Sheffield Health and Social Care NHS
NHS Foundation Trust

Policy:
Confidentiality Code of Conduct

Executive or Associate Director lead	Clive Clarke
Policy author/ lead	SHSC Information Manager
Feedback on implementation to	SHSC Information Manager

Document type	Policy
Document status	Final
Date of initial draft	9 February 2015
Date of consultation	February 2015
Date of verification	20 March 2015
Date of ratification	8 September 2016
Ratified by	Executive Directors Group
Date of issue	14 September 2016
Date for review	31 March 2019

Target audience	All SHSC Staff

Keywords	Confidentiality, Security, Disclosure, Consent

Policy Version and advice on document history, availability and storage

This is version 3 of this policy. This version replaces version 2. This version was reviewed as part of the on-going policy development and review process.

This policy is available to all staff via the Sheffield Health & Social Care NHS Foundation Trust Intranet and on the Trust's website. The previous version has been removed from the Intranet and Trust website and archived. Word and pdf copies of the current and the previous version of this policy are available via the Director of Corporate Governance.

Any printed copies of the previous version (V2) should be destroyed and if a hard copy is required, it should be replaced with this version.

Contents

Section		Page
	Flow Chart	N/A
1	Introduction	3
2	Scope	3
3	Definitions	4
4	Purpose	5
5	Duties	5
6	Process – i.e. Specific details of processes to be followed	5
7	Dissemination, storage and archiving	18
8	Training and other resource implications	18
9	Audit, monitoring and review	19
10	Implementation plan	19
11	Links to other policies, standards and legislation (associated documents)	20
12	Contact details	20
13	References	20
	Appendix A – Version Control and Amendment Log	21
	Appendix B – Dissemination Record	22
	Appendix C – Equality Impact Assessment Form	23
	Appendix D - Human Rights Act Assessment Checklist	25
	Appendix E – Development, Consultation and Verification Record	27
	Appendix F – Policy Checklist	28

1. Introduction

This Code of Conduct has been developed as a guide for staff and others working on Sheffield Health and Social Care NHS Foundation Trust (SHSC) business to the required standards of good practice in relation to providing a confidential service.

In delivering effective treatment and care, SHSC processes (obtains, holds, uses and discloses) confidential information. Confidential information may be:

- Information about named individuals (including service users, members of staff or other third parties)
- Information about SHSC or other health or social care organisations (such as financial or risk records)

Keeping information confidential is not the same as keeping it secret. It is essential that relevant confidential information is available to those who have a need to know it in order to do their work.

Confidential information should only be used for the purpose(s) it was provided for, which the individual has been informed about and has consented to unless there are exceptional circumstances.

This code sets out the principles for handling confidential information and explains what this means in practice. It is based on the NHS Confidentiality Code of Practice published by the Department of Health.

2. Scope

This code of conduct applies to all SHSC employees and non-Trust employees who work within SHSC or under contract to it. This includes, but is not limited to, all staff, whether directly employed, seconded, on honorary contracts, permanent or temporary, also agency staff, non-executive directors, students on placement and people working in a voluntary capacity.

For convenience, the term ‘staff’ is used in this document to refer to all those to whom the code of conduct applies.

The Code relates to the requirements that must be met in order to provide service users, staff and others with a confidential service. It is based around the four main requirements of the Confidentiality Model which is at the heart of the NHS Confidentiality Code of Practice. Further information about the Confidentiality Model can be found in Appendix A.

Although the Model and its requirements were written primarily for the handling of service user information, the Model’s four requirements apply to the handling of all personal information including staff, service user and carer information. The requirements in relation to confidential information are:

1. Protect - look after personal information
2. Inform - ensure that individuals are made aware of how the information they provide is used
3. Provide choice - allow individuals to decide whether their information can be disclosed or used in particular ways
4. Improve - always look for better ways to protect, inform and provide choice

The principles in section 6 are a synthesis of this model with the addition of accepted good practice.

The duty of confidentiality for all staff arises out of common law, legal obligations, staff employment contracts and professional obligations. This duty continues after the staff member no longer works for or has an association with SHSC.

Any breaches of this code including unauthorised breaches of confidentiality, inappropriate Access to or use of personal health records or abuse of computer systems will be treated as a disciplinary offence, which may result in your employment, or association, with the Trust being terminated. It may also have consequences for professional registration and possibly result in legal proceedings.

If you have concerns regarding any aspect of SHSC's business, there are internal mechanisms in place by which you can raise these issues to gain redress in a constructive and practical way. Such mechanisms include line management advice and support, complaints mechanism, grievance procedure, Chief Executive or Non-Executive Director guidance. In particular your attention is drawn to the Trust's Whistleblowing Policy and Procedure.

3. Definitions

Caldicott Guardian:
The role of the Caldicott Guardian resulted from the 1997 Review of Patient Identifiable Information, chaired by Dame Fiona Caldicott. Central to the recommendations of the review was the appointment in each NHS organisation of a Guardian of person based clinical information to oversee the arrangements for the use and sharing of clinical information. The Guardian is usually a clinician at Trust Board level who acts as the conscience of the organisation leading improvements in the way the Trust handles confidential patient identifiable information.

Caldicott Function:
Staff, skills and other resources available to support the Caldicott Guardian carry out the responsibilities of the role.

Safe Haven Procedures:
In this context a safe haven is a location (or in some cases a piece of equipment) situated within the Trust where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.

Informed Explicit Consent:
Consent, freely given, usually verbally or in writing, when the individual understands why their information is needed, who it will be shared with, what options are available to them with regard to their information and the consequences of those options.

