WARWICKSHIRE COUNTY COUNCIL

Confidential and Personal Information: A Code of Practice

Information Governance Team
Warwickshire County Council
www.warwickshire.gov.uk/informationmanagement
01926 418633

Version 8
January 2014
WCC-Public

© 2014 Warwickshire County Council

Contents

Foreword **4**
Introduction **4**
Why we need a Code of Practice 4
The Aims of the Code of Practice 4
Who the Code of Practice applies to 5
Whose information? 5
Your responsibilities 5
A. Confidentiality **6**
Confidentiality - the legal framework 6
The Duty of Confidence 6
The Data Protection Act 1998 6
The Human Rights Act 1998 6
Administrative law 6
The Caldicott Guardian and Caldicott Principles 7
B. Providing a Confidential Service **8**
The Confidentiality Model 8
Protecting service user information 8
Keeping service user information private 8
Keeping information physically and electronically secure 9
Recording service user information accurately and consistently 9
Informing service users 9
Providing choice 10
Openness with service users, their carers and families 10
Exceptions to openness 11
Special Situations 11
Confidentiality and children 11
Customers lacking mental capacity 11
Confidentiality and the deceased 11
Sexually transmitted diseases 11
Those who want access to their records 12
Improvements to the confidential service 12
C. Using and Disclosing Confidential Service User Information **13**
Disclosure with care 13

Disclosure with consent....13
Disclosure without consent....14
The form of consent....14
Key questions for disclosure decisions....15
Disclosure and child protection....16
Disclosure about Sex Offenders....16
Appendix I: The Data Protection Principles....17
Appendix II Caldicott Principles and Guardian....21
The Caldicott Principles....21
The Role of the Caldicott Guardian....21
Short Glossary of Terms....23
Appendix III Seven golden rules for information sharing....24

Foreword

Public awareness and concern about the information governance issues behind confidentiality breaches and identity theft has never been higher, but the other side of this is that confidentiality and data protection law is often quoted as a barrier to information being effectively used and shared to provide services or to protect the vulnerable and people at risk.

In fact, the legislation is not designed to make access to information difficult, but simply requires you to assess whether you have obtained, used and disclosed service users' information fairly in accordance with their rights. If you are clear on how to do this, in a balanced way with reference to risks, and this becomes integral to your approach, then you will begin to see how good information governance can make a positive contribution to both maintaining service users' rights and ensuring information can be used and shared effectively.

The adoption of this Code of Practice is a significant step forward towards achieving this.

Introduction

This Code of Practice details the expected standards for the collection and use of confidential personal information. It is one of the key documents in the Warwickshire County Council Information Governance Framework, the standard for managing confidentiality and access to information. It should be used together with other information policies and standards that define how information should be handled.

Why we need a Code of Practice

Across its services Warwickshire County Council receives a range of personal information about service users. Some of this is very intimate information provided in connection with social care or other personal services. The service users are sometimes very vulnerable and rely on us for essential, and sometimes very personal, help. They provide us with the personal details we say we require to understand their needs, and they trust us to handle what they tell us responsibly and respectfully.

All of us in public service have a legal duty of confidence to service users, their families and others with whom work brings us into contact. This means when a member of the public gives us information that is not generally available, they have the legitimate expectation that it will remain confidential.

Individuals, not just organisations, can personally be held legally responsible for the unauthorised obtaining, recording, holding, using, changing, disclosing or sharing, or destroying of personal information, so everyone who handles confidential personal or sensitive information because of their role in social care or providing personal services needs to know how to do it properly.

The Aims of the Code of Practice

This document gives details of the required practice relating to the confidentiality of information provided by individuals and organisations to support the delivery of services. It deals primarily with service users' personal information and their rights in relation to this, but the confidentially of information provided by others is also covered. Its aims are to:

- Ensure that you respect the confidentiality of people who give, or are subject of, information, and protect their rights in relation to their personal information;

- Make clear what the legal and good practice requirements are for those handling personal or confidential information on behalf of the Council; and

- Help you handle personal information safely on behalf of the Council and make appropriate decisions in relation to personal information.

