The Royal Wolverhampton NHS Trust

# OP85
# Information Sharing Policy

**Contents**

**Sections** **Page**

## 1.0 Policy Statement

### 1.1 Summary

Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected.

There is an increasing emphasis on integrated working across services with the aim of delivering more effective intervention at an earlier stage across health and social care. Whether integrated working is through specific multi-agency structures or existing services, success for those at risk of poor outcomes depends upon effective partnership working and appropriate information sharing between services.

### 1.2 Purpose

- This policy comprises of a set of rules that the organisation must comply with when sharing any personal information with another partner agency or third party, whether this be patient or staff data.
- It sets out the standards that staff must follow when sharing personal data to ensure that legislation is not breached, and that confidentiality is maintained.
- It sets the templates which must be used to document any regular information sharing, to NHS or non-NHS organisations, whether these are within Wolverhampton or national/international organisations.
- This policy supports the overarching Wolverhampton Overarching Information Sharing Protocol and the legal requirements for sharing information please see Attachment 1

### 1.3 Scope

The sharing of anonymised or purely statistical information/data is outside of the remit of this policy, as the majority of legislation and rules concern only the sharing of personal information. However, the Purpose Specific Information Sharing Agreement (PSISA) template, see Attachment 4 created under this policy can be used to document any information sharing including anonymised or statistical information.

## 2.0 Definitions

| | |
|---|---|
| **Anonymised information/data** | Recorded details which do not have any reference to individuals and this information cannot be used in conjunction with any other publicly available information to identify an individual. |
| **Consent** | Any freely given, specific and informed indication of wishes by which the data subject signifies agreement to personal data related to them being processed. |
| **Data subject** | A person who we hold data/information about |
| **IG** | Information Governance |

| | |
|---|---|
| **IGSG** | Information Governance Steering Group. |
| **Information/Data** | Recorded details on a particular topic or person. For the purposes of this policy both terms are synonymous |
| **Information/Data Sharing Partner** | Another organisation or third party who the Trust is sharing data/information with. |
| **Information/Data sharing** | The disclosure of data from one or more organisations to a third-party organisation or many organisations, Data sharing can take the form of:<br>• a reciprocal exchange of data;<br>• one or more organisations providing data to a third party or parties;<br>• several organisations pooling information and making it available to each other;<br>• several organisations pooling information and making it available to a third party or parties;<br>• exceptional, one-off disclosures of data in unexpected or emergency situations. |
| **Need to know** | A staff member is allowed access to information if they require it to carry out their job, however not all staff in similar roles will have the same need to know. For example, a college not involved in caring for a patient has no need to know every detail of their care. |
| **Personal information/ Personal data** | Recorded details which relate to a living individual who can be identified from those data, or from those data and other information, which is in the possession of or is likely to come into the possession of the data controller. |
| **PSISA** | Purpose Specific Information Sharing Agreement – a template agreement to be filled in when the Trust is sharing information with a third party for a specific reason. |
| **PSDPA** | Purpose Specific Data Processing Agreement- a template agreement to be filled in when the Trust is allowing a third party to access the Trust data and process it for a specific reason. |
| **Trusted Partner** | A valid organisation that is known to the Trust via agreement to receive, posses, maintain and transfer data e.g., another NHS Trust, Police and local authorities. |

## 3.0 Accountabilities

### Caldicott Guardian

The Caldicott Guardian will be responsible for ensuring robust policies are in place to ensure that patient information will remain confidential, that information is shared appropriately in line with the law and NHS guidance, and that best interests of patients are maintained.

### Caldicott Guardian/Nominated Lead(s) for Information Sharing

The Caldicott Guardian may delegate operational responsibility for the policy, in cases of specific sharing activities to senior managers [e.g., heads of service] who will be known as Nominated Lead(s) for Information Sharing. These staff will ensure dissemination and use of this policy and associated template agreements and monitor the implementation and compliance of this framework within their own departments.

**Managers**
Managers have a responsibility to ensure that all members of staff are aware of this policy and the framework for sharing personal information. Managers should attend appropriate training, raise awareness, and ensure that their staff attend the appropriate training.

**All Staff/ Parties involved in information sharing**

- All staff have a duty of confidentiality and to ensure that individual rights in relation to the disclosure and use of personal information are understood and withheld. Please see OP97,Confidentiality Code of Practice for more detail on maintaining confidentiality.
- All staff have a responsibility to maintain accurate records, and to ensure that requests for information are specific, recorded and provided only on a "need to know basis".
- All staff should attend appropriate training covering confidentiality and information sharing by completing their annual Information Governance Mandatory Training, and any relevant supplementary training to aid the information sharing process suggested by the Information Governance Steering Group.
- If there is any doubt about whether information should be shared, disclosed or collected, staff should speak to their manager and/or Caldicott Guardian /Nominated Lead(s) for Information Sharing.

**Information sharing partners**
Both parties who agree to the information sharing template will ensure that each organisation's Caldicott Guardian or relevant confidentiality lead / senior member of staff is aware that they have overall responsibility for compliance with this policy and for the development and implementation of the procedures associated with the policy and data sharing/processing agreements.

A designated lead must be identified for each item of information sharing with relevant involvement in the sharing process. This lead will be responsible for the monitoring of the Information Sharing Agreement and producing monitoring reports to the Information Governance Steering Group as and when requested.

Every individual working for the organisations listed in an Information Sharing Agreement is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

**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 Data Security and Protection Toolkit initiatives, implementation of IG strategy and Policy. The Group will also review confidentiality and security breaches on a bimonthly basis, with any trends or Serious Untoward Incident's exception reported to QSAG Committee and sign off the Information sharing requirements for annual submission to NHS Digital

## 4.0 Policy Detail

### 4.1 Understanding the legal framework for information sharing

- The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates public sector information sharing.
- It is essential that practitioners sharing information are clearly aware of the legal framework within which they are operating.
- The purpose therefore of detailing the law within this protocol, is to highlight the legal framework that affects all types of personal information sharing, rather than to serve as a definitive legal reference point.
- This protocol has been developed in accordance with the ICO Data Sharing Code of Practice. https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-code/

### 4.2 List (non-exhaustive) of legislation and other guidance that is of relevance to information sharing:

- The Data Protection Act 2018
- The General Data Protection Regulations 2016
- The Freedom of Information Act 2000
- The Human Rights Act 1998
- The Mental Health Act 1983
- The Children Act 1989 (sections 17, 27, 47 and Schedule 2)
- The Children Act 2004 (sections 10, 11 and 12)
- The NHS & Community Care Act 1990
- The Access to Health Records Act 1990
- The Carers (Recognition & Service) Act 1995
- The Crime & Disorder Act 1998
- The Health Act 1999 (section 31)
- The Health and Social Care Act 2012 (Section 60)
- The Local Government Act 2000 (section 2)
- The Local Government Act 1972 (section 111)
- The Education Act 1996 (sections 10 and 13), The Education Act 2002 (section 175)

- The Learning and Skills Act 2000 (sections 114 and 115)
- The Crime and Disorder Act 1998 (section 115)
- The NHS confidentiality code of practice
- The Civil Contingencies Act (2004) Part 1 and supporting regulations.
- The Access to Health Records Act 1990
- The Mental Capacity Act 2005
- The Equality Act 2010

### 4.3 Legal context for information Sharing

Legislation, under which most public sector agencies operate, defines the role, responsibility, and power of the agency to enable it to carry out a particular function.

In many instances legislation tends to use broad or vague statements when it comes to the matter of sharing personal information, for example: the agency is required 'to communicate or will co-operate with' without actually specifying exactly how this may be done. This is because legislation that specifically deals with use of personal information (collection; use; storage; destruction; protection etc.) already exists namely, the Data Protection Act 2018.

Please refer to Attachment 1 for detail on the pertinent legislation.

### 4.3 Who might we share data with?

#### 4.3.1 Sharing with patients/relatives

Sharing information with patients is an important part of a professional's role and good communication is essential to the patient's positive experiences of care.

An information sharing agreement is not necessary to share information with patients or relatives; the basis for sharing information in these cases is consent.