Informed Implied Consent:
Consent that has been signalled by the individual taking some course of action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of their information. For example a service user who attends for treatment or care may be taken to imply consent for the collection and use of their information by the professional in providing that treatment or care.

4. Purpose

The purpose of this code of conduct is to protect service users and staff from the misuse of their information and to ensure that confidential information is handled in a lawful and appropriate manner by:

- Defining what is meant by the phrase “confidential information”
- Informing you of your responsibilities in relation to such information
- Informing you of the correct procedures for dealing with confidential information so that you do not inadvertently breach confidentiality
- Providing sources of further information

5. Duties

All managers are responsible for ensuring their staff are aware of this Code of Conduct and their individual responsibilities for adherence to the Code, and that they are equipped to fulfil those responsibilities. This will include covering the Code in corporate and local induction programmes and by identifying and meeting specific or generic training needs through personal development plans.

The Trust has a duty of care to make all reasonable adjustments for staff with disabilities. In cases where staff have disabilities that impact on their ability to fulfil their responsibilities under this Code it is the responsibility of the line manager to assess the situation and ensure appropriate adjustments are put in place.

All staff are expected to adhere to this Code of Conduct. Staff must ensure that they are aware of the requirements and standards of behaviour that apply.

All staff are responsible for reporting all breaches of confidentiality, and near misses, in accordance with the Trust’s Incident Reporting and Investigation Policy. Advice on using the Trust’s incident reporting process should be obtained from line managers in the first instance. Further advice can be obtained from the Trust’s Risk Department.

If there is anything within this Code of Conduct that you do not understand, you should contact your line manager in the first instance, or the Information Manager for further information.

The Trust’s Digital Information Governance Board has authority delegated by the Quality Assurance Committee to provide direction to and oversee implementation of this Code of Conduct, including arrangements to test compliance with the Code and implementation of necessary actions arising from internal or external compliance checks. It will ensure that the Code of Conduct is reviewed periodically. The Digital Information Governance Board is accountable to the Quality Assurance Committee.

6. Process

This section sets out the principles for handling confidential information and explains what this means in practice. The topics covered are listed below.

6.1 What is confidential information?

6.2 Who has a duty of confidentiality?

6.3 Why is confidentiality important?

6.4 Inform service users and staff

6.5 Record information accurately, consistently and in a timely manner

6.6 Understand and respect the rights of individuals in relation to their information

6.7 Obtain consent to share information wherever possible

6.8 Capacity to consent

6.9 Consent of children and young people

6.10 Only disclose information without consent for legitimate reasons

6.11 Follow the relevant SHSC procedure when disclosing information without consent

6.12 Disclosing information to the police

6.13 Check list of points that must be considered before disclosing confidential information

6.14 Access to records

6.15 Keep information secure

6.16 Report incidents and near misses in line with SHSC policy

6.17 Do not hold confidential information on portable devices without authorisation

6.18 Improve standards of practice wherever possible

6.19 Use confidential information in accordance with SHSC policies

6.20 Apply policy in areas within your work area

Principle	**What this means in practice**
6.1 What is confidential information?	Confidential information may be information about identifiable individuals including, but not limited to, service users, members of staff or other third parties. It may also be organisational information about SHSC or any other health or social care organisation. It is not necessary for the name of the individual to be known for the information to be identifiable. For example, it may be possible to identify an individual when a number of data items are put together such as post code, ethnicity and medical condition. Information about deceased people is classed as confidential. Confidential information may be in a variety of forms including but not limited to electronic, paper, digital or audio format, such as records, note books, message books, x-rays, photographs, audio recordings, voicemail etc, or it may be knowledge gained from overheard conversations or seeing someone attend a clinic appointment. Examples of confidential information SHSC holds include: • Personal demographic details of service users and staff • Contact details of service users and staff • Medical details of service users and staff • Ethnicity of service users and staff • Bank and salary details of staff

	• Results of DBS (formerly CRB) checks • Organisational financial information • Waiting list data Information that has been placed in the public domain, except as a result of a breach of confidentiality, is not classed as confidential.
6.2 Who has a duty of confidentiality?	All SHSC employees and non-Trust employees who work within SHSC or under contract to it have a duty to maintain the confidentiality of information gained during their employment or association with the Trust. This includes, but is not limited to, all staff, whether directly employed, seconded, on honorary contracts, permanent or temporary, also agency staff, non executive directors, students on placement and people working in a voluntary capacity. For convenience, the term 'staff' is used in this document to refer to all those to whom the code of conduct applies. Anyone may come into contact with confidential information in the course of their duties. For example: • You may have direct access to confidential information if you are authorised to access information held in staff or service user records • You may have confidential information passed to you in connection with your work • You may become aware of information as a result of breaches of confidentiality. You are obliged to maintain the confidentiality of this information. This duty continues after you no longer work for or have an association with SHSC.
6.3 Why is confidentiality important?	Confidentiality is important to protect the privacy of all individuals (staff, service users and carers) whose information we hold. Both staff and service users provide us with confidential information about themselves. They have a legitimate expectation that we will respect their privacy and treat their information appropriately. In a service delivery setting, it is important to maintain the trust of service users. Service users entrust us with, or allow us to gather, confidential information relating to their health and other matters as a part of their seeking treatment. We use this information to assess their needs and deliver appropriate treatment and care. It is essential that clinicians/practitioners have all relevant information to hand. If service users do not trust us with their information they may withhold vital information or not seek treatment. Trust is also important in managing health and safety, and risk. Staff or service users may want to pass on information about other individuals for example, to report poor practice. Staff should be aware of the appropriate procedures, which should be followed in such cases. (In some circumstances, service users may lack the competence to extend this trust or may be unconscious, but this does not diminish the duty of confidence).