Please look at the Information Security policy, the Protective Marking, Handling and Disposal policy and other guidance, such as the Information Security Staff Guide for more detailed support.

Who the Code of Practice applies to

It applies to everyone, especially in health and social care, who in relation to the work of Warwickshire County Council, has anything to do with confidential and sensitive personal information, whether they are:

- managers and supervisors
- practitioners and student practitioners
- support, clerical and administrative staff
- other voluntary, sessional, support and ancillary staff
- agency, temporary, seconded, locum or contract staff
- foster and day carers
- researchers.

Whose information?

The Code does not cover non-personal information such as sensitive business or commercial information. It does cover, within a social care or personal service context:

- all personal information relating to identifiable living individuals;
- personal information relating to deceased people; and
- information given in confidence by third parties.

Your responsibilities

It is the responsibility of everyone handling personal information to ensure that it is:

- held securely and confidentially;
- obtained fairly and efficiently;
- recorded accurately and reliably;
- used effectively and ethically; and
- shared appropriately and lawfully.

Everyone who receives or uses sensitive or confidential personal information as part of the delivery of social or personal care is required to comply with this Code.

A. Confidentiality

This part of the Code of Practice sets out the legal basis of confidentiality, personal information and privacy.

Confidentiality - the legal framework

The rules on confidentiality, privacy and the need to safeguard personal information arise from both legislation and case law. These enshrine the need for fair and ethical treatment of information where there is a duty of confidence, issues of privacy or where personal information is involved.

The Duty of Confidence

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that information will be held in confidence. It is a legal obligation that is derived from case law and a requirement established within professional codes of conduct. In such circumstances the information should only be disclosed:

- with the permission of the provider; or,
- if the confidentiality requirement is overridden by legislation; or,
- if an effective case that it is 'in the public interest' can be made.

The Data Protection Act 1998

The Data Protection Act requires anyone who handles the personal information of living individuals to comply with eight data protection principles. It also gives individuals rights over their personal information. In assessing whether you are handling personal data within the law, these principles are critical and the most important of them are:

- the 1st Principle, which requires processing to be fair and lawful and requires criteria to be met to achieve this;
- the 2nd Principle, which requires personal data to be processed for one or more lawful purposes;
- the 7th Principle, which requires personal data to be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The full set of Data Protection Principles are shown in Appendix I.

The Human Rights Act 1998

Article 8 specifies the right to 'respect for private and family life'. Privacy is a fundamental human right, which only compelling reasons of others' rights and freedom, or of public interest can override.

Administrative law

A public authority must possess the powers to carry out what it intends to. These powers are given by statute and are consistent with the purposes for which the public authority

exists. If these powers are exceeded its action is 'ultra vires' or beyond its power and therefore illegal. In these circumstances, the obtaining of personal information would not be for a lawful purpose under the Data Protection Act and therefore a breach of the First Data Protection Principle.

The Caldicott Guardian and Caldicott Principles

The 1997 Caldicott Report and the subsequent 2013 Caldicott 2 Review made recommendations for regulating the use and transfer of patient-identifiable information between NHS organisations in England and non-NHS bodies. These recommendations were subsequently extended into Councils with social services responsibilities.

The protection and use of information largely collected from service users by health professionals and social care workers, in confidence, is a part of the overall quality of care and the aim under the recommendations of Caldicott was to ensure that confidential information was shared only for justified purposes and that only the minimum necessary information was shared in each case. A set of Caldicott Principles were defined to support this, but central to the recommendations was the appointment of a Caldicott Guardian to oversee the arrangements for the use and sharing of confidential information. The Caldicott Guardian should:

- act as the 'conscience' of the organisation, actively supporting work to facilitate and enable information sharing and advising on options for lawful and ethical processing of information as required; and

- have a strategic role that involves representing Information Governance requirements and issues at board/management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

Appendix II shows the Caldicott principles and describes the role of the Caldicott Guardian.

B. Providing a Confidential Service

This section of the Code of Practice addresses how a confidential service can be provided. It is the aim of this organisation to provide a confidential service that reflects the confidentiality attributes of the information that we gather, use and share to provide our services.