Please see OP97, Confidentiality Code of Conduct for staff for more detailed guidance on this type of information sharing.

#### 4.3.2 Sharing to provide health or social care

Information sharing partners will cover a range of organisation types, some of which will also be providing care and will comply with the same standard of governance as the NHS. These partners will be considered "Trusted" organisations.

Trusted organisations will be those that can demonstrate they are attaining an acceptable level of information governance performance are those that are meeting the NHS Operating Framework key requirements.

An information sharing agreement is optional with "Trusted" organisations. However, in such situations, a protocol can also provide a useful and complete reference for the organisation of all the required actions to comply with the terms of the information sharing is best practice to document what information the Trust is sharing and with whom.

Some organisations who provide care are mandated to carry out IG assessments and ensure they reach an acceptable standard, such as:

- NHS organisations;
- Primary care organisations

Integrated Care Boards Others who are providing or supporting care will have a requirement to meet the key requirements because they are working with or for NHS organisations or have access to national NHS services and systems. This group will include some (but not all of) organisations such as:

- Adult social care services;
- Voluntary sector providers;
- Private sector care providers;
- Hospices.

### 4.3.3 Sharing for non-care purposes

Information sharing partners will also include organisations that are not supporting care but where sharing information can have a positive impact on service users. These organisations have no current requirement to carry out IG assessments or do not provide IG assurance in the same way, such as:

- the Police;
- district & borough councils;
- Children's centre teams;
- Multi Agency Support Teams (MAST)
- education services;
- housing services;
- research organisations;
- the Department for Work and Pensions;
- fire & rescue services;
- youth offending teams;
- court services;
- probation services;

- the Crown Prosecution Service.

An information sharing agreement is needed where the partner is not classed as "Trusted".

### 4.3.4 Quick reference table for Trusted Partners

The below table can be used as a quick reference table to understand when an information sharing agreement is always required and when it is optional.

| | Sharing for care purposes | Sharing for non-care purposes |
|---|---|---|
| **Recipient organisation is achieving the required level of information governance performance** | Sharing protocol is optional. | Sharing protocol necessary that focuses on the secondary uses in question, i.e., the purpose, constraints on re-use of information, retention periods and destruction policies. |
| **Recipient organisation is unable to demonstrate the required information governance performance** | Sharing protocol necessary that addresses the required information governance standards in the recipient organisation and the legal principles that apply. | Sharing protocol necessary that addresses the required information governance standards in the recipient organisation, the legal principles that apply and the additional standards associated with the secondary uses in question, (i.e., the purpose, constraints on re-use of information, retention periods and destruction). |

## 4.4 Guidance on mandatory information sharing

If you are asked, or wish, to share information, you must use your professional judgement to decide whether to share or not and what information it is appropriate to share, unless there is a statutory duty or a court order to share.

### 4.4.1 When is sharing mandatory?

**Statutory Duties**

Each public sector organisation for example, education, social care, health or justice, will have "statutory functions or powers" given to them by the government and the law. If the sharing of information is written within the functions or powers of that organisation then sharing information for that purpose is allowed.

Refer to Attachment 2 for the flowchart to determine if sharing should be undertaken.

There are other laws which say sharing data to protect others is allowed.

| | |
|---|---|
| To improve the physical and mental health of the population and to prevent, diagnose and treat illness. | • National Health Service Act 1977<br>• Health Act 1999 |
| Safeguarding adults or children from harm | • The Children Act 1989 (sections 17, 27, 47 and Schedule 2)<br>• The Children Act 2004 (sections 10, 11 and 12)<br>• The Mental Capacity Act (MCA) 2005 and Deprivation of Liberty Safeguards (DOLS)<br>• The Mental Capacity Act 2005<br>• The Mental Health Act 1983 |
| To prevent or detect a crime and carry out justice | • The Data Protection Act 2018<br>• The Crime & Disorder Act 1998<br>• The Crime and Disorder Act 1998 (section 115)<br>• The Criminal Procedures and Investigations Act 1996 |
| Reporting diseases or dangerous occurrences to protect the health and safety of others. | • The Reporting of Injuries, Diseases and Dangerous Occurrences (Amendment) Regulations 2012<br>• Public Health (Control of Disease) Act 1984 |

This list is not exhaustive and there may be other statutory requirements to disclose information that arise during the lifetime of this policy.

Refer to OP07 Health Records Policy for further guidance on how to process requests for data e.g., police requests, court orders.

### 4.5 Guidance on one-off sharing

For clarity, an information sharing agreement is not required where the sharing is for an ad hoc request for information around a single patient or service user. Examples of such requests will include the following:

- when a service user moves house and registers to receive care from another organisation;
- where a service user registered in one part of the country seeks emergency services from another;
- where a service user is referred to a care provider outside of their catchment area for specialist treatment. The basis for all these types of sharing would be the patient or service user consenting to their information being shared so they can receive a service.

If the Trust receives an ad hoc request to share information about a large number of patients/service users, then you should consider;

1. Can the request be met using anonymised or pseudonymised data, which removes all information that could be used to identify patients or service user and replaces it with a reference number. If so then this option should be used,

and the sharing of non-personal data does not require an information sharing agreement filled in.

2. If it is necessary to identify the patient/service users in the sharing of data then an information sharing agreement is needed.

### 4.6 Guidance on deciding to share information

To inform your decision making this section sets out further information in the form of seven key questions about information sharing:

| | |
|---|---|
| **1.** Is there a clear and legitimate purpose for you or your agency to share the information? | • Is there any specific legislation containing express powers or which imply powers to share information.<br>• Is there a court order to share?<br>• Is there at least one reason under schedule 2 and one under schedule 3 of the Data Protection Act to allow you to share information? |
| **2.** Does the information enable a living person to be identified? | 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. |
| **3.** Is the information confidential? | Confidential information is:<br>• personal information of a private or sensitive nature; and<br>• information that is not already lawfully in the public domain or readily available from another public source; and<br>• information that has been shared in circumstances where the person giving the information could reasonably expect that it would not be shared with others.<br>This is a complex area, and you should seek advice if you are unsure. |
| **4.** If the information is confidential, do you have consent to share? | The person whose information you are sharing has been told what kind of information about them you will be sharing, with who and why. The person has had opportunity to raise any concerns and have you address them.<br><br>Consent can be verbal or written, though it is best practice to have written consent for sharing information. Consent can also be implicit or explicit<br><br>**Implied consent**<br>Consent to disclosure of information can be taken to be implied when needed to provide healthcare. An example |

of implied consent is where a GP refers a patient to a hospital specialist and the patient agrees to the referral. In this situation the GP can assume the patient has given implicit consent to share information with the hospital specialist

**Explicit consent**
Explicit consent must be sought for the use of information outside of care purposes unless there is a legal reason to disclose the information. Explicit consent is where a patient has expressed that they agree to disclosure of information, this should always be documented. An example of explicit consent is where a person has agreed or asked to be involved in a research trial, where their information will be shared with a drugs company.

**If consent is given information can be shared.**

**Competence to consent**

- **Children and Young People**

Everyone aged 16 or over is presumed to be competent to give consent for themselves unless the opposite is demonstrated.

The Trust acknowledges that, children between the ages of 12 and 16 who have the capacity and understanding to make decisions about their own treatment are also entitled to decide whether personal information may be passed on and to have their confidence respected.

If a child is not able to demonstrate competence to consent, someone with parental responsibility may do so on their behalf. Please see CP06 Consent to Treatment and Investigation Policy the Trust policy on consent to treatment for further advice on identifying competence.

- **Patients with a disability**

Seeking consent may be difficult, either because patients' disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they have a difficulty communicating their decision (be it to consent or object).

Extra care must be taken to ensure that information is provided in a suitable format or language that is accessible (e.g., providing large print or Braille versions of leaflets for those with reading difficulties) and to check that it has been understood.

