The Queen Elizabeth Hospital King's Lynn
NHS Foundation Trust

CONFIDENTIALITY CODE OF CONDUCT

Primary Intranet Location	Version Number	Next Review Year	Next Review Month
Information Management & Governance	5.0	2021	July

Current Author	Phil Cottis
Author's Job Title	Head of Health Records & IG
Department	Business Support
Ratifying Committee	Information Governance Committee
Ratified Date	12th July 2018
Owner	Jon Wade
Owner's Job Title	Chief Operating Officer

It is the responsibility of the staff member accessing this document to ensure that they are always reading the most up to date version. This will always be the version on the intranet.

Related Policies	Access to Health Records Policy and Procedure Confidentiality Audit Policy Creation of Corporate Records Procedure Disciplinary Policy and Procedure Disposal of IT Equipment and Media Policy Information Governance Policy Information Lifecycle & Records Management Policy Information Security Policy Interpreter & Translator Policy & Procedure. Management of Adverse Events Policy and Procedure Safe Haven Procedure Serious Untoward Incident Policy and Procedure

Stakeholders	Information Governance Committee Trust Executive Committee

Version	Date	Author	Author's Job Title	Changes
V1	March 2010	Nic McCullagh	Information Governance Manager	
V2	April 2012	Phil Cottis	IG & RA Manager	Review. Contact details. Formatting
V3	June 2014	Phil Cottis	IG & RA Manager	Review and format change
V3.1	July 2014	Phil Cottis	IG & RA Manager	New paragraph on apologising for personal data breaches (15.2)
V4	September 2015	Phil Cottis	IG & RA Manager	To comply with the requirement of the IG Toolkit v13
V4.1	June 2017	Phil Cottis	Head of Health Records & IG	2 additional sections: Disclosure when the Service User is unable to give consent; & Disclosure to Families and Carers
V4.2	April 2018	Phil Cottis	Head of Health Records & IG	GDPR compliance
V5	June 2018	Phil Cottis	Head of Health Records & IG	Review. Legislation updated

Summary of the policy
This code of conduct has been produced to protect staff, by making them aware of the correct procedures for making disclosures and dealing with confidential information.

Key words to assist the search engine
Caldicott, Confidentiality, Consent, Patient Staff, Sharing

CONTENTS

CONFIDENTIALITY CODE OF CONDUCT

1 INTRODUCTION

1.1 All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual and professional responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 2018. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information, and the NHS Constitution for England.

1.2 To this end, the Trust aims to:

- Inform patients about the use of their confidential data and to record their objections, consent or dissent (in written form and generally in their health record); and
- To provide access to a patient's data to other relevant professionals, always doing so securely, and only where there is a legal and appropriate basis to do so.

2 PURPOSE

2.1 Under the common law duty of confidentiality, any member of staff may be personally liable in a court of law for unauthorised disclosure of personal data. This code of conduct has been produced to protect staff, by making them aware of the correct procedures for making disclosures and dealing with confidential information.

3 DEFINITIONS

3.1 **Anonymised Information**
This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.

3.2 **Confidential Information**
Confidential information can be anything that relates to patients, staff or any other information (such as contracts, tenders etc) held in any form (such as paper or other forms like electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on portable devices such as laptops, PDAs, Blackberrys, mobile telephones) or even passed by word of mouth. Person identifiable information is anything that contains the means to identify an individual.

3.3 **Disclosure**
This is the divulging or provision of access to data.

3.4 **Consent**
Consent is the approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be 'no surprises') and they should understand the implications of

their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.

3.5 **Explicit Consent**

Explicit consent is unmistakeable. It can be given in writing or verbally, or conveyed through another form of communication such as signing. A patient may have capacity to give consent, but may not be able to write or speak. Explicit consent is required when sharing information with staff who are not part of the team caring for the individual. It may also be required for a use other than that for which the information was originally collected, or when sharing is not related to an individual's direct health and social care.

3.6 **Implied Consent**

Implied consent is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed. Examples of the use of implied consent include doctors and nurses.