The Confidentiality Model

The confidentiality model consists of four main requirements which are interlinked and aid the improvement of a confidential service. These are:

PROTECT: look after the subjects confidential information;

INFORM: ensure subjects are aware of how their information is used;

PROVIDE CHOICE: allow subject to decide whether their information can be disclosed or used in particular ways.

Supporting these is:

IMPROVE: always look for better ways to protect information and provide choice.

There are a number of issues that you must address in order to do this, and these are given below.

Protecting service user information

All staff members are responsible for safeguarding information at all times in accordance with WCC security policies which are available on the intranet.

This is an obligation for all those using confidential personal information. Breach of confidence, inappropriate use of service user records or abuse of computer systems may lead to disciplinary measures, bring into question professional registration and possibly result in legal proceedings against the individual involved.

PLEASE NOTE that accessing, obtaining or disclosing personal information from the County Council's databases such as Care First for personal use is a serious breach of security and will be regarded as Gross Misconduct under the Council's Dismissal and Disciplinary Procedure and may lead to dismissal. It is also a criminal offence under the Data Protection Act 1998 and if convicted you could face a fine of up to £5000 if the case is heard in the Magistrates Court or an unlimited fine if the case is heard in the Crown Court. It is therefore critical that you are familiar with the Council's security policies and that you uphold these at all times. (*See Information Security policy, other associated security policies and Employer and Employees responsibilities*)

Keeping service user information private

You must take appropriate steps to keep information private. This includes, for example, not gossiping about service users, which is an improper use of confidential information, and taking care when discussing cases in public. Disclosure is not just intentionally telling someone. Unless appropriate measures are taken you risk unintentional disclosure by:

- insecure posting, faxing, showing, e-mailing, giving written information;
- leaving information open to view;
- not locking it away properly; and/or
- showing a record that includes someone else's personal information.

The Information Security Staff guide gives further information on the steps that you should take to protect confidential information from unintentional disclosure.

Keeping information physically and electronically secure

This covers both manual and electronic information. Do not leave portable computers, or personal files or notes in unattended cars or in easily accessible areas even for a short while. Ideally lock away all files and portable equipment when not in use. If you take information home, or where the workplace is the home, then whether in files or stored electronically you must comply with the Information Security Staff guide.

Recording service user information accurately and consistently

Adherence to recording standards is essential if proper information is to be maintained. Inaccurate information can lead to incorrect decisions and poor service. Inconsistent information is difficult to interpret and can result in delays and errors. Efforts to ensure the confidential treatment of information will be undermined if that information is inaccurate. For social care records there are existing policies that set out the recording requirements for electronic and manual records. If you maintain records like these where sensitive personal information is kept then you should be aware of these policies. (*see Case Recording Policies on the document library)*

Informing service users

To obtain information fairly and lawfully you must clearly explain to people at the outset: who you are, why you need their information, what you might do with it and types of people you might share it with in order to provide them with services. Consider whether people would be surprised to learn that their information was being used in a particular way – if so, then they have not been properly informed.

The steps that you should take to ensure that people are properly informed are to:

- check that leaflets on confidentiality and information disclosure have been provided and that these have been read and understood. For example, 'Did you have a chance to look at the leaflet and did you have any questions?

- Let people know that we abide by the Social Care Record Guarantee which describes how we use their information for providing social care and keep it safe. This can be found on the Warwickshire County Council website or we can provide copies.

- make clear to people when information is being recorded or personal records accessed, For example, 'Let me just note that on your file.'

- make clear to people when you are or will be disclosing information to others. For example, 'I will telephone your health visitor and let her know what we have just agreed'.

- that when you promise confidentiality, you must be clear that it does not mean just between you and them (see rules for HIV status under Sexually Transmitted Diseases below), but that you will discuss it with your supervisor, someone else will type it, a senior manager may need to make a decision; so confidential means within the organisation, among those needing to know.

- make people aware that there can be exceptional circumstances, for example when required by the law or considerations of personal safety, when WCC can be required to disclose confidential information to others. You should normally tell them when this occurs.

