The Royal Wolverhampton Hospitals NHS
NHS Trust

OP97

Confidentiality Code of Conduct for staff □

Contents

Sections **Page**

1.0 Policy Statement [Purpose / Objectives of the policy]

The purpose of this code is to ensure everyone working within The Royal Wolverhampton NHS Trust (The Trust) is aware of their responsibilities when using confidential information and maintains the correct relationship with patients, staff and others while carrying out the business of the Organisation.

All staff 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 responsibilities but also a requirement within the Data Protection Act 2018 and, for health and other professionals, through their own professions' Code(s) of Conduct.

For the purpose of this code all data or information that can be related to an identifiable person is considered confidential; this includes patient and staff data and must only be used in line with this guidance and the law.

Staff may also come into contact with confidential non-person identifiable information, including for example commercially sensitive data or reports about the organisations business, which should be treated with the same degree of care.

The principle behind this policy is that no member of staff shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trusts security systems or controls to do so.

This policy has been written to meet the requirements of and inform staff about:

- The Data Protection Act 2018;
- UK General Data Protection Act;
- The Human Rights Act 1998;
- The Computer Misuse Act 1990;
- The legal framework governing confidentiality;
- Staffs' individual responsibilities with regard to compliance with the law;
- The information that is confidential;
- How to ensure information remains confidential;
- The systems and processes for protecting personal information;
- The circumstances under which confidential information can be disclosed;
- Who to approach in the Trust for assistance with disclosure issues;
- Possible sanctions for breaches of confidentiality; and
- Secure transfer of information.

A full list of Legislative requirements for the correct use and governance of information can be found in section 4.1.

This policy has been produced to protect staff by making them aware of the correct procedures and to minimise the risk of an inadvertent breach of any of these requirements.

2.0 Definitions

2.1 **Confidentiality**- is 'the entrusting of private matters to a person with reliance on their fidelity or competence' (The Oxford English Dictionary, Second Edition). The notions of trust and competence are vital. All employees are responsible for maintaining the confidentiality of information gained during their employment with the Trust.

2.2 **Personal identifiable information/data** - Is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number, Telephone Number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual this includes any person including patients, visitors, staff.

2.3 **Special Category Data** – the UK GDPR lists the following types of data which are likely to be more sensitive and may require extra protection.

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Safe Haven - is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-indefinable information can be held, received and communicated securely. Appendix 1.

3.0 Accountabilities

This policy applies to all staff, and external contractors who are employed to carry out work on behalf of The Trust, whether this is a temporary or time limited capacity. 3rd parties will be notified of their duties in the terms and conditions of their contract. Each individual is responsible for ensuring that they comply with relevant legislation and guidance for confidentiality of information and safe transfer of information

3.1 Director Accountabilities

3.1.1 **Chief Executive Officer** is the accountable officer for the Trusts activities, those relevant here are Information Governance and the system of Internal Controls

3.1.2 **Director of Nursing & Midwifery** is the Executive Lead with Governance under their remit and is responsible for ensuring governance arrangements are in place for the management of incidents, risks and complaints.

3.1.3 **Chief Medical Director/Caldicott Guardian** will ensure that there are robust policies in place to ensure that patient information will remain confidential and be seen only by those clinicians/staff authorised to see that data. They will ensure that breaches of this and other information governance policies in respect of patient information are investigated.

3.1.4 **Director of Finance & Information/ Senior Information Risk Officer (SIRO)** who acts as an advocate for information risk on the Board. They will ensure that breaches of this and other Information security policies in respect of the organisations information are investigated.

3.2 Specialist Staff

3.2.1 Medical Staff

Extract from General Medical Council "Confidentiality – Protecting and Providing Information" All Patients Confidentiality: good practice in handling patient information - ethical guidance - GMC (gmc-uk.org)

Patients have a right to expect that information about them will be held in confidence by their doctors. Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to give doctors the information they need in order to provide good care.

Extract form General Medical Council "0-18 years guidance: Sharing information with the consent of a child or young person"Children and young people 0-18 years - ethical guidance summary - GMC (gmc-uk.org)

Respecting patient confidentiality is an essential part of good care; this applies when the patient is a child or young person as well as when the patient is an adult. Without the trust that confidentiality brings, children and young people might not seek medical care and advice, or they might not tell you all the facts needed to provide good care.

3.2.2 Nursing staff

Extract from Nursing and Midwifery Council "The NMC Code of Professional Conduct: Standards for Conduct, Performance and Ethics" nmc-code.pdf As a registered nurse, midwife or health visitor, you must protect confidential information

3.2.3 Health Informatics Staff

All health informatics professionals shall, to the best of their ability, protect and promote the interests of patients and the public by:

- Ensuring that information systems and equipment for which they are responsible are procured, installed, maintained and operated professionally, efficiently and safely, and provide good value for the public money invested in them;
- Ensuring the security, confidentiality, accuracy, and integrity of information, and protecting the safety of patients and the public, both directly through their personal actions and indirectly through the design and operation of any information systems for which they are responsible;
- Reporting to appropriate authorities such as the Information Commissioner's Office on any improper or misleading use of information, whether accidental or deliberate, or misconduct by any person in connection with the procurement, operation or use of information systems and equipment; and

- Promoting the appropriate use of information to enhance patient and public involvement and to support patient empowerment, dignity and choice.

3.2.4 **Information Governance Lead** is responsible for coordinating information governance activities, providing advice and assistance across the Trust. Day-to-day administration of information governance through coordinating the implementation of the Data Security and Projection Toolkit (DSP Toolkit) and action plans and acting as the Trust's FOI Coordinator. Investigating suspected and actual breaches of confidentiality/security and undertaking reporting/remedial action as required.

3.2.5 **The Head of IT** will ensure that technical solutions are in place to protect all personal **and otherwise sensitive electronic information, wherever this information is accessed.**

3.2.6 Information Security Manager is responsible for coordinating information security activities, providing advice and assistance across the Trust. Continuously assessing the shortfall between security measures in place being effective and those established at a policy level thus highlighting deficiencies for remedial action. Investigating suspected and actual breaches of security and undertaking reporting/remedial action as required.

3.3 All Staff

3.3.1 **Management** responsibility for implementing all elements of information governance and providing, or accessing, appropriate levels of expertise e.g. Team Leaders/governance leads/matrons at departmental/sector level to take responsibility for daily working practice and report through their usual route.

3.3.2 **The Trust and all its employees**, whether they are on permanent, fixed term or temporary contracts, have a legal obligation and a duty of confidence to ensure that any information processed is done so in line with legal requirements and best practice. Staff are encouraged to report untoward incidents and identify risks, no matter how minor they appear, this would not only apply to clinical incidents but also to information security breaches, through the Trust's Risk Management processes.