3.7 **Personal Data**

Personal data is defined as any information relating to an person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.8 **Personal Confidential Data**

Personal confidential data relates to information about a person which would enable that person's identity to be established by one means or another. This might include:

- Name, address, post code, date of birth;
- Pictures, photographs, videos, audio-tapes or other images of patients;
- NHS number and local patient identifiable codes; and
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

Personal confidential data may be in any form including, but not restricted to, the following:

- Paper records or documents;
- Fax messages;
- Telephone conversations;
- E-mail and attachments; and
- CDs, memory sticks or other portable media.

3.9 **Public Interest**

Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure

may cause and the interest of society in the continued provision of confidential health services.

3.10 **Sensitive Data**

Data held about an individual which contains both personal and sensitive information. There are only seven types of information detailed in the Data Protection Act 2018 that are deemed as sensitive:

- Racial or ethnic origin;
- Religious or other beliefs;
- Political opinions;
- Trade union membership;
- Physical or mental health;
- Sexual life; and
- Criminal proceedings or convictions.

3.11 **Staff**

For the purpose of this code of conduct, 'staff' is used as a convenience to refer to all staff regardless of occupation, including but not restricted to permanent, fixed-term, contractors, bank, agency, temporary, honorary, visiting, voluntary and students.

4 RESPONSIBILITIES

4.1 **Chief Executive**

The Chief Executive has overall responsibility for information security in the Trust. As accounting officer the Chief Executive is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Maintaining confidentiality is pivotal to the Trust being able to supply a first class confidential service that provides the highest quality patient care. The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.2 **Senior Information Risk Owner**

An Executive Director has been appointed as the Senior Information Risk Owner (SIRO) with overall responsibility for information governance, of which confidentiality is a key part.

4.3 **Caldicott Guardian**

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

4.4 **Information Governance Committee**

The Information Governance Committee is responsible for ensuring that this code of conduct is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

4.5 **Head of Health Records & IG**

The Head of Health Records & IG is responsible for maintaining the currency of this code of conduct, providing advice on request to any member of staff on the issues

covered within it, and ensuring that training is provided for all staff groups to further their understanding of the principles and their application.

4.6 **Senior Managers**

Senior Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Incident Reporting Procedure.

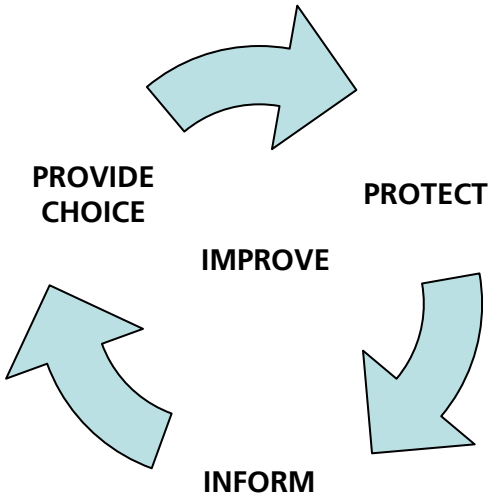
4.7 **All Staff**

Confidentiality is an obligation for all staff. Staff should note that they are bound by the document 'Confidentiality: NHS Code of Practice 2003'. There is a Confidentiality clause in their contract and that they are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues. Any breach of confidentiality, inappropriate use of health or staff records, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported.

5 THE CONFIDENTIALITY MODEL

5.1 The confidentiality model outlines the requirements that must be met in order to provide patients with a confidential service. Staff must inform patients of the intended use of their information, give them the choice to give or withhold their consent, as well as protecting their identifiable information from unwarranted disclosures. These processes are inter-linked and should be on going to aid the improvement of a confidential service.