Failure to support those with disabilities could be an offence under the Equality Act 2010 and may prevent

| | |
|---|---|
| | consent from being gained. Support for communicating with patients having specific disabilities can be obtained from the Trusts PALS department.<br><br>• **Where patients are unable to give consent - With-holding Information or Disclosing Information without consent**<br>If a patient is unconscious or unable, due to a mental or physical condition, to give consent or to communicate a decision, the health professionals concerned must take decisions about the use of information. This needs to take into account the patient's best interests and any previously expressed wishes and be informed by the views of relatives or carers as to the likely wishes of the patient. If a patient has made his or her preferences about information disclosures known in advance, this should be respected.<br><br>Please see the Trust's Mental Capacity and Deprivation of Liberty (MCA DOLA) pages for more information on making decisions on behalf of a patient. |
| **5.** If consent is refused, or there are good reasons not to seek consent to share confidential information, is there a sufficient public interest to share the information? | There will be some circumstances where you should not seek consent from the individual or their family or inform them that the information will be shared. For example, if doing so would:<br>• place a person (the individual, family member, yourself or a third party) at increased risk of harm<br>• prejudice the prevention, detection, or prosecution of a serious crime<br>• lead to an unjustified delay in making enquiries about allegations of significant harm to a child, or serious harm to an adult.<br><br>The key factors in deciding whether or not to share confidential information without consent are necessity and proportionality, i.e., whether the proposed sharing is likely to make an effective contribution to preventing the risk and whether the public interest in sharing information overrides the interest in maintaining confidentiality. |
| **6.** If the decision is to share, are you sharing information appropriately and securely? | If you decide to share information, you should share it in a safe and secure way. Please see OP97 Confidentiality Code of Conduct for staff Policy for more guidance on how to share information safely by phone, courier etc.<br><br>You will need to ensure that you:<br>• share only the information necessary for the purpose for which it is being shared;<br>• understand the limits of any consent given; especially if the information has been provided by |

| | |
|---|---|
| | a third party;<br>• distinguish clearly between fact and opinion;<br>• share the information only with the person or people who need to know;<br>• check that the information is accurate and up-to-date;<br>• share it in a secure way, for example, confirm the identity of the person you are talking to; ensure that a conversation or phone call cannot be overheard; use secure email; ensure that the intended person will be on hand to receive a fax;<br>• establish with the recipient whether they intend to pass it on to other people, and ensure they understand the limits of any consent that has been given; and<br>• inform the person to whom the information relates and, if different, any other person who provided the information, if you have not done so already and it is safe to do so. |
| **7.** Have you properly recorded your information sharing decision? | You should record your decision and the reasons for it, whether or not you decide to share information. If the decision is to share, you should record what information was shared and with whom. |

### 4.7 Which information sharing agreement should you use?

The Trust has signed up to use a 3-tier structure for information sharing agreements as set out in the Wolverhampton Overarching Information Sharing Protocol. The sharing structure is as shown in the diagram in Attachment 3.

The 3-tier structure sets out:

| | |
|---|---|
| Tier 1 – Wolverhampton Overarching Information Sharing Protocol. | This document is a high-level policy document common to all organisations delivering health, social and community services, across an area.<br>Signed by Chief Executives. |
| Tier 2 – Information Community Agreements | These documents are high-level agreements common to organisations delivering a specific function or service which may cross health, social and community services.<br>Reviewed by Governance and signed by Service Directors or the equivalent. |

| | | |
|---|---|---|
| Tier 3 – Purpose Specific Agreements | These documents are the lowest level agreement which details what is being shared, with who, why, and for what period of time.<br><br>Staff should use the templates below to document any sharing. | |
| | Purpose Specific Information Sharing Agreement (PSISA) | Used when we share with a third party who use the shared data to provide a service or function.<br><br>Attachment 4 |
| | Purpose Specific Data Processing Agreement (PSDPA) | Used when we allow a third party to access Trust data to carry out a service on our behalf.<br><br>Attachment 5 |

For more information on the 3 Tiers, what they cover and when they should be used please refer to Attachment 6.

For a flow chart to help you decide which agreement to use please use Attachment 7.

### 4.8 Seven golden rules of information sharing

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.
2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible. You can get advice from your manager or the Information Governance Team.
4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.

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

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

## 5.0 Financial Risk Assessment

| | | |
|---|---|---|
| 1 | Does the implementation of this policy require any additional Capital resources | No |
| 2 | Does the implementation revenue resources of this policy require additional | No |
| 3 | Doe the implementation of this policy require additional manpower | No |
| 4 | Does the implementation of this policy release any manpower costs through a change in practice | No |
| 5 | Are there additional staff training costs associated with implementing this policy which cannot be delivered through current training programmes or allocated training times for staff | No |
| | Other comments | |

## 6.0 Equality Impact Assessment

An equality analysis has been carried out and it indicates that:

| Tick | Options |
|---|---|
| X | A. There is no impact in relation to Personal Protected Characteristics as defined by the Equality Act 2010. |
| | B. There is some likely impact as identified in the equality analysis. Examples of issues identified, and the proposed actions include: |

## 7.0 Maintenance

This policy will be reviewed every 3 years or sooner if changes in legislation/ guidance require, or there are changes which arise from overarching area or region wide sharing protocols. 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 Committee. 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 |
|---|---|---|---|---|
| DSP Toolkit sign off- Information sharing requirements | Chief Medical Director | Report | Annual | Trust Board/ TMC |
| DSP Toolkit compliance – Information sharing requirements | Chief Medical Officer / IG Lead | Online evidence submission | Bi-annual | IGSG |
| Informing patients how their information will be used | IG Lead | Update of the Trust Fair Processing Notice | Ad Hoc | IGSG |
| Review list of sharing partners – Caldicott Log | IG Lead | Caldicott Report | Quarterly | IGSG |

## 10.0 References

**The Royal Wolverhampton NHS Trust Policies and Strategies:**

Wolverhampton Overarching Information Sharing Protocol

OP12 Information Security Policy

OP13 Information Governance Policy

OP41 Induction and Mandatory Training Policy. OP97

OP97 Confidentiality Code of Conduct for staff

*Other sources*

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

The Information Commissioners Office. (2011). ICO: Data Sharing Code of Practice https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

HM Government: (2008). Information sharing advice for safeguarding practitioners Information sharing advice for safeguarding practitioners - GOV.UK (www.gov.uk)

## Part A - Document Control

| **Policy number and Policy version:**<br><br>**Version 3.0** | **Policy Title:**<br><br>**OP85 Information Sharing Policy** | **Status:**<br><br>**Final** | | **Author:**<br><br>**IG Lead**<br><br>**Chief Officer Sponsor:**<br><br>**Chief Medical Officer/Caldicott Guardian** |
|---|---|---|---|---|
| Version / Amendment History | Version | Date | Author | Reason |
| | V0.1 | Oct 2009 | IG Officer | Creation |
| | V1.0 | Dec 2009 | IG Officer | Approved version |
| | V1.1 | May 2012 | IG Lead | Align policy with Wolverhampton overarching agreement |
| | V1.2 | June 2012 | IG Lead | Consultation with Governance department |
| | V 2.0 | Sept 2012 | IG Lead | Consultation with IGSG members and Trust wide and Policy Committee Members |
| | V 2.1 | June 2019 | IG Lead | Reviewed by Medical Director – extended to December 2019 pending full review |
| | V2.2 | April 2020 | IG Lead | Reviewed by Medical Director – extended to August 2020 pending full review |
| | V2.3 | August 2020 | IG Lead | Reviewed by Medical Director – extended to December 2020 pending full review |
| | V2.4 | January 2021 | IG Lead | Reviewed by Medical Director – extended to September 2021 pending full review |
| | V2.5 | January 2022 | IG Lead | Reviewed by Medical Director – extended to March 2022 pending full review |
| | Version 3.0 | July 2022 | IG Lead | Full review undertaken |
| **Intended Recipients:** All staff | | | | |
| **Consultation Group / Role Titles and Date:** IGSG, Policy Group | | | | |

