the Records Management Policy to ensure that corporate records are afforded the appropriate level of protection as appropriate.

Contents

1. Introduction

The purpose of this Confidentiality Code of Conduct is to lay down the principles that must be observed by all who work within the Leeds GP Confederation (the Confederation) and have access to personal confidential data about either patients or staff e.g. health records; Human Resource records.

It is important that the Confederation protects and safeguards personal information that it collects process and discloses, in order to comply with the law and the relevant NHS mandatory requirements.

All employees working in the NHS 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 a requirement of their contractual responsibilities, a requirement within the Data Protection Act 2018 and, for health and other professionals, through their own professions' Code/s of Practice. This means that employees are obliged to keep any relevant personal identifiable data e.g. patient and employee records information strictly confidential. It must be noted that employees also come into contact with non-person identifiable information which must also be treated with the same degree of care e.g. business in confidence information, financial reports.

Section 12 contains the legal and NHS-mandatory framework for confidentiality which forms the key guiding principles of this policy and consists of:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act (2018)
- The Human Rights Act (1998)
- The Computer Misuse Act (1990)
- The Caldicott Principles (1998)
- Confidentiality: NHS Code of Practice (2003)
- National Data Guardian - 10 Data Security Standards
- The NHS Constitution

This policy has been produced to ensure the Confederation is able to fulfil its duties as a member's organisation and health care provider whilst maintaining the rights of individuals in respect of their personal confidential data. Setting out the requirements placed on all staff when sharing personal confidential data. It is not possible to provide detailed guidance for every eventuality, therefore where further clarity is needed, the advice of a senior manager or the Information Governance Team must be sought.

A summary of Confidentiality Do's and Don'ts can be found at Appendix A.

2. Aims and Objectives

This policy is intended to cover personal confidential data for both patients and staff from which an individual can be identified. The data may remain within an NHS premises or be taken off site by staff that need to visit patients at home, travel to clinics, or work from home. Typically, the guidance will cover clinical information, personnel details and special categories data as defined by the General Data Protection Regulation (GDPR).

3. Definitions

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. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Personal confidential data can be anything that relates to patients, staff, their family or friends, including attendances at appointments, staff qualifications, training, disciplinary records and information about volunteers, agency staff and contractors, however stored. For example, information may be held on paper, floppy disc, CD, USB sticks, computer file or printout, laptops, mobile phones, digital cameras, video, photograph or even heard by word of mouth. However person-identifiable data must not be stored on removable media unless it is encrypted to NHS standards.

Special category data refers to personal information about: race or ethnic minority; political opinions; religious or similar beliefs, trade union membership, physical or mental condition; sexual preferences; biometric data; commission or alleged commission of offences or a legal proceeding. This category also includes sensitive health information e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, human immunodeficiency virus (HIV) and termination of pregnancy.

The General Data Protection Regulation (GDPR) consent definition:

“Freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

4. Responsibilities

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that Leeds GP Confederation policies comply with all legal, statutory and good practice guidance requirements.

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott standards with respect to patient-identifiable information.

The Corporate Committee oversees the development and implementation of Information Governance in Leeds GP Confederation and ensures that Leeds GP Confederation complies with supporting the legal and NHS-mandatory framework with regard to Information Governance. They will be responsible for reviewing and updating the Confidentiality Code of Conduct. The work done by the committee in respect to Information Governance is overseen and by the Audit Committee.

Heads of Service are responsible for ensuring that they and their staff are familiar with the Code of Conduct and that staff comply with the requirements of the: Data Protection Act (2018), Caldicott Principles, Human Rights Act - Article 8, and the Common Law of Confidentiality. They must ensure that any breaches of the Code of Conduct are reported, investigated and acted upon.

The Director of Workforce is responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the Code of Conduct.

The Head of Information Governance & Data Protection Officer is responsible for ensuring that policies reflect the current legislative position regarding information law and the provision of advice and guidance to staff throughout the organisation and that confidentiality is included in all corporate inductions for staff.

Service Managers are responsible for ensuring that this policy is implemented and that all staff is aware of the content within their service area.