5.2 The four main requirements are:



- **PROTECT** – look after person identifiable information
- **INFORM** – ensure that patients are aware of how their information is used
- **PROVIDE CHOICE** – allow patients to decide whether their information can be disclosed or used in particular ways
- **IMPROVE** – always look for better ways to protect, inform and provide choice

6 KEY PRINCIPLES

6.1 All staff must ensure that the following principles are adhered to:

- Person-identifiable or confidential data must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of;
- Access to person identifiable or confidential data must be on a need-to-know basis;
- Disclosure of person identifiable or confidential data must be limited to that

purpose for which it is required;

- Recipients of disclosed information must respect that it is given to them in confidence;
- If the decision is taken to disclose information, that decision must be justified and documented; and
- Any concerns about disclosure must be discussed with either your Line Manager or the Information Governance Team.

6.2 The Trust is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

6.3 Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

6.4 Access to rooms and offices where PCs are present or person identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person identifiable information by unauthorised parties.

6.5 All staff should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

6.6 Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin and must not be left lying around but be filed and locked away when not in use.

6.7 Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

7 DUTY OF CONFIDENCE

7.1 Patients entrust us with, or allow us to gather, personal and often sensitive information relating to their health and other matters as part of seeking treatment. They do so in confidence and have the legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. A key guiding principle is that a patient's health records are made to support that patient's healthcare.

7.2 A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.

7.3 Information that can identify individual patients must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification for doing so. (See later sections 'Disclosing without consent' and 'Legal restrictions on disclosure'.) In contrast, anonymised information is not confidential and may be used with relatively few constraints.

7.4 Staff must ensure that the obtaining of information is fair and necessary, and that the recording and verifying of the information is accurate and consistent. Patients must be informed of the importance of providing complete and accurate information.

8 DISCLOSING AND USING CONFIDENTIAL INFORMATION

8.1 It is extremely important that patients are made aware of information disclosures that must take place in order to provide them with the highest quality care. In particular, clinical governance and clinical audits might not be obvious to patients, and should be drawn to their attention. Similarly, the need to share information between members of different care teams and between different organisations involved in their healthcare provision should be explained. This is particularly important where disclosure extends to non-NHS bodies, such as Social Services.

8.2 Many uses of confidential patient information do not contribute to or support the healthcare that the patient receives. Very often these other uses are extremely important and provide benefits to society, such as medical research, public health, health service management and financial audit. However, as they are not directly linked to the healthcare that patients receive, it cannot be assumed that patients are happy for their information to be used in this way and so this must be checked.

8.3 Staff need to be aware that information disclosures of their personal information are also necessary at times to facilitate their employment and / or training. This may include, but is not limited to, disclosures to non-NHS bodies, such as training providers and support companies.

9 PATIENT CONSENT TO DISCLOSURE

9.1 The NHS Constitution states that individuals have the right to object to information about them being shared in a form that might identify them and in general to have reasonable objections to this sharing upheld. Staff must therefore ensure that patients are made aware that the information the patient gives may be recorded and shared, and the purposes for which this may apply (e.g. direct provision of healthcare, clinical audit, research etc).

9.2 When an individual provides consent for sharing information about them for a particular purpose (either for direct care or for other purposes), this consent provides a legal basis for that information sharing.

9.3 Consent may either explicit or, in certain circumstances, implied. Even when consent has been given, this does not mean that information which is unnecessary or irrelevant must be shared.

9.4 The individual is usually able to give consent for any information sharing needed to safely provide that care. Very few individuals ever express concern about information sharing where they see it as necessary to provide their care (for 'direct care'). Consent for the necessary sharing of information to support care delivery can be inferred from the fact that an individual agrees to receive that care, however, only relevant information should be shared.

9.5 There are three tests for establishing the conditions under which consent can be

implied, all of which must be met affirmatively:

- Is the person sharing the information a registered and regulated professional or one of their direct care team?
- Is the activity a type of direct care within the scope specified by the professional's regulatory body?
- Does the professional have a legitimate relationship with the person or persons concerned?

9.6 Staff should check that information about the choices available in respect of how information is used or shared is given, and whether the patient has any questions or concerns regarding this. Staff should be able to answer any questions or concerns about the use of the personal information. If they are unable to answer the questions or concerns, staff should be able to direct the questions or concerns to their line manager or another member of staff who can provide the answer. If the line manager or other team member is unable to answer the questions or concerns, advice and guidance can be sought from the Caldicott Guardian, SIRO or the Head of Health Records and IG.