| | |
|---|---|
| **Name and date of Trust level group where reviewed** | IGSG – October 2022<br>Trust Policy Group – October 2022 |
| **Name and date of final approval committee** | Trust Management Committee – October 2022 |
| **Date of Policy issue** | November 2022 |
| **Review Date and Frequency** (standard review frequency is 3 yearly unless otherwise indicated – see section 3.8.1 of Attachment 1) | October 2025 (Three-yearly) |
| **Training and Dissemination:** Policy will be made available to all staff on Trust intranet page, Information Governance Mandatory Training required annually. | |
| **Publishing Requirements: Can this document be published on the Trust's public page:**<br><br>**Yes**<br><br>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:**<br>Wolverhampton Overarching Information Sharing Protocol OP12<br>Information Security Policy<br>OP13 Information Governance Policy<br>OP41 Induction and Mandatory Training Policy.<br>Confidentiality Code of Practice<br>ICO: Data Sharing Code of Practice<br><br>HM Government: Information Sharing: Guidance for practitioners and managers | |
| **Initial Equality Impact Assessment (all policies):** **Completed: Yes**<br>**Impact assessment (as required):** **Completed: N/A** | |
| **Monitoring arrangements and Committee** | IGSG |
| **Document summary/key issues covered.**<br>Circumstances where we must share information One<br>off sharing<br>How to reach a decision on sharing information<br>Template agreements to use when sharing<br>Sharing and consent<br>Sharing for care and non-care purposes | |
| **Key words for intranet searching purposes** | |

| | |
|---|---|
| **High Risk Policy?**<br>**Definition:**<br>• Contains information in the public domain that may present additional risk to the public e.g. contains detailed images of means of strangulation.<br>• References to individually identifiable cases.<br>• References to commercially sensitive or confidential systems.<br>If a policy is considered to be high risk it will be the responsibility of the author and chief officer sponsor to ensure it is redacted to the requestee. | **Yes / No (delete as appropriate)**<br>If Yes include the following sentence and relevant information in the Intended Recipients section above –<br>In the event that this is policy is made available to the public the following information should be redacted: |

Part B **Ratification Assurance Statement**

Name of document: Information Sharing Policy

Name of author: Job Title:

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:

Date:

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**

**To be completed when submitted to the appropriate committee for consideration/approval**

| | | |
|---|---|---|
| **Policy number and policy version** | **OP85: Information Sharing Policy** | |
| **Reviewing Group** | **IGSG** | **Date reviewed:** |
| **Implementation lead: Print name and contact details** | | |
| **Implementation Issue to be considered (add additional issues where necessary)** | **Action Summary** | **Action lead / s (Timescale for completion)** |
| Strategy; **Consider** (if appropriate)<br>1. Development of a pocket guide of strategy aims for staff<br>2. Include responsibilities of staff in relation to strategy in pocket guide. | | |
| Training; Consider<br>1. Mandatory training approval process<br>2. Completion of mandatory training form | | |
| Development of Forms, leaflets etc; Consider<br>1. Any forms developed for use and retention within the clinical record **MUST** be approved by Health Records Group prior to roll out.<br>2. Type, quantity required, where they will be kept / accessed/stored when completed | | |
| Strategy / Policy / Procedure communication; Consider<br>1. Key communication messages from the policy / procedure, who to and how? | | |
| Financial cost implementation<br>Consider Business case development | | |
| **Other specific Policy issues / actions as required e.g. Risks of failure to implement, gaps or barriers to implementation** | | |

# Information Sharing Policy – Legislation

## Legal context for information Sharing

- Legislation, under which most public sector agencies operate, defines the role, responsibility and power of the agency to enable it to carry out a particular function.

- In many instances legislation tends to use broad or vague statements when it comes to the matter of sharing personal information, for example: the agency is required 'to communicate or will co-operate with' without actually specifying exactly how this may be done. This is because legislation that specifically deals with use of personal information (collection; use; storage; destruction; protection etc.) already exists namely, the Data Protection Act 2018.

- The Data Protection Act 1998, in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data). In general, recorded information held by public authorities about identifiable living individuals will be covered by the Data Protection Act 1998. It is important to take account of whether the information is held in paper records or in automated form (such as on computer or on a CCTV system): some of the provisions of the Data Protection Act 1998 do not apply to certain paper records held by public authorities. Broadly speaking, the eight data protection principles set out in Schedule 1 to the Data Protection Act 1998, and discussed further below, will apply to paper records held in a "relevant filing system" or an "accessible record", but not to other paper records.

- The Data Protection Act 1998 does not set out to prevent the sharing of personal information. To the contrary, providing that the necessary conditions of the Act can be met, sharing is perfectly legal. It is important to share information, when appropriate to do so, as to withhold it. Each information sharing episode needs to be assessed on its own merits.

## Administrative Law

- The principles of administrative law regulate the activities of public bodies; these principles are mainly enforced by way of claims for judicial review in the courts. The courts do not generally review the merits of public law decisions but consider the legality, rationality or procedural propriety of decisions made by public bodies. The rules relating to illegality are most relevant to data sharing: a public body may not act in excess of its powers. If it does act in excess of its powers, then the act is said to be ultra vires. Acts within a public body's powers are said to be intra vires. Under the Human Rights Act 1998, an act of a public authority may be unlawful on the basis that it is contrary to the ECHR. Where questions involving the Convention are involved, the Court will need to consider the merits of the decision more closely than would be the case where the traditional administrative law principles are involved.

- Local authorities derive their powers entirely from statute and cannot act outside those limited statutory powers. Most of these statutory powers relate to specific local authority functions. In addition to these specific powers, section 111 of the Local Government Act 1972 provides that local authorities are empowered to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions. Section 2 of the Local Government Act 2000 confers a wide (but not unlimited) power on local authorities to promote the well-being of their area.

- There is no general statutory power to disclose data, and there is no general power to obtain, hold or process data. As a result, it is necessary to consider the legislation that relates to the policy or service that the data sharing supports. From this, it will be possible to determine whether there are express powers to share data, or whether these can be implied. Express powers to share data are relatively rare and tend to be confined to specific activities and be exercisable only by named bodies. Implied powers will be more commonly invoked. Alternatively it may be possible to rely on section 111 of the 1972 Act or section 2 of the 2000 Act as a basis for data sharing.

- The starting point in relation to implied powers or in relation to section 111 of the 1972 Act must be the power to carry out the fundamental activity to which data sharing is ancillary. If there is no power to carry out that fundamental activity then there can be no basis for implying a power to share data or for relying on section 111 of the 1972 Act.

- A statutory power must be exercised for the purpose for which it is created. If it is not, the exercise of the power will be ultra vires.

**Administrative powers**

- Express statutory powers: Express statutory powers can be permissive or mandatory.

- Express permissive statutory powers (or gateways) to share data include section 115 of the Crime and Disorder Act 1998 (which allows persons to share information with relevant authorities where disclosure is necessary or expedient for the purposes of the Act) and regulation 27 of the Road Vehicles (Registration and Licensing) Regulations 2002 (which, among other things, permits the Secretary of State to make particulars in the vehicle registration register available for use by a local authority for any purpose connected with the investigation of an offence or of a decriminalised parking contravention). Examples of mandatory statutory gateways include: section 17 of the Criminal Appeal Act 1995, which makes it obligatory for a public body to provide information, when requested, to the Criminal Cases Review Commission in connection with the exercise of its functions; and section 6 of the Audit Commission Act 1998, which imposes a legal obligation on the Council to provide relevant information to the Audit Commission.

- Local authorities are only able to do what is expressly or by implication authorised by statute. The following statutory powers are relevant, in addition to the specific powers mentioned above:

- Section 111 of the Local Government Act 1972, which provides that a local authority has power to do anything, which is calculated to facilitate, or is conducive or incidental to, the discharge of any statutory functions.

- Section 2 of the Local Government Act 2000, which provides that a local authority has power to do anything likely to achieve the promotion or improvement of the economic, social or environmental well-being of the area.

**Data Protection Act 1998**

The key principles of the Data Protection Act are:

1. Personal Data must be processed (e.g. collected, held, disclosed) fairly and lawfully and that processing must satisfy one of the conditions in schedule 2 of the Act. The processing of sensitive data is further protected in that processing must also satisfy at least one of the conditions in schedule 3 of the Act.