3.3.3 **All staff** :

- Treat all information in the strictest confidence;
- Store all information safely when not in use, and destroy all out of date information securely, reference should be made to the NHSX Records Management code of Practice 2021 for destruction schedules;
- Wherever possible use anonymised information rather than person identifiable information and only disclose information for justifiable purposes;
- Only give information to those individuals who need to know that information and ensure that any individual, to who information is given, has a legitimate right to receive it;
- Personal and business data should be kept on the Trust's network drives. Do not keep person identifiable information on work laptops and computers or personal equipment;
- Ensure that all information received from, or sent to, another individual is secure in transit and that it is addressed correctly, whether the information is sent manually or electronically;

- Help to protect the physical security of areas in which information can be accessed, by ensuring that doors to computer and record rooms are physically secured and desks are clear;
- Maintain security of computer passwords and security codes to locked areas;
- Always log off or lock the computer before leaving a desk;
- Be vigilant of where conversations take place to prevent unintentional disclosure of information through overheard conversations;
- Never give person identifiable information over the telephone to an incoming caller;
- Always confirm identify of caller and legitimacy of the request;
- Ensure you are aware of the current local and national policies and procedures relevant to your role;
- Always report incidents relating to breaches of confidentiality verbally immediately to a Line Manager, the Local security Management Specialist and Information Governance Manager then via the incident report process. Breaches of this policy where there is suspicion of fraud or bribery, should be reported to the Local Counter Fraud Specialist as soon as practicable and in line with the Anti-Fraud, Bribery and Corruption Policy; and
- Review current flows of information, assess the risks and mitigate the risks immediately and raise any concerns to your Line Manager or the Information Governance Lead.

3.4 Committees/Boards

3.4.1 **Information Governance Steering Group**. The Chair of the IG Steering Group is the Medical Director and Caldicott Guardian. The IG Steering Group has responsibility for DSP Toolkit initiatives, implementation of IG strategy and Policy. The group will also review confidently and security breaches on a bimonthly basis, with any trends or SUI’s exception reported to Compliance Committee.

3.4.2 **Compliance Committee** will monitor compliance with the DSP Toolkit standards Risks, incidents and exceptions to compliance status will be reported to this Committee.

3.4.3 **Board Assurance Committee/ Trust Management Committee / Trust Board** Will receive risk and exception reports from compliance committee, which will include information governance issues, incidents, and risks.

3.5 Third Parties

Any third party with access to Trust data is also bound by law and guidance relating to confidentiality.

The specific responsibilities for confidentiality will be described in the third parties’ contract with the Trust including any extra confidentiality or non-disclosure statements where they are needed. Third parties must abide by the terms of their contract.

4.0 Policy Detail

4.1 Information Governance/Security – Legislative Requirements

List (non-exhaustive) of legislation and other guidance that is of relevance to information Governance and Information Security. Those in bold cover issues of security and governance directly, others listed may impact upon the use of information:

- UK General Data Protection Regulation
- Data Protection Act 2018
- The Abortion Regulations 1991
- ISO 27001
- ISO 27002
- ISO 27005
- The Access to Health Records Act 1990
- The Bribery Act 2010
- The Caldicott Principles
- The Carers (Recognition & Service) Act 1995
- The Children Act 1989 (sections 17, 27, 47 and Schedule 2)
- The Children Act 2004 (sections 10, 11 and 12)
- The Civil Contingencies Act (2004) Part 1 and supporting regulations.
- The Common law duty of Confidentiality
- The Computer Misuse Act 1990
- The Confidentiality: NHS Code of Practice
- The Copyright, Designs and Patents Act 1988
- The Crime & Disorder Act 1998
- The Crime and Disorder Act 1998 (section 115)
- The Criminal Procedures and Investigations Act 1996
- The Data Protection Act 2018
- The Education Act 1996 (sections 10 and 13), The Education Act 2002 (section 175)
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- The Equalities Act 2010
- The Fraud Act 2006
- The Freedom of Information Act 2000
- The Health Act 1999 (section 31)
- The Health and Safety at Work Act 1974.
- The Health and Social Care Act 2001 (Section 60)
- The Health and Social Care (Community Health and Standards) Act 2003
- The Health and Social Care Act 2008
- The Health and Social Care Act 2012
- The Human Fertilisation and Embryology Act 1990
- The Human Rights Act 1998
- Data Security and Protection Toolkit
- Information Security Management - BS7799|

- The Learning and Skills Act 2000 (sections 114 and 115)
- The Local Government Act 1972 (section 111)
- The Local Government Act 2000 (section 2)
- The Mental Capacity Act (MCA) 2005 and Deprivation of Liberty Safeguards (DOLS)
- The Mental Capacity Act 2005
- The Mental Health Act 1983
- The NHS & Community Care Act 1990
- The NHS (Venereal Disease) Regulations 1974
- The Records management: NHS code of practice
- The Regulation of Investigatory Powers Act 2000

4.2 Confidentiality Code of Conduct for staff– Practical Guide to Legal Framework for disclosure of information

4.2.1 Generally there are four main areas of law which constrain the use and disclosure of confidential information. These are briefly described below but are covered in more detail in the document; *Confidentiality: NHS Code of Practice 2003©*.

4.2.2 Data Protection Act 2018 (DPA)

DPA is designed to control the processing of personal data which includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. As well as information held on computers, the Data Protection Act 2018 applies to organised paper filing.

DPA identifies eight data protection principles that set out standards for information handling.

Data Protection Principle	What this means in practice
1. Processed fairly and lawfully	**Be open, honest and clear** There should be no surprises, so inform data subjects why you are collecting their information, what you are going to do with it and who you may share it with... • e.g. when formulating a research project remember to be open and transparent about what you will be doing with the information; • e.g. when working in a team, ensure that the patient/client is aware of who the members of the team are, and that all those involved with their care may need to see their notes.

2. Processed for specified purposes	**Only use personal information for the purpose(s) for which it was obtained.** Only share information outside your practice, team, home, ward, department or service if you are certain it is appropriate and necessary to do so. If in doubt, check first! • e.g. personal information on a Patient Administration System must only be used for healthcare purposes - not for looking up friends' addresses or birthdays.
3. Adequate, relevant and not excessive	**Only collect and keep the information you require.** It is not acceptable to hold information unless you have a view as to how it will be used. Do not collect information "just in case it might be useful one day!" • e.g. taking both daytime and evening telephone numbers if you know you will only call in the day; • Explain all abbreviations; • Use clear legible writing; and • Stick to the facts - avoid personal opinions and comments.
4. Accurate and kept up-to-date	**What mechanisms do you have for checking the information is accurate and up-to-date?** Take care inputting information to ensure accuracy How do you know the information is up-to-date? • e.g. each time a patient attends a clinic, they need to be asked to confirm that their details are correct - address, telephone number etc; • Check existing records thoroughly before creating new records; • Avoid creating duplicate records.
5. Not kept for longer than necessary	**Follow retention guidelines** NHSX Records Management Code of Practice 2021 • Check your organisation's retention policy; • Ensure regular housekeeping/spring cleaning of your information; • Do not keep "just in case it might be useful one day!"; • Check your organisation's disposal policy; • Dispose of your information correctly.

6. Processed in accordance with the rights of data subjects	**Patients have the right to see the information we hold about them** • Subject access- know how to handle these, DPA team in Health Records; • Patients have the right to prevent us processing their data if they wish; • Prevent processing for direct marketing - an end to junk mail and faxes; • Automated decision taking shouldn't be used, ask the patient for consent; • Compensation if we case them harm or distress; • Rectification/blocking/erasure of information we hold which the patient thinks is inaccurate; and • Request an assessment of the records we hold about them.
7. Protected by appropriate security (practical and organisational)	**Take practical steps to ensure information is kept confidential** • Ensure security of confidential faxes by using Safe Haven/secure faxes; • ALWAYS keep confidential papers locked away; • Do you have a clear desk policy?; • Ensure confidential conversations cannot be overheard; • Keep your password secret; and • Ensure information is transported securely.
8. Not transferred outside	**When sending patient information to others check who they are and where they are** • If sending personal information outside the EEA ensure consent is obtained from patients? And it the information adequately protected outside the EEA; • Be careful about putting personal information on websites - gain consent first; and • Check where your information is going e.g. where are your suppliers based? Fill in Information Sharing Agreements/Data Processing agreements, these can be found in the Information Sharing Policy.