9.7 Staff should be able to explain, in a non-threatening and non-confrontational way, the implications of disclosing or not disclosing information so that the patient can make valid choices. Sometimes this may mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment. However, patients do continue to have the right to object to the disclosure of confidential information. Where the patient is competent to make this decision, this should be respected.

9.8 Patients can change their consent at any time. Consent is not an open ended decision. Consent pertaining to the care of a person should be reviewed when any of the following criteria apply:

- The person using the service decides to remove their consent;
- There is a significant change in the person's situation e.g. a new diagnosis and/or a referral; and
- After an agreed timescale, which organisations should consider and include as part of their local policies through dialogue with their patients.

9.9 Care must be taken to ensure that the 'Your information, your rights' leaflet describing how personal information is shared is provided in a suitable format (e.g. Braille, audio tape) or language that is accessible. Staff should also be aware of the provision of translation services where necessary. For further guidance refer to the Interpreter & Translator Policy & Procedure.

10 DISCLOSING WITHOUT CONSENT

10.1 There are rare circumstances where a decision to disclose without consent may be warranted. These include:

- In the public interest / to protect the public (e.g. murder, rape, serious risk of harm could warrant breaching confidentiality);
- Court order; or

- Legislations for example Section 251 of the NHS Act.

10.2 **In the public interest / to protect the public:** Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and / or to prevent abuse or serious harm to others where they judge (on a case by case basis) that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the Trust's provision of a confidential service. Definitions are not clear but examples include murder, rape, child protection concerns, assault or the spread of an infectious disease. However, all requests for information from the Police must be directed to the Complaints and Legal Services department, as per section 12 'Requests for information by the police or media'.

10.3 **Section 251 of the NHS Act 2006:** This legislation provides the Secretary of State for Health with the authority to make regulations that set aside legal obligations of confidentiality (though not other legal requirements). Support can be granted for a specific range of activities, for example anonymising information, accessing records to contact people for the purposes of gaining consent for research, geographical analysis, linkage, validation and clinical audit.

10.4 Whoever authorises the disclosure must make a clear and accurate record of the circumstances, the advice sought and the decision making process followed so that there is clear evidence of the reasoning used and the prevailing circumstances. Disclosures should also be proportionate and be limited to relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies.

10.5 Where possible, the issue of disclosure should be discussed with the individual concerned and consent sought. Where consent is not given, the individual should be told of any decision to disclose against their wishes. This will not be possible in certain circumstances, for example where the likelihood of a violent response is significant, or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation.

10.6 **Court order:** A written request from the Police that is backed by a Court Order, stating exactly what information is needed and its purpose. This does not require the consent of the patient but they should be informed, preferably prior to disclosure. Disclosures must be strictly in accordance with terms of the court order and to the bodies specified in the order. Where staff are concerned that a court order requires disclosure of sensitive information that is not germane to the case in question, they may raise ethical concerns with the judge or presiding officer. However, if the order is not amended it must be complied with. A clear and accurate record of the circumstances should be kept.

10.7 **Disclosure when the Service User is unable to give consent:** In dealing with an urgent and immediate risk such as a suicidal person, if you are satisfied that the person lacks capacity to make a decision whether to share information about their risk, you should use your professional judgment to determine what is in the person's best interest. It is essential that you record their decision about sharing information on each occasion they do so and also the justification for this decision.

10.8 **Disclosure to Families and Carers:** All staff must make every effort to ensure the

patient is encouraged to disclose appropriate information to individuals or family members who may be able to support them, whilst ensuring that the patient does not feel under pressure to allow the disclosure.