	It is essential if the trust of staff and service users is to be retained, and legal requirements are to be met, that the NHS provides, and is seen to provide, a confidential service.
6.4 Inform service users and staff	At their first contact with the organisation/ service/member of staff you should: • Explain to service users/carers/staff why we collect information, how it might be used, who it might be shared with and seek their consent. • Make it clear to individuals what your role is and the circumstances under which confidential information may have to be shared. This gives them the opportunity to limit the information they provide. • Explain to service users in particular that the information they give may be recorded, may need to be shared in order to provide them with care and may be used to support clinical audit and other work to monitor the quality of care provided. • Explain to individuals their general rights (see section 6.6 below). • Consider if individuals would be surprised to learn that their information is being used in a particular way. If they would be, they are not being effectively informed. Staff should consider the following options in order to inform service users effectively: • Have service users been shown the leaflet "Confidentiality and Information Sharing: information for service users and carers" (available on the SHSC website under Confidentiality and Information Sharing) or a service specific leaflet? • Have service users had the opportunity to read the leaflet and ask questions? • Is it clear to service users when information is recorded or health records accessed? • Is it clear to service users when staff are or will be sharing information with others? • Are service users aware of the choices available to them in respect of how their information may be used or shared? • Check that service users have no concerns or queries about how their information is used or shared • Answer any queries personally or direct the service user to others who can answer their questions or to other sources of information • Respect the rights of service users and help them in exercising their right to have access to their health records
6.5 Record information accurately, consistently and in a timely manner	• Record information in accordance with SHSC policy and service specific procedures. • You have a duty to maintain proper records. (This is vital to the provision of care and the running of the Trust). • If records are inaccurate, future decisions may be wrong and may result in harm to a service user or member of staff. If information is recorded inconsistently, then records will be harder to interpret, resulting in delays and possible errors.

6.6 Understand and respect the rights of individuals in relation to their information	Under the Data Protection Act, individuals have certain rights about the way information about them is used. These include the right to:
	
	• See information that is recorded about them (a subject access request) and to have any part of it they do not understand explained (or authorise someone else on their behalf to request access)
	  o Access to some or all of the information may be refused where it would cause serious harm to the data subject or anyone else (any health information should be reviewed by an appropriate health professional prior to disclosure)
	  o Access to information that identifies another person will be refused unless s/he has consented to the disclosure (this does not apply if the information is from a professional involved in the care of the individual and relates to their care)
	  o The request must be answered within 40 days
	• Prevent the processing of information causing unwarranted damage and distress
	• Have inaccurate information rectified or destroyed. (In cases of dispute, the individual will be allowed to place a note on the record disputing SHSC's version of events).
	• Seek compensation
	
	Children and young people have a right to see information about them if they are judged to be competent. People with parental responsibility can apply to see a child/young person's records but this will be refused if a child is competent and does not consent.

6.7 Obtain consent to share information wherever possible	• Information will be shared with the **informed explicit consent** of the individual wherever possible. • Informed consent is when an individual understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or not to that proposed use, and gives consent. Informed consent may be explicit or implied. Explicit consent may be given verbally or in writing. • Where a third party requests access to records and has provided written consent of the individual, you should check that the consent is informed. • You should inform service users that they generally have a right to object to the use and disclosure of confidential information that identifies them. • In certain circumstances, if a service user chooses to prohibit the disclosure of information to other health or social care professionals it may mean that the care that can be provided is limited or, in rare circumstances, cannot be provided at all. Clinicians cannot treat service users safely, nor provide continuity of care, without having relevant information about a service user's condition or medical history. • You must inform service users if their decisions about disclosure have implications for the provision of care or treatment. • Where a service user has been informed about the proposed uses and disclosures involved in the delivery of their healthcare, and their right to refuse permission, and they

	agree to their information being shared, then explicit consent is not required for each specific disclosure associated with that healthcare. For example, the sharing of information within a multi-disciplinary team in a hospital or across the primary healthcare team within a GP practice does not require explicit consent for each disclosure. • Even where there are grounds for sharing information without consent it is good practice to ask permission to share that information (unless it would prejudice the investigation of a crime or would put the individual at risk of harm). • Lack of consent should not prevent the sharing of information where there are concerns about the welfare of an individual.
6.8 Capacity to consent to sharing information	• Where the individual does not have the capacity to consent, the responsibility for deciding the appropriate course of action lies with the agency giving care or, for service users who have planned ahead, the person with an appropriate and properly registered power of attorney. • Where the agency giving care is responsible for decisions about information sharing, these must be made in the best interests of the service user taking into consideration any previously expressed views of the service user. The service user's views may have been recorded in an Advance Statement although they are not legally binding. It is good practice to encourage patients to complete an Advance Statement whilst they still have the capacity to do so. • In accordance with the Mental Capacity Act 2005 (MCA), the agency, where appropriate, should consult other people, especially: anyone previously named by the service user as someone who should be consulted, carers, close relatives or friends of the patient, any attorney appointed under the MCA, the views of an appointed independent mental capacity advocate (IMCA), any deputy appointed by the Court of Protection to make decisions for the service user.
6.9 Consent of children and young people	• Young people over the age of 16 are presumed to be competent to give their own consent. • In the case of children and young people under the age of 16, consent is usually required from a person with parental responsibility (who is usually the mother or father or someone who holds a court order giving them parental responsibility). • As children get older they gain rights for themselves. Children under the age of 16 can give consent for themselves if they have sufficient understanding and intelligence to fully understand what is proposed, that is, they are Gillick/Fraser competent. • People with parental responsibility can authorise other people to make decisions about their children including the sharing of information.
6.10 Only disclose information without consent for legitimate reasons	• There are circumstances when it is necessary to share information even though the individual has not consented. • These circumstances are the exception rather than the rule. • Information can be shared without the consent of the person whom the information is about when: o It is in the public interest to do so o It is required by law