More information can be found at the Information Commissioner's web site here: https://ico.org.uk

4.2.3 Common Law of Confidentiality

Although not written in statute, the principle of common law of confidentiality states that information confided should not be used or disclosed further.

Health care professionals hold information about patients that is private and sensitive. This information is collected to provide care and treatment to individuals and generally must not be used for other purposes without the individual's knowledge and consent.

Therefore, if you are told something 'in confidence' you are not at liberty to disclose the information without permission.

4.2.4 Caldicott Principles

The Caldicott Committee was established to review the confidentiality and security requirements across the NHS with regard to person identifiable information. The committee recommended a series of six principles that should be applied when considering whether such confidential information should be shared. These are now incorporated into the *Confidentiality: NHS Code of Practice 2003©*

These principles were developed with the aim of establishing the highest practical standards for handling confidential information.

The Caldicott Principles

1. Justify the purpose(s) of using confidential information;
2. Only use it when absolutely necessary;
3. Use the minimum that is required;
4. Access should be on a strict need-to-know basis;
5. Everyone must understand his or her responsibilities for confidentiality;
6. Understand and comply with the laws on confidentiality;
7. Sharing information is as important as the duty to protect; and
8. Inform patient/service users how confidential data is used.

4.2.5 Human Rights Act 1998

Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with the Data Protection Act 2018 and the common law of confidentiality should satisfy Human Rights requirements

There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g., disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need.

4.2.6 Administrative Law

Administrative Law governs the actions of public authorities to ensure that they operate within their lawful powers. The authority must possess the power to carry out what it intends to do and in particular be aware of any restrictions that this may place on the use or disclosure of confidential information.

Where such information is processed outside these powers then the processing may be unlawful. Unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place, e.g., by obtaining explicit patient consent

4.3 Confidentiality Code of Conduct for staff – What patients have a right to know

4.3.1 Consent issues

Patients must be informed about the use and disclosure of the information associated with their healthcare; and the choices that they have and the implications of choosing to limit how information may be used or shared.

The disclosure and use of confidential patient information needs to be both lawful and ethical. The law provides a minimum standard that does not always reflect the appropriate higher ethical standards that the government and the professional regulatory bodies require.

4.3.2 Providing patients with details on how we use their information

It is the responsibility of all employees to ensure patients are aware of what happens with the information they provide.

A public notice is available here: https://www.royalwolverhampton.nhs.uk/patients-and-visitors/privacy-ico/ which describes what information the Trust will collect to provide healthcare and how this will be used and shared to provide services.

A Patient information leaflet is also available here, or by contacting the medial illustration or health records department: https://www.royalwolverhampton.nhs.uk/patients-and-visitors/patient-information-leaflets/

To inform patients correctly staff will:

- Check where practicable that information leaflets on patient confidentiality have been made available to the patient upon request; and
- Make patients aware of the choices that they have and the implications of choosing to limit how information may be used or shared.

It is extremely important that patients are made aware of information sharing that must take place in order to provide them with high quality care.

Patients need to be made aware that by not consenting to certain disclosures they may be compromising their care. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient’s condition and medical history.

Whilst patients may understand that information needs to be shared between healthcare professionals, they may not be aware of sharing between different organisations involved in the provision of their healthcare.

Efforts must be made to inform them of everyone who will be sharing their information. This is particularly important where disclosure extends to non-NHS bodies.

Make clear to patients who the information could be disclosed to and where it will be recorded.

Address any concerns or queries the patient has.

Respect the right of the patients including their right to have access to their health records.

4.3.3 Staff Must:

- Follow the Trusts CP06 Consent Policy when using patient information for care purposes.
- Ask patients before using their personal information in ways that do not directly contribute or support the delivery of their care.
- Follow OP30 Policy on Research Governance when using patient information for research purposes.
- Respect patients' decisions to restrict the disclosure or use of information except where exceptional circumstances apply such as safeguarding issues or where medical ethics override non-disclosure.

4.4 Confidentiality Code of Conduct for staff – When is it lawful for me to share information?

The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. There are three circumstances where making disclosure of confidential information is lawful, which are:

- where the individual to whom the information relates has consented explicitly.
- where disclosure is in the substantial public interest; and
- where there is a legal duty to do so

4.4.1 Where the Individual to whom the Information relates has consented

The consent of an individual is one of the reasons for disclosing patient information. However, because health information is classified as special category data, consent must be explicit. Medical professionals must be able to prove without doubt and leaving no room for ambiguity, that the patient consented to disclosure. This means documentation of verifiable evidence.

4.4.2 Where disclosure is in the Substantial Public Interest

Health Care data sets do not just require public interest as a lawful basis for sharing, they require substantial public interest because they are classified as special category data. The legislation enshrining public interest unfortunately does not define it. However, whatever the definition is, it excludes private and commercial interests, may require independent assessment, and must comply with the principles of data protection in the UK GDPR, Article 5. For example, sharing must be limited to what is necessary. Disclosing the identity of a next of kin to law enforcement, does not imply disclosing their health records as well.

Benefit to interests other than the Trust's, documented policies stating the Trust's procedure for dealing with data sharing and the justification for not gaining consent, summarise the verification criteria for reliance on substantial public interest.

Substantial public interest conditions are recorded in the Data Protection Act 2018, Schedule 1, Part 2, Substantial Public Interest Conditions. The ICO explains how substantial public interest conditions work, here.

4.4.3 Where there is a Legal Duty to do so

In conformity with the laws of the UK, we may be constrained by legal obligation to share information. For example, where there is a court order specifically mentioning the Trust or other statutory obligation.

In every circumstance, it is important to retain the evidence you accepted to justify disclosure.

Any requests/requirements to share outside of the above, you MUST refer to OP85 Information Sharing Policy – Attachment 7 **for guidance.**

4.5 Confidentiality Code of Conduct for staff – Disclosing Information For Care

4.5.1 Caldicott Principles

Information on patients must only be released on a need-to-know basis. Any disclosure of information must follow the basic Caldicott principles for confidentiality

Refer to section 4.2.4 for the Caldicott Principles.

4.5.2 Disclosing information for care

In order to support staff in making decisions on patient consent to share information the Department of Health, in conjunction with the Information Commissioners office have developed disclosure models flow charts.