Confidentiality is an obligation for all staff. Staff must note that there is a Non-Disclosure of Confidentiality Information clause in their contract and that they are expected to participate in induction training and awareness raising sessions carried out to inform/update staff on confidentiality issues. Any breach of confidentiality, inappropriate use of health or staff records or abuse of computer system is a disciplinary offence and may constitute as gross mis-conduct. Any breaches must be reported to the Head of Information Governance & Data Protection Officer and Caldicott Guardian.

It is the responsibility of the privacy officer to ensure appropriate access to deducted electronic patient records.

All staff employed by Leeds GP Confederation must work in accordance with the Leeds Safeguarding Multi-agency Policies and Procedures and local guidelines in relation to any safeguarding concerns they have for service users and the public with who they are in contact.

5. Principles

The legal and NHS mandated framework for confidentiality, forms the key guiding principles of this policy.

Staff and patients must be confident that their privacy will be respected, and that personal information about them will remain confidential. The Confederation is responsible for protecting all the information it holds and in any situation must be able to justify any decision to pass on information.

The ethical duty of confidence borne by health professionals, and the common law duty of confidence that applies to all individuals, mean that all NHS staff and associated persons have responsibility for protecting information.

The guiding principle is that information provided in confidence must not be used or disclosed in a form that might identify the person without a clear legal basis e.g. for the provision of direct patient care or explicit consent has been obtained. This duty of confidence continues after the death of the data subject, the resolution or conclusion of the topic or the member of staff has left the Confederation. There are a few exceptions where information can be disclosed without consent.

5.1 Obtaining consent and processing of information

The Leeds GP Confederation must demonstrate it is processing personal data lawfully and identify which legal basis is being used.

As the Confederation provides direct healthcare there is a clear legal basis set out in the Health & Social Care Act 2012. Where the patient is aware that their care will involve other health and social care provider's personal confidential data can be shared. For all other sharing of patient healthcare data, where direct care is not the legal basis, the explicit consent of the patient or client must be sought.

If there is an issue of consent this must be raised as early as possible in discussions with a patient / staff member i.e. at the time initial information is

collected. If it is not possible to do this then, it must be done as soon as possible afterwards (see Appendix B for further guidance on obtaining consent to share information).

When gathering information the person providing that information must be told what the information is needed for highlighting any “non-obvious” purposes for which their data will be used. For example explicit consent must be obtained for a research programme or to use the patient record as evidence towards gaining an academic or clinical qualification.

Do not collect, hold or process more information than is needed, but only hold enough information to ensure that no-one could be misled or interpret the information incorrectly.

Person-identifiable data kept must be accurate and where necessary kept up to date. When staff becomes aware that information about an individual is incorrect, the information must be corrected as soon as possible. One method of improving the accuracy of patient data is to use the NHS number.

Do not use person-identifiable information unless it is absolutely necessary. Where use of person-identifiable information is essential, each individual item of information must be considered and justified so that the minimum amount of identifiable information is used in line with the requirements/principles of the Data Protection Act 2018

It is essential that information must not be kept longer than necessary; therefore once person-identifiable information has served its purpose it must be disposed of in accordance with the Confederation’s Records Management Policy.

5.2 Disclosing information

Care must be taken to check that enquirers have a legitimate right to have access to the information that they ask for, so that information is only shared with the right people.

It is important to consider how much information is needed before disclosing it and only disclose the minimal amount necessary. For example, providing a whole medical record is generally needless and is likely to constitute a breach of confidence.

If staff have any concerns about disclosing information they must discuss this with their manager or if they are not available contact the Information Governance Team for assistance.

Patients generally have the right to object to the use and disclosure of confidential information that identifies them, for non-direct care purposes and need to be made aware of this right.

Information can be disclosed:

- With the patient's/staff explicit consent for a particular purpose.
- On a need to know basis if the person receiving the information is involved in the patient's treatment and/or care and requires the information.
- When the information is required by law or under a court order (legally required or allowed to share). In this situation staff must discuss with their manager or Information Governance staff before disclosing.
- In Child Protection proceedings if it is considered that the information required is in the public or the individual's best interest (to prevent harm).
- Information can be disclosed under the Mental Capacity Act 2005 if the person lacks capacity to give their consent, and sharing of the relevant information is in the person's best interests.
- Where disclosure can be justified for another purpose (exemptions to data protection law). This is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime (see below).