- ensure that people are aware of the choices available to them in respect of how their information may be disclosed and used. They are also entitled to change their mind.

- ensure that people's concerns or queries about how their information is disclosed and used are properly addressed.

- respect the rights of subjects and help them to have access to their personal records, these are the subjects' right under the Data Protection Act 1998.

- ensure that you communicate effectively with people. Some may be reluctant to read leaflets because of disability, illiteracy, cultural issues or language difficulties. You have an obligation to help people understand.

Providing choice

There are three aspects to providing choice in the way that information is used. These are:

- Ask subjects for their consent before using their personal information in ways that do not directly contribute to their care or support;

- Respect decisions to restrict the disclosure or use of information. You might wish to explain the safeguards that exist, such as sharing protocols, or investigate the possibility of making some compromise arrangement. Ensure that service user safety is not neglected because of such arrangements and keep a record of any agreements with the service user; and

- Explain the implications of disclosing and not disclosing, but make sure that these explanations are proportionate to the risk involved. It would be unfair to over- emphasize a risk in order to encourage a service user to consent to disclosure. Document any compromises to care that will result from an inability to disclose. You must make clear to the service user that they can change their mind.

Openness with service users, their carers and families

WCC has adopted the official and professional good practice guidance on openness with individual service user social care records. The purpose of this is to build confidence in the accuracy of records and to develop a sense of information ownership. In practice this involves:

- Customers and carers helping to write their own case record, particularly when preparing assessments, care plans or reports;

- Service users having regular access to their records (except for restricted or third party information);

- Sharing information more openly with the people it is about; and

- Routinely giving copies of key documents (such as assessments, care plans, reviews, reports) to their service users.

Exceptions to openness

Within the policy of openness, however, there are some types of information that you cannot make available. These are:

- Information about or from other people without their consent;
- Information that, if given, would hinder the prevention or detection of crime;
- The Data Protection (Subject Access Modification) (Social Work) Order 2000 exempts access if it would cause serious harm to someone's health or wellbeing;
- The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 exempts access on: fertilisation & embryology; Adoption & Parental Orders; educational needs statements; Scottish children's hearings.

Special Situations

Confidentiality and children

Children are entitled to the same duty of confidence as adults, provided those under 16 years old can understand the choices and their consequences. In exceptional circumstances, for example where there is evidence of exploitation or abuse, confidentiality may be breached. If possible, you should discuss the need to breach confidentiality with the child beforehand, unless there is a risk of harm to the child by doing so. *(Refer to additional intranet guidance on the Fraser Guidelines).*

Customers lacking mental capacity

People lacking mental capacity have the same rights under the Data Protection Act as anyone else. There are effective methods of communicating with people with learning disabilities; the Information Commissioner's guidance, and good practice, requires you to make all reasonable efforts to consult them. Most will be perfectly capable of understanding issues about their privacy and consent. There is no universal definition of mental capacity. The Department of Health describes a person with capacity as someone able to understand, retain and weigh up information relevant to the decision and its consequences.

See the Mental Capacity Act: Code of practice which gives advice on how to ascertain if people have mental capacity and if not how to proceed. This document can be found on the intranet.

Confidentiality and the deceased

When an individual has died, it is unlikely that information relating to that individual remains legally confidential. However when they were alive, the people whose information we hold and use, gave it to us on the understanding that we owed them a duty of confidence. Their information was private, intimate, sensitive. Good practice and our public duty of confidence requires us to respect the confidentiality of those who have died, as we do that of living people.

Sexually transmitted diseases

Our policy is to follow the **NHS Trusts and Primary Care Trusts (Sexually transmitted diseases) Directions 2000** and the obligation of complete confidentiality about anyone's

sexually transmitted disease. This includes HIV status. It means if someone tells you they have HIV/AIDS, it is strictly confidential to you, not to be recorded or shared more widely within the department. If you need to discuss someone's status with another employee or agency, to provide a service or benefit to them, you must have their explicit consent to do so.

Those who want access to their records

Whilst openness and transparency should negate the need for people to ask for access to their records, it is their right to make a request if they wish to do so.