Confidentiality: NHS Code of Practice 2003 © Model B1 – Disclosures to support or audit healthcare Page 26. This chart can be used for:

a) Disclosures to NHS staff involved in the provision of healthcare	(Other trusts, Acute trusts or NHS Organisations) All NHS employees are bound by the NHS Code of Confidentiality. Information may be shared to provide care if the Caldicott principles are observed and you apply the checks listed in section **4.4.3** below. Information sharing agreements must be put in place to detail what information is regularly being shared with whom, and to formally agree that each organisation will abide by the laws and guidance on sharing information which apply to the NHS. Please see OP85 Information Sharing Policy for template agreements

	You can refer to the NHS Code of Confidentiality 2003 Page 40 for more guidance on each of these purposes or seek guidance from your manager or the Trust's Medical Director and Caldicott Guardian.
b) Disclosures to social workers or other staff of non-NHS agencies involved in the provision of healthcare	(Joint Health/Social Care Teams) E.g. substance misuse or community mental health services, social work teams. All team members will be bound by similar codes of confidentiality. Information may again be shared provided you proceed as above. Information sharing agreements must be put in place to detail what information is regularly being shared with whom, and to formally agree that each organisation will abide by the laws and guidance on sharing information which apply to the NHS. Please see OP85 Information Sharing Policy for template agreements
c) Disclosures to clinical auditors	(Audit/Commissioning) This information must be anonymised wherever possible. Helpful guidance can again be found in the Confidentiality: NHS Code of Practice 2003 © Pages 41 – 42. Remember that even anonymised data can lead to patients being identifiable e.g. if the data relates to a very small number of patients. Also just using the patient's postcode as a means of anonymising is not acceptable.
d) Disclosures to parents and guardians	(Parents and Guardians) Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidence as adults. Children under 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on and generally to have their confidence respected. • Explicit consent of a competent patient is needed before disclosing information to parents, guardians. • This may be agreed when confirming for next of kin details and what information will be given to next of kin about the patient's condition. (Relatives/ Friends) Relative and friends of patients may ask staff for updates on a patient's condition. • Explicit consent of a competent patient is needed before disclosing information to relatives or friends; and • Local protocols can be developed for each department/area where this will be carried out in practice to ensure all staff follow the same procedure

	and the risk of breach of confidentiality is minimised.
e) Disclosures to carers without parental responsibility	Carers often provide valuable healthcare and, subject to complying with the best practice outlined, every effort should be made to support and facilitate their work. Only information essential to a patient's care should be disclosed, not all details of the patient's condition/care will be appropriate to share with carers. • Explicit consent of a competent patient is needed before disclosing information to a carer; • The best interests of a patient who is not competent to consent may warrant disclosure; and • Patients must be made aware that this information is being shared and the reasons for this.

4.5.3 Practically staff will need to:

- Always check the member of staff is who they say they are and is authorized to see the information.
- Check the employee's ID badge and/or their internal extension number or bleep number or email address prior to giving them any information.
- Also check whether they are authorized to see the information. An authorised person is anyone who needs to know the information to fulfil the responsibilities of their post. Do not assume that all of your work colleagues are authorised to see the same information that you are.
- Don't be bullied into giving out information
- If in doubt, check with your manager or the health professional in charge of the patient's care.

4.6 Confidentiality Code of Conduct for staff – Disclosing information for other medical purposes

4.6.1 Information on patients must only be released on a need-to-know basis. Any disclosure of information must follow the basic Caldicott principles for confidentiality

Refer to section 4.2.4 for the Caldicott Principles.

4.6.2 In order to support staff in making decisions on patient consent to share information the Department of Health, in conjunction with the Information Commissioners office have developed disclosure models flow charts.

Confidentiality: NHS Code of Practice 2003 © Model B2 – Disclosures for other medical purposes Page 27

This chart can be used for:

- Disclosure to researchers;
- Disclosure to NHS Managers and/or the Department of Health, e.g., commissioning, prescribing advisers, financial audit, resource allocation etc;
- Disclosures to Occupational Health Practitioners;

- Disclosures to bodies with statutory investigative powers – GMC, the Health Service Ombudsman, CHAI;
- Disclosures to NHS Complaints Committees;
- Disclosure to cancer registries;
- Disclosure to hospital chaplains;
- Disclosure to non-statutory investigations;
- Disclosure to government departments;
- Disclosure to the police;
- Disclosure required by a court, including a coroner's court, tribunals and inquiries;
- Disclosure to Sure Start Teams;
- Disclosure to the media; and
- Disclosure to solicitors.

You can refer to the NHS Code of Confidentiality 2003 Pages 42 – 43 for more guidance on each of these purposes or seek guidance from your manager or the Trust's Medical Director and Caldicott Guardian.

To submit a request for Caldicott Guardian approval sharing for these other medical purposes, fill in the following form and send electronically to the Trust's Medical Director. Caldicott Form.

4.6.3 Practically staff will need to:

- Always check the member of staff is who they say they are and is authorized to see the information;
- Check the employee's ID badge and/or their internal extension number or bleep number or email address prior to giving them any information;
- Also check whether they are authorized to see the information. An authorised person is anyone who needs to know the information to fulfil the responsibilities of their post. Do not assume that all of your work colleagues are authorised to see the same information that you are;
- Don't be bullied into giving out information; and
- If in doubt, check with your manager or the health professional in charge of the patient's care.

4.6.4 Research

There may be different types of research taking place within the Trust; information disclosure will be dependent on the nature of each research project. Information will need to be either anonymised before use or explicit consent sought from research subjects. There is a strict Research Governance Framework which sets out to define standards and good practice in research, across all aspects of healthcare. The Framework applies to all those who participate in, host, fund, manage or undertake research. You must refer all cases of research to the Research and Development team within the Trust, contact details can be found on the Trusts intranet site, please also refer to OP30 Policy on Research Governance.

4.7 Confidentiality Code of Conduct for staff – Disclosing Information for Reasons Other Than Care

4.7.1 Information on patients must only be released on a need-to-know basis. Any disclosure of information must follow the basic Caldicott principles for confidentiality

Refer to section 4.2.4 for the Caldicott Principles.

4.7.2 In order to support staff in making decisions on patient consent to share information the Department of Health, in conjunction with the Information Commissioners office have developed disclosure models flow charts. Confidentiality: NHS Code of Practice 2003 © Model B3 – Disclosures for non-medical purposes Page 28

You can refer to the NHS Code of Confidentiality 2003 Pages 43 – 45 for more guidance on each of these purposes or seek guidance from your manager or the Trust's Chief Medical Officer and Caldicott Guardian.

To submit a request for Caldicott Guardian approval for one off or ad hoc sharing for these non-medical purposes, fill in the following form and send electronically the Trusts Medical Director. (Caldicott Form)

4.7.3 Others

E.g. Children's Centres, Education, Probation, Connexions
This is a complex area. Frequently there will need to be a specific Information Sharing Agreement between these agencies and the Trust for regular sharing, defining what information may be shared and with whom. Please see OP85 Information Sharing Policy for template Information Sharing Agreements and the process to follow for reviewing and approving these agreements

In the absence of any such agreement or if in any doubt, you can contact your manager or the Caldicott Guardian. There are Acts of Parliament (refer to section 4.1) that govern the disclosure/sharing of personal patient information, some make it a legal requirement to disclose and others state that information cannot be disclosed

4.8 Confidentiality Code of Conduct for staff – Information requests from police

4.8.1 Police access to health information

Police have no general right of access to health information, staff must not feel bullied to pass information to the police, rather a decision must be taken on a case-by-case basis if the police request access to health information.

There must be a written audit trail of police requests for information and the decision taken for each request.

Refer to OP07 Health Records Policy for detail.

4.8.2 When information can be shared with police:

There is no absolute definition of "serious crime", but section 116 of the Police and Criminal Evidence Act 1984 identifies some "serious arrestable offences":

- Treason;
- Murder and manslaughter;
- Rape and certain sexual offences;
- Kidnapping and the taking of hostages;
- Causing an explosion and offences under the prevention of terrorism legislation;
- Certain firearm offences;
- Hijacking;
- Causing death by reckless driving;
- Making a threat which if carried out would be likely to lead to:
  - a serious threat to the security of the state or to public order;
  - serious interference with the administration of justice or with the investigation of an offence;
  - death or serious injury;
  - substantial financial gain or serious financial loss to any person;
- Where risk to children is suspected and disclosure is necessary under the Children's Act 1989, Children's Act 2004, Working Together to Safeguard Children 2010; and
- Where a court order exists, the information can be shared with the police.