	Examples of sharing information in the public interest include: • Where a child is believed to be at risk of harm (Children Act 1989) • Where there is a risk of harm to anyone, including the data subject • Where information is required for the prevention, detection or prosecution of a serious crime **Examples of sharing information where it is required by law include:** • If the individual gives information about suspected terrorism (Anti-terrorism, Crime & Security Act 2001 and Terrorism Act 2000) • Notification of certain infectious diseases • Where it is required by court order • Under the Mental Health Act 1983 where a service user objects to their 'nearest relative' being consulted re: - - An application for Treatment Order (Section 3) is being considered - An application for assessment and treatment (Section 2) in relation to the service user has been made - Under the Mental Health Act (Patients in the Community) Act 1995 where the service user is known to have the propensity to violent or dangerous behaviour • Domestic Violence, Crime and Victims Act 2004 gives victims of specified sexual or violent offences the right to be informed of certain decisions if the offender becomes subject to provisions under the MHA 1983. **Confidential information that is disclosed without consent must follow the appropriate process**
6.11 Follow the relevant SHSC procedure when disclosing information without consent	• If it is felt necessary to share information where consent is withheld the individual should be informed of this decision (unless it would prejudice the investigation of a crime or would put the individual at risk of harm). It may be appropriate to give the individual an opportunity to disclose the information him/herself. • If it is not possible to obtain the consent of the individual, or it is not desirable, then the decision whether to share information should be taken at an appropriate level within the organisation. • The authority to disclose information may vary within different parts of SHSC and may depend on the reason for/circumstances of disclosure. It may lie with the Caldicott Guardian/Caldicott function, professional lead such as the clinical director or other senior manager. • You should ask your line manager for the procedure you should follow or obtain advice from the information governance lead. • It is a requirement of SHSC that the reasons for the final decision (either to share or not to share) should be recorded. • It is important where information is shared without consent that the member of staff documents what information was

	released and when, to whom it was disclosed, and why it was felt justified. • All non-consented disclosures must be reported to the Caldicott Guardian and information governance lead.
6.12 Disclosing information to the police	• Requests for personal information should be in writing which can include faxes on headed paper. If requests are submitted by e-mail they should be from a genuine .pnn e-mail address. • The request for information should specify why it is required. (See section 6.10 for legitimate reasons for disclosing information without consent). • If it is not possible for the applicant to specify why the information is required (for example, because it would prejudice the investigation of a crime) then the request should be signed by a senior officer. • Information should only be disclosed with the proper authority (See section 6.11 and 6.13.4). • Disclosures to the police may be very sensitive. Consider if special arrangements need to be put in place to facilitate disclosure, for example, nominate a member of staff to deal with the request. • Where police produce a consent form for the records they wish to access, a member of staff should check with the data subject that the consent is informed.
6.13 Check-list of points that must be considered before disclosing confidential information	The purpose of these questions is to help you decide the appropriate action to take if you are asked to disclose confidential information about a service user, carer or member of staff. They are not sequential or definitive but are intended as a guide to good practice. 6.13.1 Have I verified the applicant's identity? 6.13.2 Is there a legitimate reason for disclosing the information? 6.13.3 Is the information requested adequate, relevant and not excessive for the purpose? 6.13.4 Do I have the authority to disclose the information? 6.13.5 What is the most appropriate method of disclosing the information? 6.13.6 Who do I need to inform that I have disclosed confidential information? 6.13.7 What do I need to record about the request and disclosure/non-disclosure?
6.13.1 Verifying identity	You must ensure that you can confirm the identity of the person and/or legitimacy of the organisation requesting information. **Requests in person** If you are not familiar with the individual then you can ask for some photo ID. **Telephone requests** You can verify identity in the following ways: *Request from another agency* Telephone the individual back via the main switchboard of their organisation. If you do not know the telephone number (for example, because it is an agency that you are not familiar with), then you should independently verify the number via a telephone

	directory/directory enquiry service, that is, don't accept the number as given by the applicant. Unless there is a local procedure in place that states otherwise, you should ask for the request to be put in writing (which includes by fax). All requests from the police should be put in writing. **Written requests** Written requests from organisations (for example, a solicitor or substance misuse agency) must be on headed notepaper. The address should be independently verified (that is, you should not accept an address/fax number given to you for an organisation that you are unfamiliar with). The identity of the applicant should be verified for all written requests.
6.13.2 Legitimate reasons for disclosing information	1. Disclosure is required law, for example, by statute or court order. 2. There is an overriding public interest in disclosing the information. 3. Disclosure of the information is required for the purposes of providing care. 4. The service user/staff member who is the subject of the data wishes the information to be disclosed.
6.13.3 Disclosing information that is adequate, relevant and not excessive for the purpose	Consider: 1. What does the recipient hope to achieve by the disclosure? (That is, what is the purpose of disclosing information?) 2. What is the minimum amount of information you can share to achieve that purpose? 3. Who does the information need to be shared with?
6.13.4 Authority to disclose information – consented and non-consented disclosures including routine bulk transfers of patient identifiable data (PID)	Confidential personal or SHSC information may only be disclosed with the proper authority and must be protected against improper disclosure at all times. Authority to disclose may be obtained from the service user/staff member or from the designated individual in the Trust. **Authority from the service user/staff member** The service user/staff member has given authorisation for the disclosure of his/her information. **Appropriate authority from within SHSC** Disclosures of information that breach confidentiality should be authorised by the Caldicott Guardian/Caldicott function or by a designated senior manager/professional lead such as a clinical director where there are local departmental procedures in place. (Advice can be obtained from the information governance lead). All non-consented disclosures should be reported to the Caldicott Guardian. All bulk transfers of PID must be referred to the Director of IM&T for authorisation before they can commence.
6.13.5 Appropriate methods of communicating confidential information	The most appropriate method of communicating information will depend on a number of factors including the sensitivity of the information, its destination and the urgency of the request. Information should be transferred effectively, that is, it should reach its destination in a timely manner, and confidentially. As a general rule, you should inform the intended recipient if you are sending them confidential information so that they can inform you if they have received it or not.