2. Personal Data shall be obtained and processed for only one or more specific and lawful purpose(s).

3. Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s).

4. Personal Data shall be accurate and kept up to date.

5. Personal Data shall not be held for longer than is necessary.

6. Processing of Personal Data must be in accordance with the rights of the individual.

7. Appropriate technical and organisational measures should protect Personal Data.

8. Personal data should not be transferred outside the European Union unless adequate protection is provided by the recipient.

With few exceptions the Data protection Act 1998 requires anyone processing personal information to notify (register) with the Information Commissioner.

- The registration details include the type of information held, the purpose of use and who the information may be disclosed to. It is therefore essential that anyone considering sharing personal information establishes that their registration covers who they may disclose information to, or what information they may collect (when receiving shared information). If their registration does not cover these matters adequately, amendments must be registered with the Information Commissioner.

- The first and second principles of the Data Protection Act are crucial when considering information sharing. In essence, these require that personal information should be obtained and processed fairly and lawfully and that personal information should only be used for a purpose(s) compatible with the original purpose.

- Schedules 2 and 3 of the Act set out conditions that must be met before personal information can be processed fairly and lawfully – For personal information to be processed lawfully, one of the conditions in Schedule 2 must be met. For sensitive personal information, one of the conditions in Schedule 3 must also be met.

- Sensitive information, as defined by the Act, includes information concerning a person's physical or mental health; sexual life; ethnicity or racial origin; political opinion; trade union membership; criminal record or details of alleged offences etc.

- In order for there to be no misunderstanding, on anyone's part, it is always advisable for the 'collector' of the information to ensure that the person is made fully aware of why the information is needed, what will be done with it, who will have access to it, their rights and if appropriate seek to inform consent of the individual concerned before sharing that information. This will usually be done via the use of Privacy Notices.

- There are circumstances where information can be shared even if informed consent has not been given. These include the following:

    - Section 29 of the Act permits disclosure for the purposes of prevention or detection of crime, or apprehension or prosecution of offenders, and where those purposes would be likely to be prejudiced by non-disclosure.

    - Disclosure is also permitted where information has to be made public, or where disclosure is required by law.

    - For the purposes of the common law duty of confidentiality, if there is no informed consent, this is the point where the need for confidentiality would have to be balanced against countervailing public interests – again preventing crime is accepted as one of those interests. See the more detailed discussion of confidentiality, below.

    - For the purposes of the Human Rights Act 1998, Article 8 – Right to respect for private and family life, would need to be considered. See the more detailed discussion of Article 8, below.

- The Data Protection Act gives individuals various rights in respect of their own personal data held by others, namely the right to:

    - Access to their own information (subject access request).

    - Take action to rectify, block, erase or destroy inaccurate data.

    - Prevent processing likely to cause unwarranted substantial damage or distress.

    - Prevent processing for the purposes of direct marketing.

  - To be informed about automated decision taking processes.
  - Take action for compensation if the individual suffers damage.
  - Apply to the Information Commissioner or the court to have their rights under the Act enforced.

- Section 7 of the Act, gives an individual the right to access the information held about themselves, irrespective of when the information was recorded or how it is stored (manual or electronic).
- Disclosure of information held on an individual's record that identifies or has been provided by a third party is subject to certain restrictions (e.g. section 7(4) and the exemption provided by section 30 of the DPA).
- The Act provides the holder of the information a limited number of exemptions to decline/refuse access to an individual's record which are set out under Part IV of the Act.
- The Data Protection Act 1998 does not apply to personal information relating to the deceased person.

  The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 apart from section 3.1.(f) which continues to provide a right of access to the health records of deceased person made by their personal representatives and others having a claim on the deceased's estate.
  In all other circumstances, disclosure of records relating to the deceased person should satisfy common law duty of confidence.
  It is also worth noting that third party information that is held within a record of a deceased person is still covered by the Data Protection Act 1998, where the third party is still alive.

- **Schedule 2** of the Data Protection Act 1998 specifies conditions relevant for the processing of any personal data, namely:

  1. The data subject has given his/her consent to the processing, or
  2. The processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract, or
  3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract, or
  4. The processing is necessary to protect the vital interests of the data subject.
  5. The processing is necessary-for the administration of justice for the exercise of any functions conferred on any person by or under any enactment for the exercise of any functions of the Crown, a Minister of the Crown or a government department for the exercise of any other

functions of a public nature exercised in the public interest by any person, or

6. The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

- **Schedule 3** of the Data Protection Act 1998 specifies additional conditions relevant for the processing of sensitive personal data. In addition to meeting a condition set out in schedule 2, at least one other condition must be met in schedule 3, namely:

1. The data subject who the sensitive information is about has given his/her explicit consent, or
2. The processing is necessary to comply with employment law, or
3. The processing is necessary to protect the vital interests of the:
    a. the individual, (where consent cannot be given or reasonably obtained), or
    b. another person, (where the individual's consent has unreasonably been withheld), or
4. In the course of legitimate activities of specified non-profit organisations and does not involve disclosing personal data to a third party unless the individual has consented. Extra limitations apply to this condition, or
5. The individual has deliberately made the information public, or
6. Processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights, or
7. Processing is necessary for administering justice, or for exercising statutory or government functions, or
8. Processing is necessary for medical purposes, and is undertaken by a health professional or someone who is subject to an equal duty of confidentiality, or
9. To monitor equality of opportunity and is carried out with appropriate safeguards for the rights of the individual.

Further conditions relating to the processing of sensitive personal information are detailed in Data Protection (Processing of Sensitive Personal Data) Order 2000.

**Human Rights Act 1998 and European Convention on Human Rights**

- The Human Rights Act 1998(the HRA) gives effect to the principal rights guaranteed by the European Convention on Human Rights (the Convention). In general, it is unlawful under the HRA for a public authority to act inconsistently with any of the Convention rights.

- Article 8.1. of the European Convention on Human Rights (given effect via the Human Rights Act 1998), provides that "everyone has the right to respect for his private and family life, his home and his correspondence."

- This is however, a qualified right i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights.

- Article 8.2 of the European Convention on Human Rights provides "there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

- In the event of a claim arising from the Act that an organisation has acted in a way which is incompatible with the Convention rights, a key factor will be whether the organisation can show, in relation to its decision(s) to have taken a particular course of action:

    - that it has taken these rights into account;

    - that it considered whether any breach might result, directly or indirectly, from the action, or lack of action;

    - if there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;

        - (if qualified rights) whether the organisation has proceeded in the way mentioned below. "Evidence of the undertaking of a 'proportionality test', weighing the balance of the individual rights to respect for their privacy, versus other statutory responsibilities e.g. protection of others from harm, will be a significant factor for an organisation needing to account for its actions in response to claims arising from the Act".

**Crime and Disorder Act 1998**

- The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.

- Section 115 of the Act provides a power (not a statutory duty) to exchange information between partners where disclosure is necessary to support the local Community Safety Strategy or other provisions in the Crime and Disorder Act. This power does not over ride other legal obligations such as

compliance with the Data Protection Act (1998), the Human Rights Act (1998) or the common law duty of confidentiality.

- Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service, fire brigades or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Act.

- Whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the information. It should be noted, however, that this does not exempt the provider from the requirements of the second Data Protection principle.

**Common Law Duty of Confidentiality**

- All staff working in both the public and private sectors should be aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this.

- A duty of confidence arises when one person (the "confidant") is provided with information by another (the "confider") in the expectation that the information will only be used or disclosed in accordance with the wishes of the confider. If there is a breach of confidence, the confider or any other party affected (for instance a person whose details were included in the information provided) may have the right to take action through the courts.

- Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, the Department of Health and relevant professional bodies accept that there is an ethical duty to respect the confidentiality of the dead.

**Exemptions to the duty of confidentiality**

- The duty of confidence is not absolute and the courts have recognised three broad circumstances under which confidential information may be disclosed. These are as follows:

    - Disclosures with consent. If the person to whom the obligation of confidentiality is owed (whether an individual or an organisation) consents to the disclosure this will not lead to an actionable breach of confidence.