4.8.3 Handling Police requests

Request made by the Police, verbally and in writing, must be passed to the Health Records Team, contact details below.

Health Records Department
The Royal Wolverhampton NHS Trust
New Cross Hospital
Wolverhampton
WV10 0QP

Email: rwh-tr.healthrecordsaccess@nhs.net
Chat: MS Teams

4.9 Confidentiality Code of Conduct for staff – Information requests from media

4.9.1 How to handle Media requests

The Communications Department is responsible for handling media inquiries.

All media enquiries must come through the Communications Office. Any journalist contacting an officer directly must be referred to the Communications Office please refer to OP06 Media Relations Policy.

4.9.2 Media Relations Procedure for staff.

The Trusts OP06 Media Relations Policy covers the procedure you must follow as staff to:

- Handle Media Calls during office hours;
- Handle Media Calls out of hours;
- Contacting the media directly;
- Condition Checks- how consent to disclose details of a patient's condition will be sought;
- Using the Trust facilities for photography and filming to create materials for the wider media;
- High profile patients and visitors;
- Whistle blowing using the media (Whistleblowing Policy); and
- Trade union exemptions.

For any advice or guidance on any aspect of media relations, please contact the Communications Team on:

Tel: 01902 447297/442600 during office hours
Email: rwhtr.CommunicationDept@nhs.net

4.10 Confidentiality Code of Conduct for staff – Transferring/Sharing information safely by post, phone, transport (safe havens)

4.10.1 What is meant by sharing patient identifiable information safely?

Examples of transferring personal identifiable information are:

- taking a document and giving it to a colleague;
- making a telephone call; and
- passing information held on computer to another person.

In all cases, however simple or complicated, the principles of confidentiality and Data Protection apply, in order to ensure make sure personal identifiable information is not disclosed inappropriately.

4.10.2 What is a Safe Haven

The term safe haven is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-indefinable information can be held, received and communicated securely.

Safe haven procedures must be in place where staff are likely to receive personal information from other sites, or who may wish to send personal information to other sites. Please see Appendix 1 for a flow chart to follow for the safe haven process.

4.10.3 Location/security arrangements for safe havens

- The safe haven must be a room that is locked or accessible via a coded keypad known only to authorised staff; or
- The office or workspace must be sited in such a way that only authorised staff can enter that location i.e., it is not an area which is readily accessible to any member of staff who work in the same building or office, or any visitors;

- If sited on the ground floor, any windows must have locks on them;
- The room must conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage;
- Manual paper records contained person-identifiable information must be stored in locked cabinets;
- Computers must be not left on view or accessible to unauthorised staff and have a secure screen saver function and be switched off when not in use; and
- Equipment in the safe haven must have a code password and be turned off out of office hours.

4.10.4 **Post**

Best practice with regard to confidentiality requires that all correspondence containing personal information must always be addressed to a named recipient. This means personal information/data must be addressed to a person, a post holder, a consultant or a legitimate safe haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it must be addressed to an agreed post holder or team leader.

4.10.4.1 **Paper or electronic media**

When transferring paper notes, or electronic media such as CD or DVD disks or memory sticks, which contain personal identifiable information, make sure “Confidential” is marked in a prominent place on the front of the envelope. Ensure that the address of the recipient is correct and clearly stated, for example:

- Full name;
- Designation (job title);
- Department;
- Organisational address; and
- Write a return address on the back of the envelope – giving only generic details or PO Box Number.

Ensure arrangements are in place to check that post has been safely received e.g. asking the recipient by phone or e-mail that they have received the confidential information.

Use the tracking system to ensure the movement of post especially clinical notes so that the information can be followed throughout their journey and found if needed by others. Ask your line manager if you are unsure about this.

Please follow OP12 Information Security Policy -Encryption/ Removable media procedures to ensure any removable media being used to store and transport patient data are properly secured with encryption. Please see Appendix 1 for a flow chart to follow for the safe haven process.

4.10.4.2 **Use of Royal Mail Registered and recorded Delivery Services**

On occasions it will be deemed appropriate to use the Royal Mail Registered or Recorded Delivery services. In particular this will be for sensitive data. However, it will be the responsibility of the department manager to determine what the appropriate level of security in transit must be and address any cost implications.

4.10.5 **Approved Courier Service**

To use the Trust approved courier services please contact buying office in procurement on telephone: 01902 695483.

This is the only approved Trust method of using a courier service as this provides an audit trail of records being transported.

- Your department must record which records/information is being couriered;
- Check the identity of the courier when they arrive;
- Sign a log to document the handover of records from the Trust to the courier;
- Call the recipient to advise the records are being courier to them;
- Courier must get signed receipt of the records from the recipient; and
- Confirmation of receipt is received by department who sent the records.

Please see Appendix 2 for an example log of transporting records.

4.10.6 **Phone**

If a request for information is made by telephone,

- Always try to check the identity of the caller;
- Check whether they are entitled to the information they request;
- Take a number, verify it independently and call back if necessary;
- Be aware of bogus callers. These can be lone individuals, private investigators or individuals working for debt collection agencies who have been sub-contracted. Extreme vigilance is required at all times. Always verify a caller's details and ensure they are entitled to the information they are requesting before you release it. Alert your line manager if you suspect an instance of a bogus caller; and
- If you have any concerns about disclosing/sharing patient information you must discuss this with your manager and if they are not available, someone with the same or similar responsibilities. If you cannot find anyone to discuss the issue with you must take down the caller's details and ring them back when you are satisfied the disclosure of information can take place.

Please see Appendix 1 for a flow chart to follow for the safe haven process.

4.10.7 **Transport**

As part of remote or mobile working, it is often necessary that paper-based records are available. This would be the case for treating patients in their own home when using clinical records, or when attending tribunals using staff personnel records.

It is necessary that these records are handled with due care and responsibility and the following points may assist in this: -

- Use a case or sealed envelope or wallet to ensure the papers are kept together and nothing can blow away;
- Where several visits are involved, care must be taken to ensure only individual patient notes are required are taken into that patient's home. Other patients' records must remain in a secure locked container out of sight (the boot of a vehicle);
- Travel with car doors locked. A boot could easily be opened by someone at a set of traffic lights, as could a passenger door on the car next to where one's bag is placed;
- Transport documents directly to and from the place of work to the client's address. Do not make stops, for example at the local supermarket;
- Basic rule is that Personal Identifiable Data of patients of staff should not be taken home. Work files must be returned to the work base at the end of the working day;
- Locally it may be deemed necessary to take records home and this must be carefully considered by management and a risk assessment completed;
- Local procedures must be in place to identify those occasions on which the department management will allow such exceptions to the basic rule of not taking Personally Identifiable Data home. In this case records must be returned within 24 hours and staff must ensure that while away from the work base care records are stored safely and securely to avoid any breach of confidentiality;
- Local procedures must specify the responsibilities that staff have to protect those records while in their home and must not undermine any basic principle of confidentiality or security outlined in this policy and OP12 Information Security Policy;
- If documents are taken home at the end of the day, they must not remain in the car, even if it is locked in the garage. Bring the documents into the house and store them in what you consider to be a safe location. This must be somewhere where other occupants of the house will not casually look through them. They must not be left adjacent to doors or windows, they must be out of site and in a locked container/bag/draw;
- Staff are personally responsible for records they take off base;
- Write down local procedures to reflect local practice;
- Please see Appendix 1 for a flow chart to follow for the safe haven process; and
- Please also refer to OP07 Health Records Policy for detail on staff responsibilities for Tracking and Tracing records.