11 CONFIDENTIALITY AFTER DEATH

11.1 When an individual has died, information relating to that individual remains confidential under the common law

11.2 An ethical obligation to the relatives of the deceased exists and health records of the deceased are public records and governed by the provisions of the Public Records Act 1958. This permits the use and disclosure of the information within them in only limited circumstances. The Access to Health Records Act 1990 permits access to the records of a deceased person by those with a claim arising out of that individual's death. This right of access is negated however if the individual concerned requested that a note denying access be included within the record prior to death (this might be part of a formal advance directive).

11.3 There is no equivalent statutory provision in relation to social care records. Local authorities generally provide access to social care records through the Freedom of Information Act. However, the guidance issued by the ICO on s.41 of the Freedom of Information Act means relatives could pursue a case for breach of confidence.

12 REQUESTS FOR INFORMATION BY THE POLICE OR MEDIA

12.1 Requests for information from the Police must be directed to the Complaints and Legal Services department. Please contact the Legal Services Support Officer on ext 3429 or email Legal.Services@qehkl.nhs.uk

12.2 Any requests for information from the media (e.g. newspapers, TV companies etc) should be directed to the Trust Communications Team: Telephone ext 3216 during office hours or 07557 012663 or 07557 012662 outside of office hours.

13 CONFIDENTIALITY OF PASSWORDS AND SMARTCARDS

13.1 Passwords issued to or created by staff should be regarded as confidential and must be kept secure. Password must not be communicated to anyone and staff must not use someone else's password to gain access to information.

13.2 Smartcards are issued to staff for their own use only. Smartcards must not be shared, must not be left unattended nor the password communicated to anyone else.

14 ABUSE OF PRIVILEGE

14.1 It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

14.2 The Data Protection Act legislates that there is a requirement for the Trust not to disclose third party information which may be held in a health record when someone is exercising their right of access, this cannot be complied with if staff directly access

their, a family member's or friend's record.

14.3 In addition, it is DoH policy that staff should not be in a more privileged position than the general public so that they should not be accessing their records when this is not something that is not available to the general public.

14.4 Seek out or looking at information or offering to sell information is an offence under the Data Protection Act and may attract an unlimited personal monetary fine and/or disciplinary action that may result in dismissal.

14.5 Requests for access should be made by writing to legal Services via the Trust Access to Health Records Policy & Procedure, even if a family member says they give their consent.

15 REPORTING BREACHES OF CONFIDENTIALITY

15.1 Breaches of confidentiality and near misses must be reported in accordance with the Incident Reporting & Management Policy & Procedure.

15.2 The Trust will formally write to patients, staff etc to explain and apologise for every personal data breach (except near misses) reported by the Trust and undertakes to provide details of the actions taken to prevent recurrence.

15.3 Failure to maintain patient or staff confidentiality or to not respect individual's disclosure decisions may result in disciplinary action.

16 CONFIDENTIALITY AUDITS

16.1 Good practice requires that all organisations that handle person identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems.

16.2 All work areas within the Trust, which process (handle) confidential patient information will be subject to confidentiality audit procedures.

17 TRAINING AND GUIDANCE

17.1 Training to implement this policy will be provided by the IG & RA Team at Corporate Induction and through the Data Security Awareness Training Workbook.

17.2 More specialised guidance on how to maintain patient and staff confidentiality and advice around consent and disclosure of confidential information is available from the IG & RA Team at IGHelp@qehkl.nhs.uk.

18 DISSEMINATION OF DOCUMENT

18.1 Following approval by the Information Governance Committee, this code of conduct will be uploaded onto the Trust intranet site under ICT and on the Information Governance intranet page. Policy notification will be through a broadcast email and through the Information Governance Newsletter.

19 REFERENCES

19.1 References to Standards

- Data Security & Protection Toolkit v.15
- NHS Care Record Guarantee
- NHS Constitution for England

19.2 Legislation

- European Union General Data Protection Regulation
- Computer Misuse Act (1990)
- Data Protection Act (2018)
- Human Rights Act (1998)
- NHS Act (2006)

19.3 Guidance

- Ensuring Security and Confidentiality in NHS Organisations (E5498)
- NHS Confidentiality Code of Practice (November 2003)
- NHS Confidentiality Code of Practice - Supplementary Guidance: Public Interest Disclosures (November 2010)

20 EQUALITY IMPACT STATEMENT

20.1 A Stage 1 (Screening) - Equality Impact Assessment has been undertaken and no negative impact on any group was indicated (see Appendix 1).