    - Disclosures which are required or allowed by law. "Law" in this context includes statute, rules of law, court orders etc.

    - Disclosures where there is an overriding public interest (e.g. to protect others from harm).

    - The courts have generally taken the view that the grounds for breaching confidentiality must be strong ones.

- The duty of confidence only applies to person identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.

- Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained before disclosure of their information. Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence.

**Caldicott Principles**

- Although not a statutory requirement, NHS and Social Care organisations are committed to the Caldicott principles which encapsulate the above mentioned statutes when considering whether confidential information should be shared. These are:

  - Justify the purpose(s) for using personal information.

  - Only use personal information when absolutely necessary.

  - Use the minimum amount of personal information that is required.

  - Access to personal information should be on a strict need to know basis.

  - Everyone with access to personal information must be aware of his/her responsibilities.

  - Everyone with access to personal information must understand and comply with legislation that governs personal information.

**Access to Health Records Act 1990**

Within the governance structures and processes of healthcare organisations, Practitioners have been given professional accountability to protect specific 1st and 3rd party statements. This may include clinical assessments, diagnostics and results as well as sections of sensitive care plans and progress notes.

**The Children Act 2004**

- The Children Act 2004 created the legislative framework for developing more effective and accessible services focused around the needs of children, young people and families by ensuring co-operation, clearer accountability and safeguarding of children. The key event, which led to these proposals for fundamental change, was the death of Victoria Climbie. This demonstrated that there were major flaws within the systems

and structures for safeguarding and ensuring the welfare of children and young people.

Main provisions of the Act:

- A duty on agencies to co-operate to improve the well being of children and young people
- A duty to safeguard and promote the welfare of children
- A power to set up a new database with information about children

- Summary of the Children Act 2004

The following is a brief account of the key parts of the Act that specifically relate to the Change for Children programme in England.
Children's Services in England – Part 2

1. Section 10 establishes a duty on Local Authorities to make arrangements to promote co-operation between agencies in order to improve children's well-being, defined by reference to the five outcomes and a duty on key partners to take part in those arrangements. It also provides a new power to allow pooling of resources in support of these arrangements.

2. Section 11 creates a duty for the key agencies who work with children to put in place arrangements to make sure that they take account of the need to safeguard and promote the welfare of children when doing their jobs.

3. Section 12 allows further secondary legislation and statutory guidance to be made with respect to setting up indexes that contain basic information about children and young people to help professionals in working together to provide early support to children, young people and their families. Case details are specifically ruled out of inclusion in the indexes.

**Civil Contingency Act 2004 – Part 1**

This deals with information sharing between responder bodies, as identified in the Act, as a distinct duty under the Act and as a means of achieving other duties under the Act, and is summarised below:

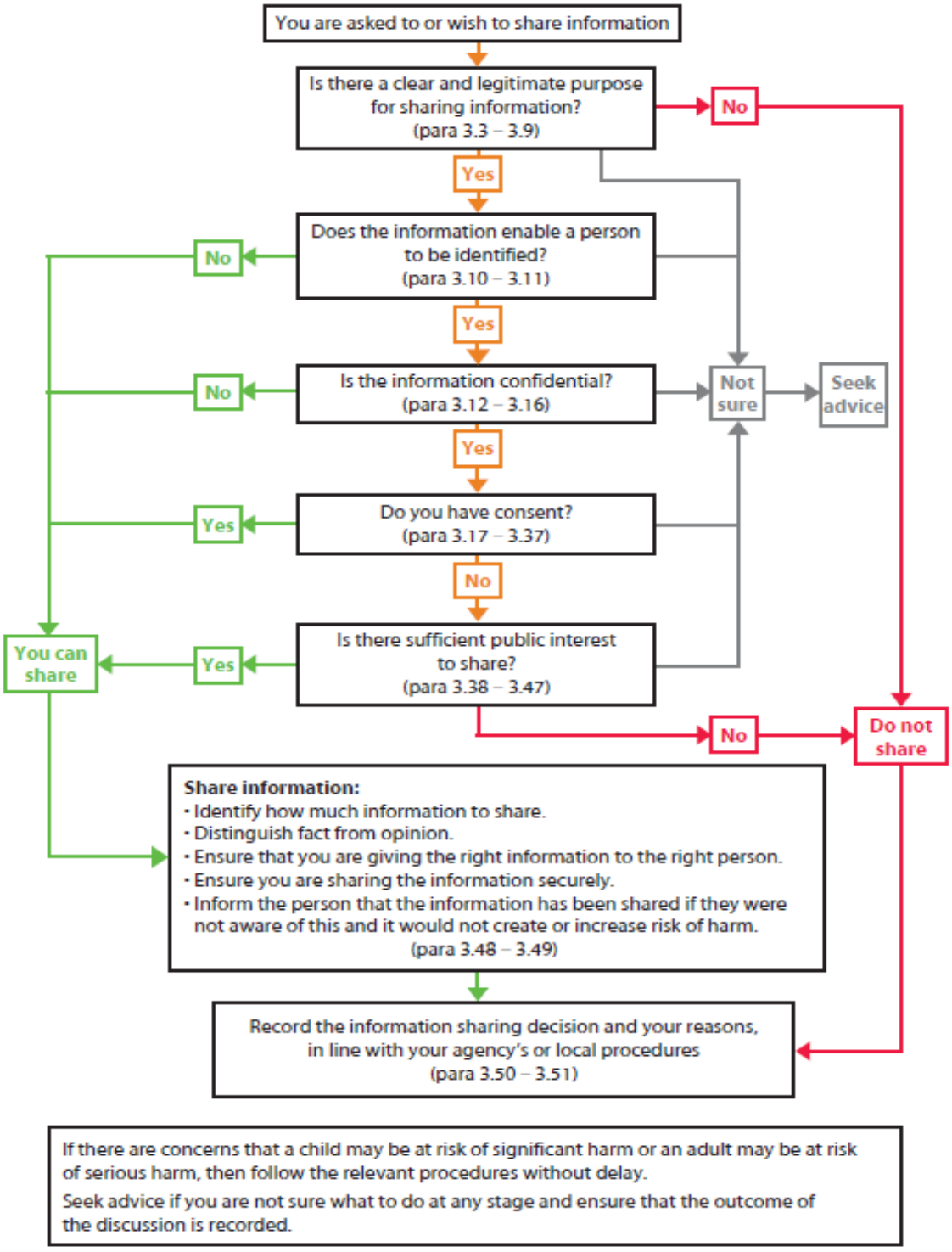
- Information sharing is a crucial element of civil protection work, underpinning all forms of co-operation.
- The initial presumption is that information should be shared, but that some information should be controlled if its release would be counter productive or damaging in some other way.
- There are various types of information. Information may be suitable for some audiences, but not for others. Also, the circulation of information can be limited to certain classes of organisation or individual.
- In most instances, information will pass freely between responders, as part of a more general process of dialogue and co-operation.