4.10.8 **Email/Electronic transfer**

Data can be sent by email securely from an nhs.net account or by use of a file transfer service e.g., egress, fast drive.

When sending personal identifiable information by email/electronic transfer;

- Personal and identifiable information must be encrypted;

- Sending details from and NHSmail account ending in .nhs.net to the following email accounts is automatically encrypted and considered secure:
    - .x.gsi.gov.uk;
    - .gsi.gov.uk; .
    - .gse.gov.uk;
    - .gsx.gov.uk;
    - .pnn.police.uk;
    - .cjsm.net;
    - .scn.gov.uk;
    - .gcsx.gov.uk, and
    - *.mod.uk*
- Email sent to any other address that is not secure must be sent with the inclusion of [secure] placed first in the subject title;
- Identifiable or potentially identifiable data transferred by electronic means must be sent separately from other information;
- Password protection can also be applied to further assure the security of personal data being transferred; and
- Passwords must be issued separately, preferably via telephone once the data are received.

Please also refer to email guidance within OP12 Information Security Policy.

4.10.10 **Local Protocols**

Local protocols must be developed where a service area or department has a variation of Trust procedure, or a requirement to meet other service specific or external standards. Local protocols must support information security and must not remove any of the minimum safeguards outlined in this policy.

Local protocols must be disseminated to all relevant staff, and the procedures followed to ensure maximum security of identifiable information.

4.11 Confidentiality Code of Conduct for staff – Professional responsibility to maintain confidentiality

4.11.1 **Contract of Employment**

The obligation to maintain confidentiality is either an expressed term of or expressed in your contract of employment and outlined in Trust Policy as a condition of service for all staff.

The Trust takes its responsibilities extremely seriously in respect of monitoring confidentiality. Any employee found to be in breach of the Trusts policy's on the appropriate use of information; accessing the Trust's information in any format without authorisation, or in passing on any information to persons not having the right to it, will be deemed to have breached confidentiality and their contract. Any breaches of this Policy where there is a suspicion of fraud or bribery, will be dealt with in line with the Anti-Fraud, Bribery and Corruption Policy. GP02 Anti-Fraud and Anti-Bribery Policy.

4.11.2 **Failure to observe this Confidentiality Code of Conduct**

- Could breach Legislation such as the Data Protection Act 2018;
- Could breach the rights of the people we hold personal information about;
- Could damage the reputation of the Trust;
- Will be regarded as misconduct;
- Could result in disciplinary action being taken against you;
- Could result in criminal investigation depending on the circumstances;
- Could lead to your conduct being reported to Professional Regulatory Bodies; and
- Could lead to legal action being taken against you by others.

4.11.3 **Staff accessing their own records.**

Staff are strictly forbidden from using the Trust's systems to access their own personal information unless specifically authorised to do so by a manager, or a written request has been made under the Data Protection Act to view information recorded about them.

4.11.4 **Staff accessing records of colleagues/friends/relatives**

Staff are also strictly forbidden to access personal information of colleagues, friends, or relatives unless they are directly involved in that patients care or staff management. If these records need to be accessed in your day-to-day duties you have a professional duty to keep this information confidential and only use it for work purposes.

4.11.5 **Confidentiality on computer systems**

Identifiable information must not be used in training, testing systems, or demonstrations without explicit consent. Test data must be used for this purpose.

Trust systems have the facility to monitor and record who has accessed patient and staff records, this information may be used if you are found to be breaching this or any other Trust policy and will be used as evidence in disciplinary matters.

4.12 Confidentiality Code of Conduct for staff – Seven golden rules of information sharing

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

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

4.12.3 **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible. You can get advice from you manager or the Data Protection Team.

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

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

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

4.12.7 **Keep a record** of your decision and the reasons for it – whether it is to share information or not.

- If you decide to share data, then record what you have shared, with whom and for what purpose.
- For patient and staff data a note must be made in the person's paper record or in their record on an electronic system.

5.0 Financial Risk Assessment

A financial risk assessment has been undertaken and no financial risks have been identified as a result of implementing this policy.

6.0 Equality Impact Assessment

An assessment has been undertaken, no adverse effects have been identified for staff, patients or the public as a result of implementing this policy.

7.0 Maintenance

This policy will be reviewed every 3 years or sooner if changes in legislation or guidance require. Responsibility lies with the Information Governance Steering Group.

8.0 Communication and Training

Approved Trust policies will be made available to staff via the Trusts intranet page.

All staff are required to complete Information Governance Training on an annual basis via Trust Induction and/or Mandatory training days. Please see OP41 Induction and Mandatory Training Policy. Where necessary to support specific roles and responsibilities a training needs analysis shall be reviewed by the IGSG.

This policy will be implemented and communicated through the work of the Information Governance Steering Group. An assessment of compliance with the requirements of the Data Security and Protection Toolkit will be undertaken each year. The Policy will be also implemented by the Information Governance Strategy which will set standards and a framework for monitoring.

9.0 Audit Process

Criteria	Lead	Monitoring method	Frequency	Committee
Data Security and Protection Toolkit sign off- confidentiality requirements	Medical Director	Report	Annual	Trust Board/ TMT
Incidents and breaches- IG Confidentiality	IG Lead	Report	Bi-monthly	IGSG
Complaints	IG Lead	Report	Bi-monthly	IGSG
Informing patients how their information will be used	Information Asset Owners	Information Asset Review	Annually and/or at the inception or entry into service of the Information Asset	IGSG
Informing patients how their information will be used	Data Protection Officer	Update of the Trust's fair processing notice	Ad Hoc	IGSG
Disclosing information	IG Lead	Update and review of Register of information sharing agreements	Ad Hoc	IGSG

10.0 References

The Royal Wolverhampton NHS Trust Policies and Strategies:

Policies

CP06 Consent Policy.

CP18 Clinical Photography, Video and Audio Recordings

OP07 Health Records Policy

OP13 Information Governance Policy

OP12 Information Security Policy

OP30 Policy on Research Governance

OP41 Induction and Mandatory Training Policy.

OP85 Information Sharing Policy

Strategies

Information Governance Strategy

Other sources

Definition of confidentiality used. The Oxford English Dictionary. Second Edition. (1989).Northamptonshire. Oxford University Press.