	By post • Ensure you have an up to date address for the intended recipient • Confidential information should marked 'Private and confidential: for the addressee only' • Confidential information sent in both the internal and external post should be in sealed envelopes or packaging • Depending on the sensitivity of the information and where it is being sent to, information may be double or single wrapped, and delivered by hand/recorded delivery/ normal post/internal post - but not in a transit envelope (either sealed or unsealed) • Confidential information sent/transferred on a CD rom/floppy disc/memory stick must be encrypted. **By fax** • It may not be appropriate to fax very sensitive confidential information • Confidential information should be faxed using a safe haven fax, where appropriate, or safe haven procedures • A safe haven fax is one that is located in a separate office that has restricted access • Confidential information can be sent to faxes situated in open offices by using safe haven procedures: The intended recipient should be telephoned and informed that you are about to send them confidential information. The intended recipient should wait by the fax machine and collect the fax immediately it arrives. The recipient should telephone you to let you know it has arrived. • Always fax information to a named recipient • Routinely used numbers should be pre-programmed into the fax machine • Faxed information going astray is usually due to user error so it is important to take care to enter the fax number accurately. If there is any doubt, a test fax can be sent followed by the confidential fax using the redial button. **By telephone** Ensure you know the identity of the caller before giving out information. (See 'verifying identity' above). Do not leave confidential information on voicemail. **By e-mail** Confidential information should not be shared by e-mail unless it is part of a process agreed and authorised by the information governance lead/Caldicott function. See the e-mail policy for details of how confidential information can be sent by e-mail securely.
6.13.6 Informing appropriate individuals that confidential information has been disclosed	**The service user/staff member** 1. Even where there are grounds for disclosing confidential information without consent it is good practice to ask permission to do so (but see point 4 below). 2. Where a service user/staff member has disclosed information that you feel needs to be disclosed to a third party, it may be appropriate to give the service user/staff member an opportunity to disclose this information him/herself first. You should follow this up later, by an

	agreed date with the individual, to ensure the information has been disclosed. 3. If it is decided that it is necessary to disclose information even though the service user/staff member has specifically withheld their consent, it is good practice to inform him/her of your intention. 4. The service user/staff member should not be asked for permission to release information or told that information about them has been disclosed without their consent if it would prejudice the investigation of a crime or would put any individual at risk of harm. **Other health and social care professionals** It is important to identify and inform any individuals who need to be made aware that confidential service user/staff member information has been disclosed. This is particularly important where information has been disclosed without consent.
6.13.7 Recording information about disclosures	All relevant information about disclosures must be recorded in the service user's notes/staff personal file. This includes: • The name of the person and agency making the request • The method of the request (telephone, in writing, by fax etc) • The purpose of the request • Whether information was disclosed or not • Who the information was disclosed to and by what method • Reasons for disclosure or non-disclosure • If there was service user/staff member consent to the disclosure or not • Who has been informed of the disclosure
6.14 Access to records	• The Data Protection Act 1998 gives individuals a general right of access to **view or receive a copy of information** that is held about them. An individual can apply for access to his/her own information or authorise someone else to apply for access to this information on his/her behalf. Responses must be made within 40 days. Requests should be referred to the Corporate Affairs Dept. • Requests to access the health records of deceased people can be made under the Access to Health Records Act 1990. Under this Act, the patient's personal representative or anyone with a claim on the deceased's estate can request access to their records. Responses must be made in 21 days.

6.15 Keep information Secure	Personal information should be held, used and shared securely and confidentially and in line with SHSC policies.
	For example:
	
	Confidentiality in public places
	• Be aware of the difficulties of maintaining confidentiality in open plan offices
	• Do not discuss confidential information in public areas where it may be overheard, for example:
	  o In corridors
	  o In reception areas
	  o When using mobile phones
	• Do not record confidential information where it may be accessed by unauthorised people – for example, on white

boards, card systems that are not locked away etc.

Access to information

- Do not browse electronic systems or records
- Do not access information which you do not have a need to know
- Save information on a secure server where available
- Ensure information stored in a shared drive is accessible only to those with a need to know
- Consider how PC screens are positioned? Can confidential information be seen by anyone who does not have a need to know
- Do not leave confidential information unattended, for example, do not leave information out on your desk or information systems logged on
- Share information on a need to know basis

Information security

- Lock information away when not in use
- Information not stored on a server, for example, confidential information held on a PC or lap top hard drive must be encrypted and must be backed up regularly, kept in a secure place and transferred to a server as soon as possible
- Information must only be stored on such portable devices in accordance with SHSC policy (see section 6.17)
- Do not introduce unauthorised software onto your PC or laptop
- Use up to date anti-virus software
- Virus check CDs, memory sticks etc. before introducing them onto your PC

Records taken Away from Trust Premises

- Any staff taking confidential information away from Trust premises must risk-assess the need for adequate security. This requirement is set out in the Remote Working and Mobile Devices Policy.