5.2.1 Disclosures / Exemptions of the Data Protection Act 2018

Under the Data Protection Act 2018 Schedule 1 (10) disclosures to the police without consent can occur for the:

- Prevention or detection of crime, or
- Apprehension or prosecution of offenders.

Disclosure is NOT compulsory and only allows for the release of personal information where not releasing it would be likely to significantly harm any attempt by the police to prevent crime or catch a suspect.

The police must submit a written request form specifying what information they require. The request must be passed to the Data Protection Office, who will log and review the request to ensure it complies with the Act i.e. that it is for specific information related to an incident and not excessive in relation to the crime; that it is made by a sufficiently senior officer and it is for one of the purposes set out in the Act.

The Data Protection Officer will discuss with the team receiving the request whether disclosure must take place and either take the agreed action or advise the relevant service of the outcome in order that they can take action.

Where the purpose for which the information will be used is not for the direct health care of the patient and a different statutory basis has not be identified, there is a need to ensure that the patient has provided explicit consent. Additional efforts to gain consent may be required or alternative approaches that do not rely on identifiable information will need to be developed.

Care must be taken, particularly with confidential clinical information to ensure that the means of transferring it from one location to another are as secure as they can be. Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail. For further information see the Information Handling Policy.

5.3 Working in the Community

There are situations when staff need to work from home, undertake home visits and/or travel to clinics all of which mean that these staff may have to carry personal confidential data with them.

To ensure safety of that data, staff must ensure that this is kept with them at all times and that it is kept in a secure place if they need to take it home at the end of their working day. For further information see the Information Handling Policy.

Staff must try and minimise the amount of personal confidential data that is taken out of NHS premises. If staff have to carry confidential data around during the day they must consider their travel plans, for example calling into shops or petrol station on the way home or whilst travelling to work when they are least likely to be carrying patient records.

If staff need to carry confidential records they must ensure the following are considered and remember that there is personal liability under the Data Protection Act 2018 and their contract of employment for breach of these requirements:

- Ensure any personal information in paper form is in a bag prior to them being taken out of NHS buildings so the contents cannot be actually read or dropped by accident.
- Make sure information is put in the boot of a vehicle or carried on their person while being transported. Information must not be left unattended in a vehicle.

If staff must take records home they have a personal responsibility to ensure the records are kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or the outside folder of the records or have any access to the records. To minimise the

loss in the unfortunate event of theft please keep paper records in a separate bag to your laptop computer at home. For manual records they must be logged as being back within the Confederation.

5.4 Working from Home

Some staff may work from home on occasions and must ensure that when working out of office they do not save any confidential or restricted information on non-Leeds GP Confederation computers / laptops.

Staff must never email work to or from their personal email account. If access to confidential information is required when working away from a Confederation base, an application for access to the Remote Access Solution (RAS) must be used.

Paper records taken off site must not be viewed by non-Leeds GP Confederation staff or those not involved in the provision of healthcare to the patient unless the patient has consented.

5.5 Vigilance

All staff have a duty of confidentiality and must take care to keep person-identifiable information private and not to divulge information accidentally. Staff must not:

- Talk about patients in public places or where they can be overheard.
- Leave any medical records or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents.
- Leave a computer terminal logged onto a system where personal and sensitive information can be accessed, unattended.
- Leave patient records in the car unattended for any length of time.

Staff have a responsibility to ensure the safety and security of person-identifiable information held in paper and on computers.

Passwords must be kept securely and must not be disclosed, passwords must not be shared at any point. Staff must not use someone else's password to gain access to information. Use a code to write them down if you cannot remember them and never write them in a full form.

5.6 Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to oneself, one's own family, friends, acquaintances or anyone with whom the staff member does not have a legitimate care relationship. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

5.7 Reporting of breaches

All breaches of confidentiality must be reported using the incident reporting procedure found on the Confederation intranet.

The incident must be recorded on DATIX which will trigger a formal investigation and reporting process to NHS Digital and the Information Commissioner depending on the severity.