Department of Health (2010).The NHS Confidentiality Code of Practice <https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice>

National Information Governance Board (2011) The NHS Care Record Guarantee for England (version 5) < http://www.nigb.nhs.uk/pubs/nhscrg.pdf >

Part A - Document Control

Reference Number and Policy name: **OP97** **Confidentiality Code of Conduct for staff**	**Version:** **2.0 August 2022**		**Status: FINAL**	**Author: IG Officer** **Chief Officer Sponsor: Chief Medical Officer**
Version / Amendment History	**Version**	**Date**	**Author**	**Reason**
	V0.1	April 12	IG Lead	Creation
	V0.2	June 12	IG Lead	Consultation with Governance department
	V0.3	June 12	IG Lead	Trust Wide consultation and with Policy committee members
	V 1.0	Sept 12	IG Lead	New Policy approved TMT
	V 1.1	June 19	IG Lead	Reviewed by Medical Director – extended to December 2019 pending full review
	V1.2	April 2020	IG Lead	Reviewed by Medical Director – extended to August 2020 pending full review
	V1.3	August 2020	IG Lead	Reviewed by Medical Director – extended to December 2020 pending full review
	V1.4	July 2021	IG Lead	Reviewed by Chief Medical Officer – extended to November 2021 pending full review
	V2.0	June 2022	IG Lead	Review
Intended Recipients: All staff				
Consultation Group / Role Titles and Date: Information Governance Action Group - June 2022				

Information Governance Streering Group – October 2022	
Name and date of Trust level committee where reviewed	Trust Policy Group – August 2022
Name and date of final approval committee	TMC – October 2022
Date of Policy issue	November 2022
Review Date and Frequency [standard review frequency is 3 yearly unless otherwise indicated]	August 2025
Training and Dissemination: Policy will be placed on the Trust intranet and all staff informed via an AUB. Staff will complete annual Mandatory Information Governance Training.	
Publishing Requirements: Can this document be published on the Trust's public page: Yes **If yes you must ensure that you have read and have fully considered it meets the requirements outlined in sections 1.9, 3.7 and 3.9 of OP01, Governance of Trust-wide Strategy/Policy/Procedure/Guidelines and Local Procedure and Guidelines, as well as considering any redactions that will be required prior to publication.**	
To be read in conjunction with: CP06 Consent Policy OP30 Policy on Research Governance OP41 Induction and Mandatory Training Policy. OP85 Information Sharing Policy OP13 Information Governance Policy OP12 Information Security Policy Information Governance Strategy	
Initial Equality Impact Assessment [all policies]:	**Completed Yes**
Full Equality Impact assessment [as required]:	**Completed NA**
Monitoring arrangements and Committee	IGSG
Document summary / key issues covered: Confidentiality compliance to law and guidance. Expectations of staff for maintaining confidentiality. Maintaining confidentiality in practice, guidance on disclosing information to others. Safe haven procedures for sharing information by phone, fax, post and manual transfers. Consequences of failure to maintain confidentiality.	

Key words for intranet searching purposes	Confidentiality Conduct
High Risk Policy?	**No**

Part B **Ratification Assurance Statement**

Name of document: Confidentiality Code of Conduct for Staff

Name of author: Daniel Okonofua Job Title: Interim Head of Data Security & Protection/DPO

I, the above named author confirm that:

- The Strategy/Policy/Procedure/Guidelines (please delete) presented for ratification meet all legislative, best practice and other guidance issued and known to me at the time of development of the said document.

- I am not aware of any omissions to the said document, and I will bring to the attention of the Executive Director any information which may affect the validity of the document presented as soon as this becomes known.

- The document meets the requirements as outlined in the document entitled Governance of Trust- wide Strategy/Policy/Procedure/Guidelines and Local Procedure and Guidelines(OP01).

- The document meets the requirements of the NHSLA Risk Management Standards to achieve as a minimum level 2 compliance, where applicable.

- I have undertaken appropriate and thorough consultation on this document and I have detailed the names of those individuals who responded as part of the consultation within the document. I have also fed back to responders to the consultation on the changes made to the document following consultation.

- I will send the document and signed ratification checklist to the Policy Administrator for publication at my earliest opportunity following ratification.

- I will keep this document under review and ensure that it is reviewed prior to the review date.

Signature of Author: DUKHIME

Date: 04/08/2022

Name of Person Ratifying this document (Chief Officer or Nominee):
Job Title:
Signature:

- I, the named Chief Officer (or their nominee) am responsible for the overall good governance and management of this document including its timely review and updates and confirming a new author should the current post-holder/author change.

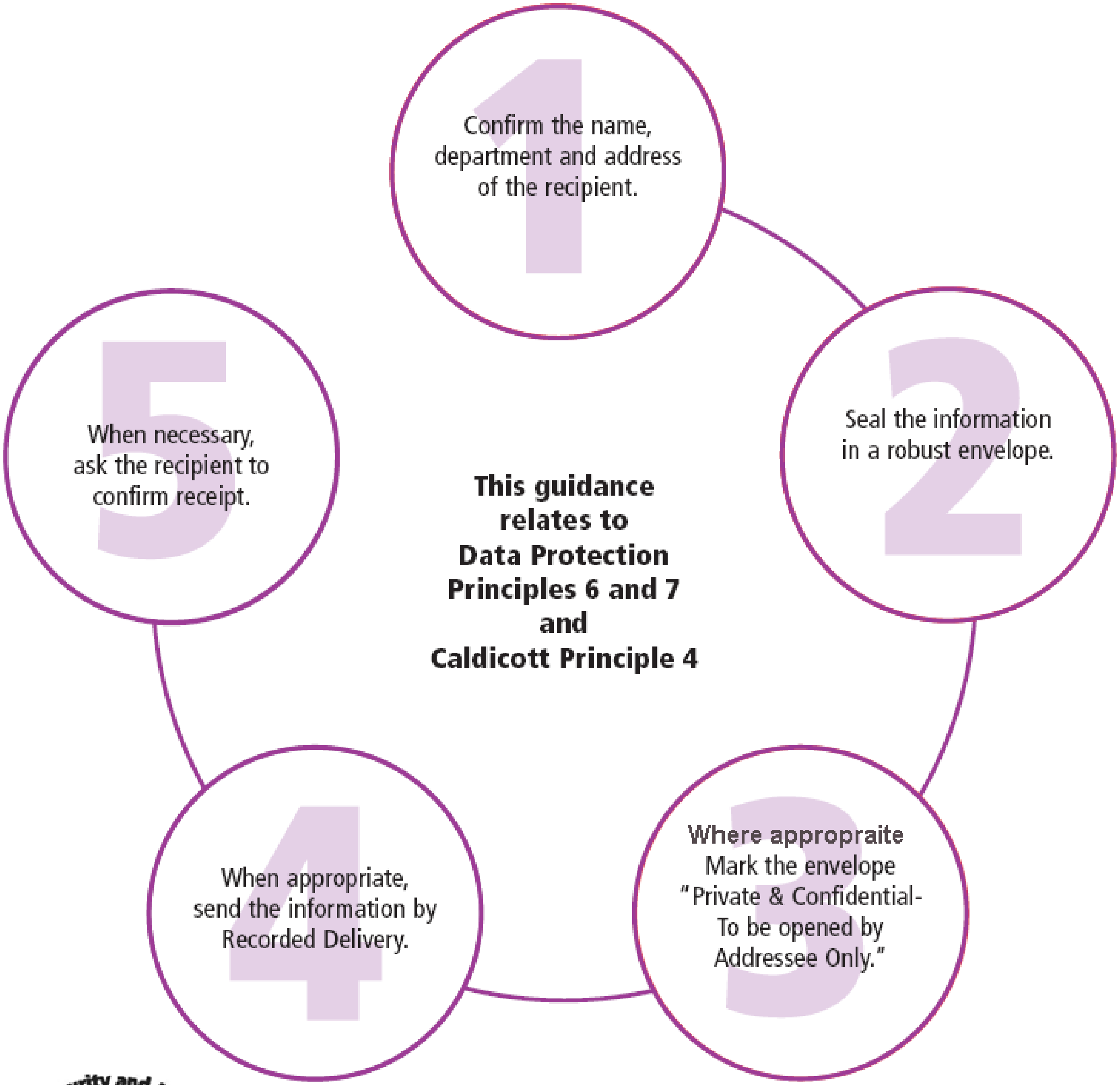
To the person approving this document:

Please ensure this page has been completed correctly, then print, sign and email this page only to:
The Policy Administrator

IMPLEMENTATION PLAN

Policy number and policy version	Policy OP97 Version 2.0	
Reviewing Group	Information Governance Action group	**Date reviewed:**
Implementation lead: Head of Information Governance/DPO		
Implementation Issue to be considered (add additional issues where necessary)	**Action Summary**	**Action lead / s (Timescale for completion)**
Strategy; **Consider** (if appropriate) Development of a pocket guide of strategy aims for staff Include responsibilities of staff in relation to strategy in pocket guide.	N/A	
Training; Consider Mandatory training approval process Completion of mandatory training form	N/A	
Development of Forms, leaflets etc; Consider Any forms developed for use and retention within the clinical record **MUST** be approved by Health Records Group prior to roll out. Type, quantity required, where they will be kept / accessed/stored when completed	N/A	
Strategy / Policy / Procedure communication; Consider Key communication messages from the policy / procedure, who to and how?	Staff will be informed by Team Brief	Policy Team / Comms
Financial cost implementation Consider Business case development	N/A	
Other specific Policy issues / actions as required e.g. Risks of failure to implement, gaps or barriers to implementation	N/A	

Guidance for sharing personal information by POST



1

Confirm the name, department and address of the recipient.

2

Seal the information in a robust envelope.

3

Where appropraite Mark the envelope "Private & Confidential- To be opened by Addressee Only."

4

When appropriate, send the information by Recorded Delivery.

5

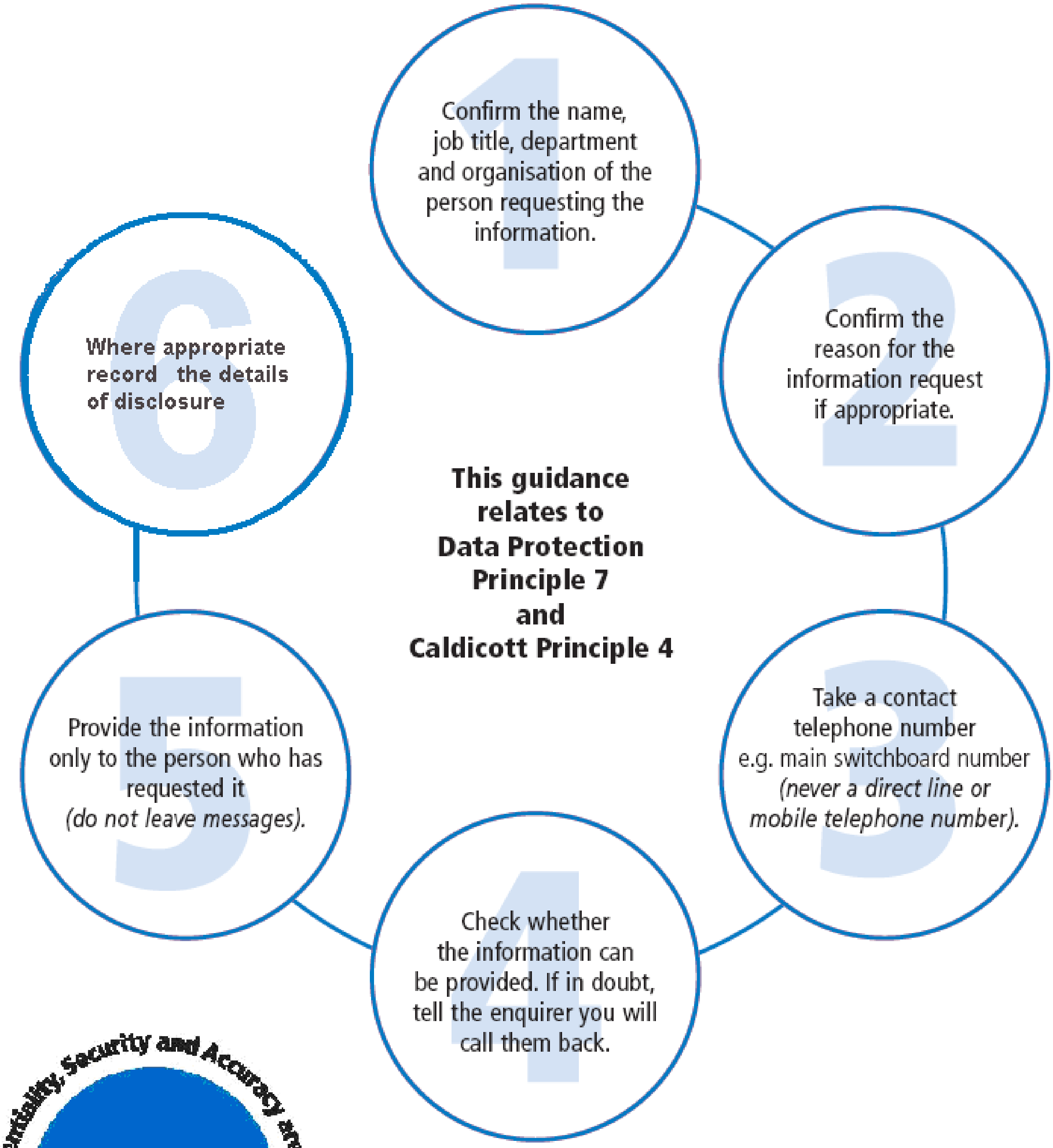
When necessary, ask the recipient to confirm receipt.

This guidance relates to Data Protection Principles 6 and 7 and Caldicott Principle 4

Information Confidentiality, Security and Accuracy are your Responsibility

Information Governance

Guidance for sharing personal information by PHONE



1 Confirm the name, job title, department and organisation of the person requesting the information.

2 Confirm the reason for the information request if appropriate.

3 Take a contact telephone number e.g. main switchboard number *(never a direct line or mobile telephone number).*

4 Check whether the information can be provided. If in doubt, tell the enquirer you will call them back.

5 Provide the information only to the person who has requested it *(do not leave messages).*

6 Where appropriate record the details of disclosure

This guidance relates to Data Protection Principle 7 and Caldicott Principle 4

Information Confidentiality, Security and Accuracy are your Responsibility

Information Governance

Guidance for **TRANSPORTING** personal information

1. Personal identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.

2. Record what information you are taking off site and why, and if applicable, where and to whom you are taking it.

3. Information must be transported in a sealed container.

4. Never leave personal identifiable information unattended.

5. Ensure the information is returned back on site as soon as possible.

6. Record that the information has been returned.

This guidance relates to Data Protection Principle 7 and Caldicott Principles 4 and 6

Information Confidentiality, Security and Accuracy are your Responsibility

nformation Governance

The Royal Wolverhampton Hospitals NHS
NHS Trust

Appendix 2

Confidentiality Code of Conduct for staff – Example Courier log

Service/Department Name:										
Service Head/Department Manager:										
Courier's ID Checked	**Date of dispatch:**	**Time of dispatch:**	**No items dispatched (i.e. 3 letters, 2 records) 5 items in total.**	**Dispatch Ref:**	**Name of dispatcher:**	**Name of intended recipient:**	**Organisation Name:**	**Courier Signature:**	**Recipient notified by phone of dispatch:**	**Date Receipt Returned: (Proof of delivery)**