- However, a formal system exists to request information in circumstances where that is necessary.
- Information may also be accessible from open sources, and responders should endeavour to use this route as well.
- Not all information can be shared. Responders may claim exceptions in certain circumstances (and, as a result, not supply information as requested).
- Exceptions relate to sensitive information only. Where the exceptions apply, a responder must not disclose the information. (Readers of this document are advised to read Chapter 3 of the Guidance Notes to the Civil Contingency Act 2004)

**OP85 Attachment 2**

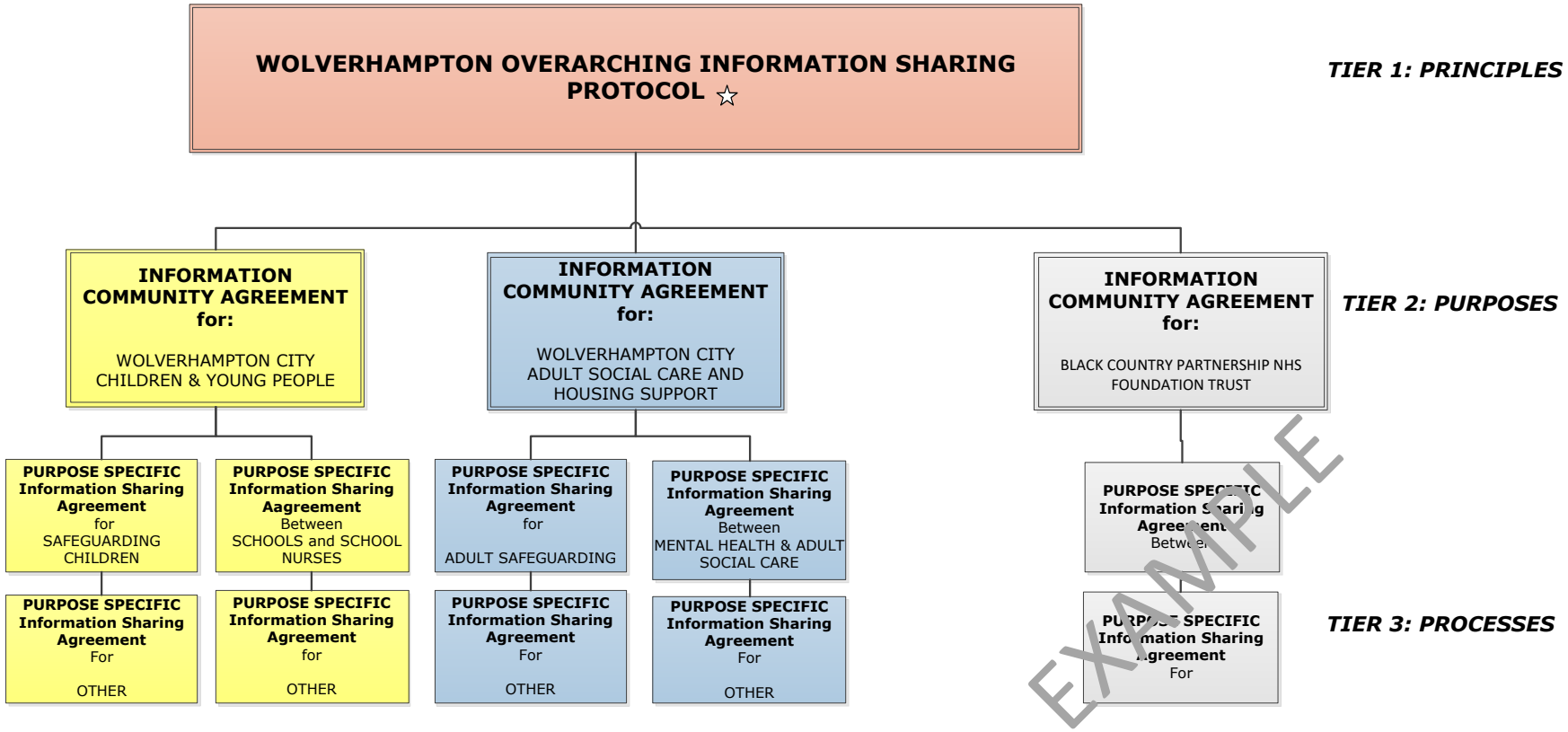
## Information Sharing Policy – Guidance on Deciding To Share Information Data Flow

To inform your decision making this section sets out further information in the form of seven key questions about information sharing:



Reference: HM Government: Information Sharing: Guidance for practitioners and managers

**Attachment 3**




☆ Main agencies represented in multi-agency approach include Wolverhampton City Council, Wolverhampton City PCT, Royal Wolverhampton Hospital Trust, Black Country Partnership Foundation Trust, West Midlands Police, Job Centre Plus, Probation Services, Schools, Wolverhampton Homes, & Wolverhampton Voluntary Sector Council.

The Royal Wolverhampton NHS Trust

# Purpose Specific Information Sharing Agreement

**Version Control:**

| | |
|---|---|
| **Version** | 2.0 |
| **Review Date** | _ _/_ _/202_ |

# Contents

# 1. Introduction

1.1. This Information Sharing Agreement is between:

**Organisation 1**

**The Royal Wolverhampton NHS Trust (RWT)**

And

**Organisation 2**

**Insert name of organisation**

1.2 This Agreement details the specific purpose(s), including legislative powers and duties, for sharing appropriate information, the operational procedures required (how & when this will happen), what data is to be shared, the consent processes involved and the process for review.

1.3 This Agreement is binding on both parties and each organisation will work towards meeting the commitments made. It is a working document and therefore the contents can be reviewed and altered to reflect and address new risks and changing circumstances. Such changes would be subject to ratification by both parties.

1.4 The contents of this document must be summarised and distributed to appropriate operational/delivery staff within the signatory organisations. The exact mechanism as to how this will be achieved will vary dependent on internal communication structures.

1.5 A signed copy of this Agreement, must be held by each party. Copies of the document can be made available upon request.

1.6 This Agreement can be terminated at any time by either party, providing sufficient notice no less than one calendar month.

# 2. Lawful Basis for Sharing

2.1 This Agreement is between the organisations listed in 1.1.

2.2 In order to share information between the parties there must be a defined and justifiable purpose(s) and hinged on the lawful basis stated in 2.3

2.3 The lawful basis that underpins this relationship and the duties and powers to facilitate the lawful sharing of appropriate information between the named organisations are summarised as follows:

| UK GDPR Article 6 | Processing of Personal Data (delete as appropriate) |
|---|---|
| 6a | **Consent:** The data subject has given consent to the processing of their personal data for this or other purposes |
| 6b | **Contract:** Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract |
| 6c | **Legal Obligation:** Processing is necessary for compliance with a legal obligation to which the controller is subject |
| 6e | **Public Task:** The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. |
| 6d | **Vital Interests:** Processing is necessary in order to protect the vital interests of the data subject or of another natural person |

| UK GDPR Article 9 | Processing of Special Category – Sensitive Data (delete as appropriate) |
|---|---|
| 9a | **Explicit Consent:** The data subject has given explicit consent to the processing of those personal data for one or more specified purposes |
| 9b | **Employment, Social Security and Social Protection:** Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the Data subject in the field of employment and social security and social protection law |
| 9c | **Vital Interests:** Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent |
| 9e | **Publicly Accessible:** processing relates to personal data which are manifestly made public by the data subject |
| 9f | **Legal Defence/Claims:** Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity |
| 9g | **Public Interest:** Processing is necessary for reasons of substantial public interest, on the basis of UK law which shall be proportionate to the aim pursued |
| 9h | **Health and Social Care:** Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of UK law or pursuant to contract with a health professional |

| | |
|---|---|
| 9i | **Public Health:** Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices |
| 9j | **Research:** Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes |

- The Data Protection Act (2018)
- Health and Social Care Act 2008
- National Health Service Act 2006
- Common Law Duty of Confidentiality

2.4 Any information shared and the processes used to share such information will be compliant with relevant legislation.

2.5 Both parties are responsible for ensuring their organisation complies with the National Data Guardian's 10 Data Security Standards:

1. All staff ensure that personal confidential data is handled, stored, and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful appropriate purposes.
2. All staff understand their responsibilities under the National Data Guardian's data security standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3. All staff complete appropriate data security training and pass a mandatory test, provided through the redesigned Information Governance Toolkit or equivalent training programme.
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All instances of access to personal confidential data on IT systems can be attributed to individual authorised users.
5. Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses, or which force staff to use workarounds that compromise data security.
6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data breach or near miss, with a report made to senior management within 12 hours of detection. Significant cyber-attacks are to be reported to CareCERT immediately following detection. It may also be appropriate to make reports to the National Cyber Security Centre (NCSC) and Information Commissioner's Office (ICO).

7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses and it is tested once a year as a minimum, with a report to senior management.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.
9. A strategy is in place for protecting IT systems from cyber threats, based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian's data security standards.