On a routine basis a report on breaches of confidentiality of personal information shall be presented to the Corporate Committee the information will enable the monitoring of compliance and enable improvements to be made to the policy.

6. Training Needs

All new staff will be made aware of the existence of this guidance via corporate and local induction process. Managers must highlight to staff their responsibility to ensure that they review the content of this guidance and the importance that Confederation place on this matter and remind staff of the "non-disclosure of confidentiality information clause" in their staff contract.

Managers must actively ensure that staff with access to personal data, undertake and complete the mandatory Data Security Awareness training as approved by the Corporate Committee.

Refer to the Statutory and Mandatory Training Policy including Training Needs Analysis. Up to date information is available on the Intranet for course details.

7. Monitoring Compliance and Effectiveness

An audit of this Code of Conduct will be supported and informed by analysis of breaches of confidentiality and complaints from the public.

8. Approval and Ratification process

The policy has been approved by the Corporate Committee on behalf of the Executive.

9. Dissemination and Implementation

Dissemination of this policy will be via the Confederation website.

10. Review arrangements

This policy will be reviewed in three years by the author or sooner if there is a local or national requirement then ratified by the Corporate Committee.

11. Associated documents

Data Protection Policy
FOI Procedure
Individual Rights and Subject Access Request Procedure
Information Governance Policy and Framework
Information Handling Policy
Network Security Policy
Records Management Policy

12. References

A Manual for Caldicott Guardians (2017)
Access to Health Records Act (1990)
Computer Misuse Act (1990)
CQC Safe Data, Safe Care (2016)
Data Protection Act (2018)
Environmental Information Regulations (2004)
Freedom of Information Act (2000)
General Data Protection Regulation (2018)
Health and Social Care Act (2012)
Health and Social Care (Safety and Quality) Act (2015)
Human Rights Act (1998)
National Data Guardian – 10 Data Security Standards (2018)
Records Management Code of Practice for Health and Social Care (2016)
Information Security Management Code of Practice (2007)

Information: To Share or Not to Share (2013) (Caldicott2)
Privacy and Electronic Communications Regulations (2003)
Report on the Review of Patient-Identifiable Information (1997) (The Caldicott Report)
National Data Guardian - Review of Data Security, Consent and Opt-Outs (2016)
The NHS Constitution (2015)

APPENDIX A - Confidentiality of Personal Data - Do's and Don'ts

Do

- Do safeguard the confidentiality of all personal information that you come into contact with. This is a statutory obligation on everyone working within the Confederation.
- Do clear your desk at the end of each day, keeping all portable records containing personal data in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to personal information, or put them into a password-protected mode, if you leave your desk unattended.
- Do ensure that you cannot be overheard when discussing patients.
- Do challenge and verify where necessary the identity of any person who is making a request for confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer personal information securely when necessary i.e. only use an nhs.net email account to send patient identifiable information to another nhs.net email account or other secure email listed in email policy or encrypt an attachment.
- Do seek advice if you need to share information without consent, and record the decision and any action taken.
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don't

- Don't share passwords or leave them lying around for others to see.
- Don't disclose information without the consent of the person concerned, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless absolutely necessary, anonymise where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

APPENDIX B - Guidance on Obtaining Consent to Share Personal Information

Why consent is needed

The NHS needs to record information about patients and their health in order to efficiently manage services and protect patient safety. Normally patients must give consent to their information being recorded and shared. The consent given must be "**informed**" i.e. the patient must be made aware of why information about them is needed, how it will be used and stored and if it is to be shared, who it will be shared with and why.

Obtaining consent

All individuals over the age of 13 are assumed to have capacity to consent unless it can be proven otherwise (Mental Capacity Act 2005).

Every individual has the right to make their own decisions and is assumed to have capacity to do so unless proved otherwise.

Capacity can be defined as being able to understand and retain relevant information and then to consider it so that a choice can be made.

It is best practice to revisit the issue of consent with the patient at each new episode of care to ensure that the information held about them is accurate and up to date, and that they are still happy for this information to be shared where necessary.