Please see the 'DPA Subject Access Guidance' on the intranet which gives advice on how to deal with a subject access request and also covers when an access to records request is sent by an agent acting on behalf of the subject, when information is requested on a deceased person and requests for information made by the police.

Improvements to the confidential service

All staff should be committed to the improvement of the confidential service, by ensuring that:

- They seek training and support to understand and implement this Code of Practice and the Information Security Staff guide; and
- They report possible breaches or risk of breaches of this Code of Practice to their manager, the ICT Service desk as appropriate.

C. Using and Disclosing Confidential Service User Information

This part of the Code of Practice deals with the steps necessary to ensure that using and disclosing confidential information is fair and legal.

Disclosure with care

Information sharing protocols

Follow any established information sharing protocols. WCC is updating and developing information sharing protocols that set out the standards and procedures that apply when disclosing confidential service user information with other organisations and agencies. Staff must work within these protocols where they are available and within this code of practice where they are absent or do not address the issue.

Identify enquirers

Protect service user information from unauthorised access by ensuring that you check the identity of people requesting information. Seek official identification or ring them back via a switchboard or a number that can be verified. Check also that they have a right to have access to the information.

Emails, faxes and mail

When confidential information is transferred between locations or organisations it must be by a secure means and not subject to unintentional disclosure. The Information Security Staff guide provides more details on safe transmission but please also refer to the other Corporate Security policies and the Protective marking policy.

Share the minimum necessary to provide the service or satisfy other purposes

The Caldicott Principles (see Appendix II) established this as an approach, but staff must also be aware that a balance must be struck here. Sufficient information must be provided to allow the service to be effectively provided, or in a more serious case to prevent someone being put unnecessarily at risk.

Disclosure with consent

When you have properly informed the subject about how you intend or need to use their personal information, you should then wherever possible obtain their consent to do so. People rarely refuse, if they are adequately consulted and informed. However, you should bear in mind that:

- people have the right to change their mind and withdraw consent; and
- obtaining consent is not a one off exercise. If circumstances substantially change then the person should be told and fresh consent sought.

Disclosure without consent

If you cannot obtain the person's consent, but still need the information, then you must have another legal basis on which to obtain and use the information. The First Principle of the Data Protection Act 1998 sets out the specific circumstances where this can be done.

The law permits disclosure without consent if it is necessary to safeguard someone. The public interest, for example, in child protection or mental health cases may override the public interest in maintaining confidentiality. You must be able to justify disclosure in each case, and get legal advice if in doubt.

The law also allows for disclosure without the person's consent: if there is a court order; for the prevention or detection of crime; or the apprehension or prosecution of offenders, where non-disclosure would be likely to prejudice those objectives.

When agencies have a valid need to share information regularly with each other, the best way of ensuring that it is properly handled is to work within carefully worked out information protocols between the agencies involved, and to take legal advice in individual cases where necessary.

Finally the big advantage of obtaining the subject's informed consent is that you can ensure that you are always acting legally and in the process of obtaining that consent you are being open about your intentions. This is the preferred approach and best practice.

The form of consent

Consent for non-sensitive information

Consent does not always have to be written in order to use information. You can judge the individual circumstances whether to seek signed or verbal consent. If verbal, you should clearly record the details. In some circumstances written consent might be better: at the beginning; when working with children and vulnerable adults; or if circumstances are complicated or volatile. It gives people something clear to refer to again later. Verbal consent might be better: when a good working relationship is established; to avoid appearing unduly bureaucratic if there is other paperwork to deal with; or when an intended disclosure is straightforward and welcome.

Consent for disclosure of sensitive personal information

Explicit consent is required, in writing, for the disclosure of sensitive personal information. Sensitive personal information is defined by the Data Protection Act as information about:

- Racial or ethnic origin;
- Political opinions;
- Religious or other beliefs of a similar nature;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life (including sexual orientation and sexually transmitted diseases);

- Committed or alleged offences (we have a valid interest in Schedule 1 Offenders, Child Protection, the background of employees and foster carers); and

- Pre-trial/court proceedings, sentences & disposals.