21 MONITORING COMPLIANCE

21.1 Compliance with this policy will be monitored in the following manner (see table below):

Key elements (Minimum Requirements)	Process for Monitoring (e.g. audit)	By Whom (Individual / group /committee)	Frequency of monitoring
Roles and responsibilities	Monitored at appraisal, following review of the individual's knowledge & skills framework (KSF) together with the job description.	Line manager	Annually
How the organisation provides IG Training. In house training sessions are delivered regularly throughout the year to meet the needs of the Trust	Electronic Staff Record (ESR) is utilised to identify all staff who are non- compliant	IG Team	Monthly

Reducing the number of confidentiality breaches	Management of incidents relating to Information Governance	IG Team	Monthly
Ensuring best practice across the Trust	Undertaking Information Security Audits (as part of Confidentiality Audits)	IG Team	Monthly

APPENDIX 1

EQUALITY IMPACT ASSESSMENT
Equality Impact Assessment Tool
(To be completed and attached to any policy document when submitted to the appropriate committee for ratification.)

STAGE 1 - SCREENING

Name & Job Title of Assessor: Phil Cottis – IG & RA Manager	**Date of Initial Screening: 07/05/10**
Policy or Function to be assessed: Confidentiality Code of Conduct	

		Yes/No	Comments
1.	**Does the policy, function, service or project affect one group more or less favourably than another on the basis of:**		
	• Race & Ethnic background	No	
	• Gender including transgender	No	
	• Disability:- This will include consideration in terms of impact to persons with learning disabilities, autism or on individuals who may have a cognitive impairment or lack capacity to make decisions about their care	No	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
2.	**Does the public have a perception/concern regarding the potential for discrimination?**	No	

Signature of Assessor: Phil Cottis **Date: 19th June 2018**
Head of Health Records & IG

Signature of Line Manager: Jon Wade **Date: 19th June 2018**
Chief Operating Officer

APPENDIX 2: CONFIDENTIALITY DOS AND DON'TS

Dos

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

Don'ts

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

APPENDIX 3: SUMMARY OF LEGAL AND NHS MANDATED FRAMEWORKS

The Trust is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Trust, who may be held personally accountable for any breaches of information security for which they may be held responsible. Trust shall comply with the following legislation and guidance as appropriate:

European Union General Data Protection Regulation

The European Union General Data Protection Regulation (GDPR) is a set of rules about how organisations should process the personal data of data subjects. GDPR lays out responsibilities for organisations to ensure the privacy and protection of personal data, provides data subjects with certain rights, and assigns powers to regulators to ask for demonstrations of accountability or even impose fines in cases where an organisation is not complying with GDPR requirements.

Lawful, fair and transparent processing

Organisations must process personal data in a lawful, fair and transparent manner ie:

- *Lawful* means all processing should be based on a legitimate purpose;
- *Fair* means organisations take responsibility and do not process data for any purpose other than the legitimate purposes; and
- *Transparent* means that organisations must inform data subjects about the processing activities on their personal data.

Limitation of purpose, data and storage

Organisations must limit processing, collect only that data which is necessary, and not keep personal data once the processing purpose is completed.

Data subject rights

The data subjects have the right to ask the organisation what information it has about them, and what the organisation does with this information. In addition, a data subject has the right to ask for correction, object to processing, lodge a complaint, or even ask for the deletion or transfer of his or her personal data.

Consent

As and when the organisation has the intent to process personal data beyond the legitimate purpose for which that data was collected, a clear and explicit consent must be asked from the data subject. Once collected, this consent must be documented, and the data subject is allowed to withdraw his consent at any moment.

Personal data breaches

The organisation must maintain a Personal Data Breach Register and, based on severity, the regulator and data subject should be informed within 72 hours of identifying the breach.