Section 6.7 of the policy highlights the following :-

  - Confidential information, whether manual or electronic, must be protected by adequate security, for example, it must be :-
  - Kept out of sight, for example, in the locked boot of the car when transported;
  - Not left unattended, for example, not left in the car boot overnight or when the car is parked up and left during visits etc.;
  - Locked away when not being used;
  - Kept secure and guarded from theft, unauthorised access and adverse environmental events when taken home.

See also section 6.9 regarding the need for assessing the potential risk before working on confidential information at home.

	Send personal information appropriately (see 6.13.5) • By post – in a sealed envelope marked 'Private and confidential: for the addressee only' • By fax – use safe haven procedures, for example, telephone the recipient before faxing to ensure they are there to collect it • By portable media – confidential information must be encrypted and transferred appropriately • By telephone – ensure you know the identity of the caller before giving out information • E-mail – confidential information should not be shared by e-mail unless it is part of an authorised process • Don't leave confidential messages on voicemail **Confidential waste** Confidential information may be stored in a number of formats such as paper records, information in notepads/message books, floppy disk/CDs/DVDs, hard drive of computers etc. All such information and devices storing such information must be disposed of appropriately and in line with SHSC policy, for example, use of 'confidential waste' boxes, shredding, destruction of hard drives by IT Dept. etc. **Passwords** Use passwords to access electronic systems in line with SHSC policy, for example, in deciding what the password should be, how often it is changed, not sharing passwords, locking workstations, password-protecting documents etc. In particular: • Do not share passwords with others • Change your password at regular intervals • Do no re-use old passwords • Do not write your passwords down in an obvious place • Avoid using short passwords or using names or words that are associated with you, for example, children's or pet's names • Use a combination of numbers and letters
6.16 Report incidents and near misses in line with SHSC policy	Report security incidents such as theft or unauthorised disclosure, including near misses, in line with SHSC policy.
6.17 Do not hold confidential information on portable devices without authorisation	• Confidential information must not be stored on mobile devices such as laptops, memory sticks or PDAs without the prior approval of the information governance lead/Caldicott Guardian • Working on confidential information at home also requires authorisation as above. (See section 6.15 regarding records taken away from Trust premises).
6.18 Improve standards of practice wherever possible	It is not be possible to achieve best practice overnight but we must work towards continuous improvement. In order to work towards achieving best practice staff must: - • Be aware of the issues surrounding confidentiality, and seek training, support and advice as necessary in order to deal with them effectively • Feedback comments or suggestions to managers on systems, procedures or working practices that give a cause

	for concern or could be improved • Report breaches, suspected breaches and near misses
6.19 Use confidential information in accordance with SHSC policies	Be aware of all relevant SHSC policies and procedures. These are available on the intranet.
6.20 Apply policy within your work area	• Inform the staff you manage of their responsibilities in relation to SHSC information governance policies • Ensure these are adhered to or action is taken to address non-compliance

7. Dissemination, storage and archiving (Control)

This policy will be achieved through induction processes (corporate and local), the provision of training and day-to-day management of individuals.

The policy will be made available to all staff via the SHSC intranet.

Changes to this policy will be made by the SHSC Information Manager at the request of or approved by the Digital Information Governance Board (DIGB).

8. Training and other resource implications

Departmental managers are responsible for ensuring that their staff are aware of and comply with this policy.

9. Audit, monitoring and review

Monitoring Compliance Template						
Minimum Requirement	Process for Monitoring	Responsible Individual/ group/committee	Frequency of Monitoring	Review of Results process (e.g. who does this?)	Responsible Individual/group/ committee for action plan development	Responsible Individual/group/ committee for action plan monitoring and implementation
Compliance with this Code of Conduct	Review as part of the Information Governance Toolkit assessment	Care Records & Information Sharing Group	Annual	Digital Information Governance Board	Care Records & Information Sharing Group	Digital Information Governance Board

This policy will be reviewed in March 2018 or sooner if national guidance changes

10. Implementation plan

Action / Task	Responsible Person	Deadline	Progress update
Upload new policy onto intranet and remove old version	Director of Corporate Governance	16/09/2016	Issued on 19.09.2016
Ensure staff are aware of this policy	SHSC Team managers	Ongoing	Communication to be sent to all staff via the Communication Digest on 22.09.2016.

11. Links to other policies, standards and legislation (associated documents)

This code forms part of an overall suite of information governance policies overseen by the Digital Information Governance Board.

12. Contact details

Title	***Name***	***Phone***	***Email***
Caldicott Guardian	Clive Clarke	2718758	Clive.Clarke@shsc.nhs.uk
Chief Information Officer	Nicola Haywood-Alexander	3050725	Nicola.Haywood-Alexander@shsc.nhs.uk
Information Manager	John Wolstenholme	3050749	John.wolstenholme@shsc.nhs.uk

13. References

The main references in compiling this Code are :