It must be made clear to patients that under the Data Protection Act they have the right to withhold their consent for their information to be shared *(see **What if consent is refused** below).* They also have the right to change their mind about disclosing information, at any time before disclosure is made or afterwards to prevent further disclosure taking place.

If information is to be shared for non- care purposes or outside of health and social care then explicit consent must always be sought.

Consent whether given, limited or withheld must be recorded. Where possible the patient must be given a copy of any written consent given by them, and a copy must be placed on the individual's file.

Under the Data Protection Act patients have a right to access their health records and amend any information that might be incorrect and as such must be informed of this.

<u>Children</u>

A child of 12 or over is normally assumed to have sufficient understanding and be competent to make a decision about access to their records, although some children under this age may also be competent to make this decision.

The decision on whether a child is competent must be made by the health professional that is currently responsible for providing the clinical care for the patient, failing that, a health professional that has the necessary skills and experience and is most suitable to advise on such matters. The Consent Policy will provide further information.

Capacity to give consent

Where there is evidence that a person does not have the capacity to give valid consent to disclose information, it is good practice to involve relatives or the person with legal

authority to act on their behalf with senior professionals in the decision making process. The Mental Capacity Act 5 Key Principles must also be taken into account.

What if consent is refused?
If a patient chooses not to give consent or to limit their consent it is legitimate to discuss the consequences of this with them i.e. that it may not be possible to provide certain services or that provision of services may be delayed. As such patients must be encouraged to discuss the potential implications of restricting access to their records so that they are able to make an informed choice.

Sharing information without consent
There are a number of circumstances where you may be justified in sharing information without the patient's consent.

Information may be shared without explicit consent where it is shared for medical purposes and the information is shared between health professionals. However it is still necessary to ensure that the patient is aware of how their information will be used and that they have a choice about whether their information must be shared.

Where there is evidence that significant harm would be caused to the service user, or to another if information was not shared. This includes issues relating to child, adult or public protection. Failure to do so could be viewed as failure of the organisation to discharge their duty of care, particularly if there is resultant harm.

Where sharing is necessary, in the vital interests of the service user, or another person, this refers to life or death circumstances.

Where sharing is necessary for the prevention or detection of crime or the apprehension or prosecution of offenders, personal information may be provided to the Police under Section 115 of the Crime and Disorder Act.
Section 115 does not impose a requirement to exchange information and responsibility for the disclosure remains with the agency that holds the data. However, information given in confidence must not be disclosed unless there is a clear overriding public interest in doing so. Where possible information must be anonymised before being shared without consent.

A written record must be made whenever information is shared without consent giving details of the grounds for the decision.

Information for patients
The Confederation's poster and leaflet on the use of personal information must be displayed in all receptions and patient areas and leaflets must be included in all patient correspondence.

If a patient requires a more detailed explanation about how their information may be used staff must provide them with contact details of the Patient Experience team, a Senior Manager able to deal with the query or Information Governance Team. Or if the patient prefers staff must arrange for a Senior Manager or member of IG Team to contact the patient to discuss their concerns.

Further advice
Specialist advice must be sought if there is any uncertainty regarding the appropriateness using any of the above justifications for sharing information. Advice must be sought from a Senior Manager, or the Information Governance Team.

APPENDIX C - Reporting of policy breaches

What must be reported?

Misuses of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches must be reported in line with the Leeds GP Confederation Incident Reporting Policy and recorded on Datix. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they must discuss their concerns with their line manager. The following list gives examples of breaches of this policy which must be reported:

- Sharing of passwords
- Unauthorised access to the Leeds GP Confederation systems either by staff or a third party
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know
- Disclosure of personal data to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and NHS Code of Confidentiality
- Sending data in a way that breaches confidentiality
- Leaving confidential information lying around in public area
- Theft or loss of patient-identifiable information
- Disposal of confidential information in a way that breaches confidentiality i.e. disposing of patient record and or content of, in ordinary waste paper bin.