Privacy by Design

Organisations should incorporate organisational and technical mechanisms to protect personal data in the design of new systems and processes; that is, privacy and protection aspects should be ensured by default.

Data Protection Impact Assessment
To estimate the impact of changes or new actions, a Data Protection Impact Assessment must be conducted when initiating a new project, change, or product. The Data Protection Impact Assessment is a procedure that needs to be carried out when a significant change is introduced in the processing of personal data. This change could be a new process, or a change to an existing process that alters the way personal data is being processed.

Data transfers
The controller of personal data has the accountability to ensure that personal data is protected and GDPR requirements respected, even if processing is being done by a third party. This means controllers have the obligation to ensure the protection and privacy of personal data when that data is being transferred outside the organisation, to a third party and / or other entity within the same organisation.

Data Protection Officer
When there is significant processing of personal data in an organisation, the organisation should assign a Data Protection Officer. When assigned, the Data Protection Officer would have the responsibility of advising the organisation about compliance with EU GDPR requirements.

Awareness and training
Organisations must create awareness among employees about key GDPR requirements, and conduct regular training to ensure that employees remain aware of their responsibilities with regard to the protection of personal data and identification of personal data breaches as soon as possible.

Data Protection Act (2018)

The UK's third generation of data protection law has now received the Royal Assent and its main provisions will commence on 25 May 2018. The new Act aims to modernise data protection laws to ensure they are effective in the years to come.

What is the difference between the DPA 2018 and the GDPR?

The GDPR has direct effect across all EU member states and has already been passed. This means organisations will still have to comply with this regulation and we will still have to look to the GDPR for most legal obligations. However, the GDPR gives member states limited opportunities to make provisions for how it applies in their country. One element of the DPA 2018 is the details of these. It is therefore important the GDPR and the DPA 2018 are read side by side.

However, the DPA 2018 is not limited to the UK GDPR provisions.

What else does the DPA 2018 cover?

- The DPA 2018has a part dealing with processing that does not fall within EU law, for example, where it is related to immigration. It applies GDPR standards but it has been amended to adjust those that would not work in the national context.
- It also has a part that transposes the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. The Directive complements the General Data Protection Regulation (GDPR) and Part 3 of the DPA 2018sets out the requirements for the processing of personal data for criminal 'law enforcement

purposes'. The ICO has produced a detailed Guide to Law Enforcement Processing in addition to a helpful 12 step guide for quick reference.

- National security is also outside the scope of EU law. The Government has decided that it is important the intelligence services are required to comply with internationally recognised data protection standards, so there are provisions based on Council of Europe Data Protection Convention 108 that apply to them.

Human Rights Act (1998)

Article 8 of the Act refers to an individual's 'right to respect for their private and family life, for their home and for their correspondence'. This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

Computer Misuse Act (1990)

The Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

NHS Confidentiality Code of Practice (2003)

The NHS Confidentiality Code of Practice outlines for main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information;
- Inform patients of how their information is used;
- Allow patients to decide whether their information can be shared; and
- Look for improved ways to protect, inform and provide choice to patients.

The Caldicott Report (1997)

The report recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

1. Justify the purpose(s) of using confidential information;
2. Do not use patient-identifiable information unless it is absolutely necessary;
3. Use the minimum necessary patient-identifiable information that is required;
4. Access to patient-identifiable information should be on a strict need-to-know basis;
5. Everyone with access to patient-identifiable information should be aware of their responsibilities;

6. Understand and comply with the law;

The Caldicott 2 Report (2013) added a seventh principle:

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

APPENDIX 4: REPORTING OF POLICY BREACHES

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

All breaches should be reported to the IG & RA Manager via Datix. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager or Information Governance staff. The following list gives examples of breaches of this policy which should be reported:

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

Seeking Guidance
It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or Information Governance staff should be sought.

Reporting of Breaches
A regular report on breaches of confidentiality of person identifiable or confidential information shall be presented to the Information Governance Committee. The information will enable the monitoring of compliance and improvements to be made to the policy and procedures.