Key questions for disclosure decisions

Q. If the purpose served by disclosing is not consistent with the purpose for which the information was obtained, under what power is the information to be disclosed?
A. Public bodies should only do things they have been set up to do and obtain information for specified purposes. These are permitted, but disclosure to other bodies for other purposes may not be. Ensure that you know under what power the information will be legally disclosed or seek advice.
Q. Is the disclosure a statutory requirement or required by order of a court?
A. Disclosure must be complied with, although in exceptional circumstances there could be scope to ask the court to amend an order.
Q. Is the disclosure required to support the provision of the service or to assure the quality of that service?
A. Sometimes information must be shared in order to provide a service or improve the quality of service within the department, for example for performance audit purposes. Check that the service user understands this and what the limits of confidentiality are, address any concerns, and honour any objections they may raise if possible. Where you do this you do not need to seek explicit consent each time you share information.
Q. Is the disclosure to support a broader service purpose?
A. Examples of this are where service user information is used for research purposes. The explicit consent of service users must be sought unless: disclosure is justified in the public interest, is required by law, or the information has been anonymised.
Q. Have appropriate steps been taken to inform service users about the proposed disclosures?
A. There is a legal requirement to inform service users in general terms, about who sees information about them and for what purposes. Where the purpose of providing information is to seek consent then details are required and service users need to be made aware of their rights and how to exercise them.
Q. Is the explicit consent of a service user needed for a disclosure to be lawful?
A. Explicit consent is required to disclose 'sensitive information' (as defined in DPA1998 see Appendix II) unless: an overriding 'public interest' case can be made; or the disclosure is required by the courts; or there is risk of harm to someone.

Disclosure and child protection

Where there are concerns that a child (or vulnerable adult) may be suffering significant harm, it's essential for professionals and relevant others to share information.

"In deciding whether there is a need to share information, professionals need to consider their legal obligations, including whether they have a duty of confidentiality to the child. Where there is such a duty, the professional may lawfully share information if the child consents or if there is a public interest of sufficient force. This must be judged by the professional on the facts of each case. Where there is a clear risk of significant harm to a child, or serious harm to adults, the public interest test will almost certainly be satisfied. However, there will be other cases where practitioners will be justified in sharing some confidential information in order to make decisions on sharing further information or taking action – the information shared should be proportionate…. Assessing the needs of a child and the capacity of their parents or wider family network adequately to ensure their safety, health and development very often depends on building a picture of the child's situation on the basis of information from many sources."
(Working Together to Safeguard Children: a guide to inter- agency working to safeguard and promote the welfare of children, 2006)

Unless to do so would place a child at increased risk, the nature of the child protection concerns should be explained to family members and to children, where appropriate, and their consent to contact other agencies sought. This requires careful explanation in plain language. It may be helpful to have written as well as verbal explanations. Children's Services must make sure both children and adults have all the information they need to help them understand child protection processes. Information should be clear and in everyday language, available in the family's first language where needed.

Disclosure about Sex Offenders

Disclosure of information should always take place under the terms of the inter-agency protocol, and integrated into a risk assessment and management system. Each case should be judged on its merits, taking account of the degree of risk.

Appendix I: The Data Protection Principles

The First Principle- Fairly and lawfully

Personal data shall be processed fairly and lawfully

You must clearly explain to people at the outset: who you are, why you need their information, what you might do with it, types of people you might share it with and anything else relevant to their specific circumstances. If informants are third parties, you must ensure that data subjects are appropriately informed as soon as possible. If you are authorised, or legally obliged, to supply information, then you have fairly obtained it.

Conditions

You must satisfy at least one of the following conditions:

a) The data subject freely gave **specific, informed consent**;
b) It is necessary to meet or set up a contract with the data subject;
c) You have to do it to comply with a legal obligation;
d) It is necessary to protect the vital (life-threatening) interests of the data subject;
e) It is necessary for the administration of justice, a legal duty, government requirement or a public function in the public interest;
f) It is necessary for our own legitimate purposes, so long as they don't conflict with the rights and freedoms of the data subject (most common condition).