Reporting procedure for breaches identified by a staff member

If possible you must raise your concerns initially with the individual(s) concerned in the alleged breach and attempt to informally resolve the problem. If you and the individual concerned believe that there has been a policy breach, the relevant Line Manager must be made aware of the issue and the proposed resolution. After the issue has been acknowledged and appropriately dealt with, the Line Manager must complete the Leeds GP Confederation Incident Reporting Form.
Advice from relevant officers such as the Information Governance staff must be sought if you are unsure what would constitute a breach or when additional guidance is required when addressing resolution of breaches.

Reporting procedures for complaints made by member of the public

Where a member of the public has made a complaint, the Complaints Procedure must be followed and the Line Manager who has received the complaint must fill in Leeds GP Confederation Incident Reporting Form.

Appendix D – Confidentiality Agreement for System Administrators

This agreement describes the responsibilities of System Administrators under the NHS Confidentiality Code of Practice 2003 and the Data Protection Act 1998 when undertaking work for the Leeds General Practice Confederation (GP Confederation).

The GP Confederation is under common law duty to ensure that confidential information is protected from inappropriate disclosure.
Furthermore, under Principle 1 of the Data Protection Act 1998 personal information must be processed (disclosed) lawfully. The GP Confederation will only be able to comply with these conditions where it has ensured that system administrators are subject to, and comply with, patient confidentiality, information security, freedom of information and data protection requirements.

What is confidential information?

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician; colleagues to colleague; employee to employer; commissioner to contractor) in circumstances where it is reasonable to expect that information will be held in confidence. It:

- Is a legal obligation that is derived in case law.
- Is a requirement established within professional codes of conduct.
- Must be included within NHS employment contracts as a requirement linked to disciplinary procedures.

The public entrust the NHS with, or allow us to gather, sensitive information relating to the clinical and business activities of the NHS.
They do so in confidence and they have a legitimate expectation that all persons who may be exposed to, or process information will respect the confidentially of that information and act appropriately. It is essential, if the legal requirements are to be met and the trust of the public retained, that the NHS provides, and is seen to provide, a confidential services in all of clinical and business activities.

GP Confederation Responsibilities:

- The GP Confederation must take all reasonable steps to ensure that system administrators comply with their contractual obligations to keep personal information secure and confidential.
- In addition to the contractual performance requirements above, the GP Confederation must also ensure that system administrators are aware of the possible impact of the Freedom of Information Act 2000.

Related legislation

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Confidentiality: NHS Code of Practice 2003
- Caldicott Principles
- Common Law Duty of Confidentiality
- Code of Conduct for Employees in Respect of Confidentiality

Staff Responsibilities

a. Staff must ensure that they have read and comply with the Code of Conduct for

Employees in Respect of Confidentiality and other relevant Information Governance policies and procedures.

b. Staff must keep all information which they are required to access in connection with their role for the GP Confederation secure at all times and shall only process such data in accordance with instructions received from the GP Confederation.

c. Staff must be aware of the possible impact of the Freedom of Information Act 2000 on the confidential information connected with their role & responsibilities.

d. Data will, at all times, remain the property of the GP Confederation and must be returned in its entirety on termination of employment.

e. Under the Data Protection Act 1998 a breach of confidentiality may constitute an offence which may lead to a prosecution.

Statement of Confidentiality

I (Name) ……..……..

Am aware of the relevant legislation, best practice guidelines and related GP Confederation policies and procedures and agree that:

I understand within the course of my work the GP Confederation; I may have access to or hear confidential information about patients, members of staff or other business activities of the GP Confederation or other organisations.

I understand that no information of a personal or confidential nature concerning individuals or the Trust may be disclosed without proper authority having first been given.

I understand that failure to comply with the above rules will be regarded as serious misconduct, which could result in action being taken against myself or from legal action by others.

PRINT NAME:

SIGNATURE:

DATE:

ON BEHALF OF THE LEEDS GP CONFEDERATION

MANAGER'S NAME:

JOB TITLE

SIGNATURE:

DATE:

NB. This document must be retained with other documentation pertaining to the staff member's contract of employment

Policy Consultation Process

Title of Document	Confidentiality Code of Conduct
Author (s)	Head of Information Governance, LCH (former), Head of Development and Governance
New / Revised Document	Revised
Lists of persons involved in developing the policy	Head of Development and Governance
List of persons involved in the consultation process	Corporate Committee