• Access to Health Records Act 1990;
• Anti-terrorism, Crime & Security Act 2001;
• Children Act 1989;
• Common Law Duty of Confidence;
• Computer Misuse Act 1990;
• Data Protection Act 1998;
• Domestic Violence, Crime and Victims Act 2004;
• Freedom of Information Act 2000;
• Health and Social Care Act 2012;
• Human Rights Act 1998;
• Mental Capacity Act 2005;
• Mental Health Act 1983;
• Mental Health Act (Patients in the Community) 1995;
• Police and Criminal Evidence Act 1984;
• Terrorism Act 2000;
• Caldicott Review of Patient Identifiable Information 1997;
• Information: To share or not to share? The Information Governance Review 2013;
• Confidentiality: NHS Code of Practice;
• NHS Information Governance Requirements;
• Professional Codes of Conduct;
• A guide to confidentiality in health and social care – Treating confidential information with respect 2013;
• Code of practice on confidential information 2014;

Appendix A – Version Control and Amendment Log

Version No.	Type of Change	Date	Description of change(s)
1.0	Original policy approved by Information Governance Committee	September 2007	New policy approved along with other Information Governance policies developed by city-wide information governance group and after consultation with and agreement by staff-side.
1.0	Policy re-formatted and approved by Information Governance Committee	March 2008	
2.0	Policy revised and approved	April 2009	Organisation name changes, clarification of scope, addition of advance statements, additional guidance on taking records off Trust premises
2.1	Policy revised	February 2015	Minor updates
2.1	Policy approved by Information Governance Steering Group	April 2015	
3.0	Ratified and issued.	September 2016	Ratified by EDG.

Appendix B – Dissemination Record

Version	Date on website (intranet and internet)	Date of "all SHSC staff" email	Any other promotion/ dissemination (include dates)
2.0	April 2009		
3.0	September 2016	September 2016	

Appendix C – Stage One Equality Impact Assessment Form

Equality Impact Assessment Process for Policies Developed Under the Policy on Policies

Stage 1 – Complete draft policy

Stage 2 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? If **NO** – No further action required – please sign and date the following statement. If **YES –** proceed to stage 3

This policy does not impact on staff, patients or the public (insert name and date)

Stage 3 – **Policy Screening** - Public authorities are legally required to have 'due regard' to eliminating discrimination , advancing equal opportunity and fostering good relations , in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance on equality impact assessment for examples and detailed advice this can be found at http://www.shsc.nhs.uk/about-us/equality--human-rights

	Does any aspect of this policy actually or potentially discriminate against this group?	**Can equality of opportunity for this group be improved through this policy or changes to this policy?**	**Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?**
AGE	**No**		**No**
DISABILITY	**No**		**No**
GENDER REASSIGNMENT	**No**	**Adherence to this policy supports our legal obligations to the maintain the confidentiality of service user information**	**No**
PREGNANCY AND MATERNITY	**No**		**No**
RACE	**No**		**No**
RELIGION OR BELIEF	**No**		**No**
SEX	**No**		**No**
SEXUAL ORIENTATION	**No**		**No**

Stage 4 – **Policy Revision** - Make amendments to the policy or identify any remedial action required (action should be noted in the policy implementation plan section)
Please delete as appropriate: no changes made.

Impact Assessment Completed by (insert name and date)	J Wolstenholme, 7 Sept 2016

Appendix D - Human Rights Act Assessment Form and Flowchart

You need to be confident that no aspect of this policy breaches a person's Human Rights. You can assume that if a policy is directly based on a law or national policy it will not therefore breach Human Rights.

If the policy or any procedures in the policy, are based on a local decision which impact on individuals, then you will need to make sure their human rights are not breached. To do this, you will need to refer to the more detailed guidance that is available on the SHSC web site
http://www.justice.gov.uk/downloads/human-rights/act-studyguide.pdf
(relevant sections numbers are referenced in grey boxes on diagram) and work through the flow chart on the next page.

1. **Is your policy based on and in line with the current law (including case law) or policy?**

☐ **Yes. No further action needed.**

☐ ~~**No. Work through the flow diagram over the page and then answer questions 2 and 3 below.**~~