Sensitive personal information

Sensitive personal information is defined by the Data Protection Act as information about:

- Racial or ethnic origin;
- Political opinions;
- Religious or other beliefs of a similar nature;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life (including sexual orientation and sexually transmitted diseases);
- Committed or alleged offences (we have a valid interest in Schedule 1 Offenders, Child Protection, the background of employees and foster carers); and
- Pre-trial/court proceedings, sentences & disposals.

Additional conditions for processing sensitive data

To process it, on top of the previous conditions, you must **also** satisfy at least one of these:

a) the data subject gave **explicit consent**;

b) employment law legally entitles or obliges us to do it;

c) you are protecting someone's vital interests & can't reasonably get consent;

d) political, philosophical, religious and Trade Union organisations processing members' details;

e) the data subject has deliberately made it public;

f) you have to do it in connection with legal proceedings and preparing for them;

g) It is in the substantial public interest and is necessary:

- to prevent or detect unlawful acts, where to get consent would undermine this;
- to carry out our duty to protect people from dishonesty, malpractice, other seriously improper conduct, unfitness, incompetence or mismanagement, where to seek the data subject's explicit consent would interfere with that function;
- to carry out our work of counselling, advising, supporting or providing services, where to seek the data subject's explicit consent would interfere with those services, or isn't possible or reasonable;
- for research purposes.

h) It is a legal obligation or government requirement;

i) It is necessary for medical purposes normally by health professionals, or exceptionally by others who owe the same duty of confidence as they do;

j) In relation to racial or ethnic origin, if it is in connection with promoting and maintaining Equal Opportunities policies.

The Second Principle - Specified and lawful purposes

Personal data shall be obtained only for one or more specified and lawful purposes and shall not be used for purposes incompatible with these.

You cannot record anything you like; we have to notify (and may need to justify) our notified purposes to the Information Commissioner, along with the types of data subjects and personal data concerned, and people we might disclose it to. Purposes are set types of activity to do with personal information (there is one for Social Work, for example). You can only process within these limits. Our full registered Purposes are on the ICO website.

The Third Principle - Adequate for purpose

Personal data shall be adequate, relevant and not excessive.

You should not record information on a "just in case" basis, or disclose it, without reference to its necessity or relevance to the Department's legitimate business.

The Fourth Principle - Accuracy

Personal data shall be accurate and kept up to date.

In addition to the general requirement to process accurate and up-to-date information, the Act places an onus on us to verify the accuracy of third party information.

The Fifth Principle - No longer than necessary

Personal data shall not be kept for longer than is necessary.

The Retention, Storage & Destruction Policy sets timescales for keeping personal information.

The Sixth Principle - The rights of the data subject

Personal data shall be processed in accordance with the rights of data subjects. Data subjects are entitled:

- To know that we process their information;
- To know what information we process, why, and who we might disclose it to;
- To give or refuse consent to our disclosing their information to others. There are a few, exceptional circumstances where consent is not necessary, or where we can override
  a refusal;
- To have access to it, with some limited exceptions, within 40 days (not 40 working days) and in a form they can understand, and to have a permanent copy of it as it was at the time they asked for it;
- To challenge its accuracy or relevance, and have us correct or erase it within 21 days;
- To have us tell third parties we gave the inaccurate or irrelevant information to, of the correction or erasure, so we must clearly record who we told;
- To stop processing that is likely to cause damage or distress, and to compensation if injured by our processing their personal information;
- To know the logic of decisions entirely based on automated processing: for example, if charges are solely calculated by computer, people are entitled to know how that automated calculation works;
- To privacy for their personal information.

The Seventh Principle – Security measures

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing and against accidental loss or destruction.

Measures must ensure a level of security appropriate to the nature of the data and the harm that might result from a breach of security. It means:

- Being confident in the reliability of employees with access to personal data;
- Recruiting, inducting, supervising and training staff to appropriate security standards;
- Satisfying ourselves about the security of people we disclose information to, from other agencies to contractors servicing equipment or removing confidential waste;
- Siting computers, printers, fax machines, photocopiers, papers where

personal information can't be seen by unauthorised people;

- Turning equipment off and locking papers away when unattended;
- Complying with departmental requirements on logging on and off computers, accessing software applications and safeguarding passwords;
- Complying with corporate and departmental instructions: on confidentiality, using computers, internet and e-mail use, working at home (computers or paper records); back-up procedures; retention, storage & destruction of records; fire safety; and
- Only disclosing personal information to those we are legally entitled to tell.

The Eighth Principle - Transfer outside the EU

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix II Caldicott Principles and Guardian

The Caldicott Principles

The Caldicott Report set out a number of general principles that health and social care organisations should use when reviewing its use of client information and these are set out below:

Justify the purpose(s)

Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

Do not use personally identifiable information unless it is absolutely necessary.

Personally identifiable information items should not be used unless there is no alternative.

Use the minimum personally identifiable information.

Where the use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

Access to personally identifiable information should be on a strict need to know basis.

Only those individuals who need access to personally identifiable information should have access to it.

Everyone should be aware of their responsibilities.

Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect patient/client confidentiality.

Understand and comply with the law.

Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

The duty to share information can be as important as the duty to protect patient confidentiality.

Sharing in the best interest of the patient within the framework set out by these principles.

The Role of the Caldicott Guardian

The Caldicott Guardian's Role is strategic, advisory and facilitative as follows:

1. Oversee the protection and use of service user information;

2. Raising awareness for security across the organisation;

3. Developing and agreeing information sharing protocols for information sharing with other organisations;

4. Responsible for agreeing and reviewing internal and external protocols, ensuring that they address national guidance policy and law and that their operation is monitored. Protocols should underpin and facilitate the development of cross boundary working;

5. Determining levels of access to information systems;

6. Enforcing strict need to know principles;

7. Reviewing and justifying the use of service user identifiable information;

8. Making improvements to:

    a. database design
    b. staff induction
    c. training
    d. staff compliance with guidance;

9. Strategic role in developing the security and confidentiality policy representing confidentiality requirements at board level;

10. Responsible for continuous improvement of confidentiality and security procedures;

11. Overseeing the completion of the Information Governance Framework Toolkit relating to the Caldicott Guardian's responsibilities;

12. Agreeing annual improvement plans;

13. Monitoring practical standards against annual improvement plans to ensure year on year improvement; and

14. Liaising closely with ICT Security, Data Protection and FOI Officers and others charged with similar responsibilities so that nothing is overlooked.

Short Glossary of Terms

Confidential information	Within this document confidential information refers to all personal information and any information given 'in confidence' that is not generally known.
Personal information	Is information relating to living and identifiable people only.
Processing	Is a data protection term meaning anything we do with information from collection to disposal.
Purpose	A data protection term. When we obtain personal information we must say why we need that information and what we are going to do with it.
Notification	The organisation is obliged to notify the Information Commissioner's Officer of the purposes for which we hold personal data. This record may be inspected by the public. It is illegal for us to hold personal data without a notified purpose being recorded.
Information Safe Haven	The term *information safe haven* is a term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the safe haven principles. Basically these are procedures to ensure that confidential and personal information is handled safely at all times within the organisation.
Disclosure	Any time personal information is given to someone other than the subject
Subject or Data Subject	Under the Data Protection Act - the person that the personal information is about
Duty of Confidence	Our legal obligation under common law to keep secure information provided 'in confidence'
Third Party Information	Personal information **about** third parties that might be recorded on a file, but which the subject of the file is not entitled to see. Distinguish this from information **provided** by third parties where permission might be needed to disclose to the data subject.
Non relevant persons	People whose personal information should not be disclosed, because their role is incidental in service provision. For example, it might be unnecessary to record or disclose the name and home phone number of a clerk taking meeting minutes.
Ultra vires	If an organisation exceeds its statutory powers, it is acting unlawfully and *ultra vires.*
Legal power	Before disclosing personal or confidential information to an individual or organisation you must be sure under what legal power they are entitled to that information. For example the Police have powers under the prevention and pursuance of crime legislation to require access to information and there are protocols dealing with how this should operate.
Consent	Consent from the subject can be required to process personal information and also to disclose or share information.

Appendix III Seven golden rules for information sharing

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.

2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.