2. **On completion of flow diagram – is further action needed?**

☐ **No, no further action needed.**

☐ ~~**Yes, go to question 3**~~

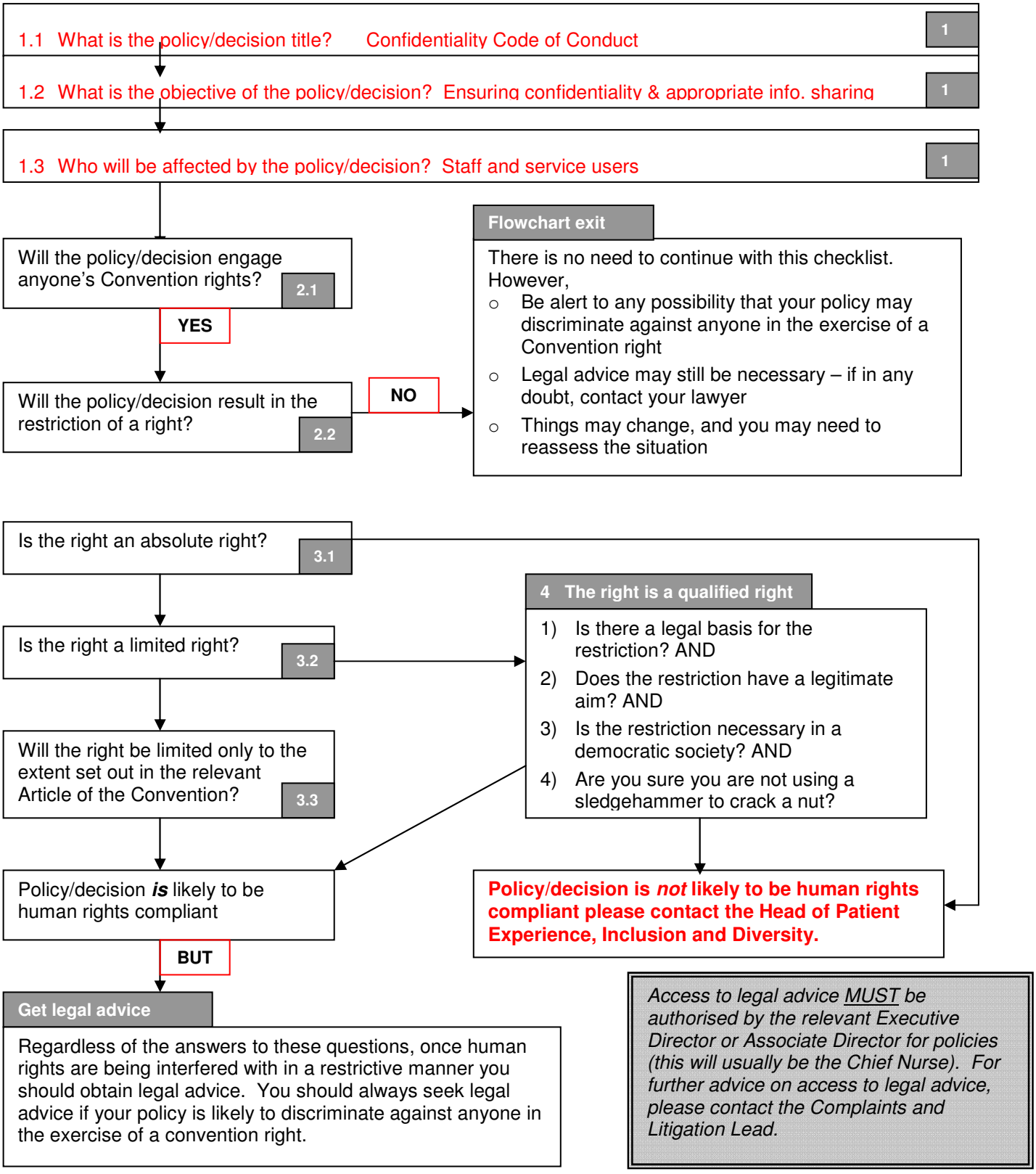
3. **Complete the table below to provide details of the actions required**

Action required	By what date	Responsible Person

Human Rights Assessment Flow Chart

Complete text answers in boxes 1.1 – 1.3 and highlight your path through the flowchart by filling the YES/NO boxes red (do this by clicking on the YES/NO text boxes and then from the Format menu on the toolbar, choose 'Format Text Box' and choose red from the Fill colour option).

Once the flowchart is completed, return to the previous page to complete the Human Rights Act Assessment Form.



Appendix E – Development, Consultation and Verification

This policy was developed by the SCT Information Department jointly with the Sheffield PCT Information Governance Group in order to establish a common approach to Information Governance across the city.

The policy was revised in light of national guidance issued in early 2008.

The draft policy was presented to and approved by the SCT Information Governance Committee.

It was submitted to the JCF and agreed by Staff Side

The policy was approved by the EDG.

The policy was revised and submitted to the Information Governance Steering Group in October 2010.

The policy was revised and submitted to the Information Governance Steering Group in February 2015 and approved in April 2015

The policy was re-formatted in line with Trust requirements and submitted to EDG for approval in September 2016

Appendix F –Policies Checklist

Please use this as a checklist for policy completion. The style and format of policies should follow the Policy template which can be downloaded on the intranet (also shown at Appendix G within the Policy).

1. Cover sheet ✓

All policies must have a cover sheet which includes:

- The Trust name and logo ✓
- The title of the policy (in large font size as detailed in the template) ✓
- Executive or Associate Director lead for the policy ✓
- The policy author and lead ✓
- The implementation lead (to receive feedback on the implementation) ✓
- Date of initial draft policy ✓
- Date of consultation ✓
- Date of verification ✓
- Date of ratification ✓
- Date of issue ✓
- Ratifying body ✓
- Date for review ✓
- Target audience ✓
- Document type ✓
- Document status ✓
- Keywords ✓
- Policy version and advice on availability and storage ✓

2. Contents page ✓

3. Flowchart ✓

4. Introduction ✓

5. Scope ✓

6. Definitions ✓

7. Purpose ✓

8. Duties ✓

9. Process ✓

10. Dissemination, storage and archiving (control) ✓

11. Training and other resource implications ✓

12. Audit, monitoring and review ✓

This section should describe how the implementation and impact of the policy will be monitored and audited and when it will be reviewed. It should include timescales and frequency of audits. It must include the monitoring template as shown in the policy template (example below).

Monitoring Compliance Template						
Minimum Requirement	Process for Monitoring	Responsible Individual/ group/committee	Frequency of Monitoring	Review of Results process (e.g. who does this?)	Responsible Individual/group/ committee for action plan development	Responsible Individual/group/ committee for action plan monitoring and implementation
A) Describe which aspect this is monitoring ?	e.g. Review, audit	e.g. Education & Training Steering Group	e.g. Annual	e.g. Quality Assurance Committee	e.g. Education & Training Steering Group	e.g. Quality Assurance Committee

13. Implementation plan ✓

14. Links to other policies (associated documents) ✓

15. Contact details ✓

16. References ✓

17. Version control and amendment log (Appendix A) ✓

18. Dissemination Record (Appendix B) ✓

19. Equality Impact Assessment Form (Appendix C) ✓

20. Human Rights Act Assessment Checklist (Appendix D) ✓

21. Policy development and consultation process (Appendix E) ✓

22. Policy Checklist (Appendix F) ✓