## 3. Service Overview and Purpose

| | |
|---|---|
| Name of Project, Initiative or Service | |
| Purpose of the Information Sharing | |
| Who is the information about? RWT staff, RWT patients, other? If "other" please provide details | |
| Will this be an information outflow or inflow to RWT, or both? | |
| What system will be used for Information Sharing | |

## 4. Information Sharing Process and Procedures

### 4.1 Information to be shared

4.1.1 Information shared between the parties will be that stated in section 6, which is necessary to achieve the purpose stated in section 3.

4.1.2 Under the General Data Protection Regulations (GDPR), the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

4.1.3 If additional information is required on a repeated basis over and above what is defined in this Agreement, to enable the Agreement to achieve its aims, the lead officers for each organisation should agree an addition to the sharing Agreement, ensuring that the new information meets the same legislative basis as the original. This addition should be made to the Agreement and all parties should sign up to it.

4.1.4 The Data Sharing Table **in Section 6** contains summary details of what information can be shared, relevant contact details, methods of requesting and transferring information and the frequency of transfer for each item.

## 4.2 Ensuring Data Quality

4.2.1 The parties are responsible for ensuring that processes and procedures are in place for maintaining information accuracy, and for ensuring that information shared is of sufficient quality.

## 4.3 Information Use, Review, Retention and Deletion

4.3.1 Parties to this Agreement undertake that information shared will only be used for the specific purpose for which it was shared. It must not be shared for any other

purpose outside of this Agreement or be disclosed to a third party without obtaining the express written permission of the party that provided the information.

4.3.2 In line with each organisation's own retention policy, the information should not be kept any longer than is necessary.

| | |
|---|---|
| **RWT** Retention Period | https://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf |
| **Insert name of organisation** Retention Period | |

4.3.3 The following destruction process will be used when the information is no longer required:

- Shredding (crosscut) for paper records
- Secure deletion from electronic devices; it is important that the data must be rendered unreadable when the device on which it resides is disposed of or recycled

Personal data which is ready for disposal should always be treated as confidential waste and must be kept secure.

### 4.4 Subject Access Requests

4.4.1 If a request is received from a data subject to access records this will be dealt with by the relevant organisation in accordance with their respective procedures.

4.4.2 If shared data is involved, then the originating organisation should be informed of any disclosure and may advise on its release. However, the final decision will remain with the organisation who received the request.

## 5. Roles and Responsibilities

### 5.1 Roles and Responsibilities under this Agreement

5.1.1 Parties to this Agreement are advised to appoint Specific Points of Contact (SPOC)

5.1.2 Access to information provided under this Agreement will be the responsibility of the SPOC for the parties.

5.1.3 It is the responsibility of everyone sharing information and accessing and using the information that has been shared to take appropriate decisions and hold the information securely to the party's standards. See addendum

5.1.4 The SPOC within each organisation will be the first port of call for questions about this Agreement. If there is a problem such as a potential data breach, relevant SPOC must be contacted, and in the case of a data breach incident, the relevant Data Protection Officer should also be contacted.

5.1.5 Only appropriate and authorised persons will have access to the information specified in this Agreement. If in doubt, a person intending to share or access information should contact their SPOC.

### 5.2 Governance, Monitoring and Review

5.2.1 The review, monitoring and amendment of the Agreement will be undertaken by the SPOC with advice from both parties Information Governance Department. Formal review will be undertaken as the review date stated in this document or subject to legislation or policy changes.

5.2.2 If a significant change takes place which means that the Agreement becomes an unreliable reference point, then the Agreement will be updated as needed and a new version circulated to replace the old.

5.2.3 If the lead SPOC departs their role, an alternative lead must be nominated as soon as possible.

### 5.3 Indemnity & Jurisdiction

5.3.1 As recipients of information covered under this Agreement, signatories will accept total liability for a breach of this Information Sharing Agreement by their organisation, should legal proceedings be served in relation to the breach.

5.3.2 This Agreement is legally binding and is governed by and shall be interpreted in accordance with the law of England and Wales.

### 5.4 Signatures

5.4.1 By signing this Agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself are sufficient to meet the purpose of this Agreement.

5.4.2 Signatories must ensure the parties comply with relevant legislation and with the provisions set out in this Agreement

## 6. Data Sets

| | |
|---|---|
| Data to be shared | ✓ Name – First and last names (patient and staff)<br>✓ Address including postcode (patient and staff)<br>✓ Email address (patient and staff)<br>✓ Home and/or mobile telephone number (patient and staff) |

| | |
|---|---|
| | ✓ Gender (patient and staff)<br>✓ Date of birth (patient and staff)<br>✓ Ethnicity (patient and staff)<br>✓ Language spoken (patient and staff)<br>✓ GP practice (patient and staff)<br>✓ NHS number (patient and staff)<br>✓ Health data (patient and staff)<br>✓ Safeguarding data (patient and staff)<br>✓ Next of kin (patient and staff)<br>✓ Next of kin (patient and staff) |

## 7 List of Designated SPOC

| Name of Organisation | SPOC & Position Held | Contact Details (Telephone Number & Email Address) |
|---|---|---|
| RWT | | |
| RWT | | |
| Insert name of organisation | | |
| Insert name of organisation | | |

## 8. Information Sharing Agreement Authorisation

In signing this Agreement, you are agreeing to the sharing conditions in the introduction of this Agreement.

Sharing is not authorised until this is signed on behalf of both parties, Agreements can only be signed by SIRO or Caldicott Guardian.

| **RWT Signatory** | |
|---|---|
| Registered Business Address | Corporate Services Centre, New Cross Hospital, Wolverhampton. WV10 0QP |
| ICO Registration Number | Z8441040 |
| Name | Jonathan Odum |
| Position | Chief Medical Officer / Caldicott Guardian |
| Signature | |

| | |
|---|---|
| Date | |
| | |
| **Insert name of organisation Signatory** | |
| Registered Business Address | |
| ICO Registration | |
| Name | |
| Role | |
| Signature | |
| Date | |

# Appendix 1: Conditions for Sharing

## Information Governance

1.1 All organisations shall have in place appropriate internal information governance and/or operational policies and procedures to facilitate the effective processing of personal information which is relevant to the needs of the organisation, their managers/practitioners, and their service users.

## Staff Requirements

1.2 The conditions, obligations and requirements set out in the Information Sharing Arrangement and this Addendum apply to all appropriate staff, agency workers, and volunteers working within those organisations.

1.3 All organisations are strongly advised to ensure that staff have entered appropriate confidentiality arrangements that detail the possible consequences of unauthorised or inappropriate disclosure of service user information. This may be incorporated into staff contracts if deemed necessary.

1.4 Each organisation must ensure that all appropriate staff have the necessary level of DBS clearance in accordance with relevant legislation and Government guidance.

## Service User Awareness & Rights

1.5 Each organisation has a duty to ensure that all service users are aware of the information that is being collected and recorded about them, the reasons for doing so (including any statistical/analytical purposes), with whom it may be shared and why. This can be achieved by the issuing of a Privacy Notice (Fair Processing Notice).

1.6 Each organisation has a duty to ensure that all service users are aware of their rights in respect of information processing/sharing, including any limits and/or restrictions, in respect of Data Protection legislation, the Human Rights Act 1998, the Common Law Duty of Confidentiality and, where appropriate, the Freedom of Information Act 2000 and how these may be exercised.

1.7 This will include providing appropriate support in order that service-users may best exercise those rights, e.g. providing service users with information in alternative formats or languages or assisting them with a Subject Access Request.

1.8 All service users have a right to expect that information disclosed by them or by other parties about them, to an organisation will be treated with the appropriate degree of respect and confidence. This is covered by a Common Law Duty of Confidentiality. However, this right is not absolute and may be overridden in certain circumstances.

1.9 In addition, all service users must be made aware under what circumstances their consent will be required, and the procedure by which it will be sought, to obtain and share their personal information

## Data Access, Security, Transfers & Hosting

1.10 Each organisation must ensure that appropriate technical and organisational measures are in place that protect against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information. Thus:

- Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information to be stored and/or shared, including information transferred to/received from other organisations.

- Each organisation must ensure that mechanisms are in place to address the issues of; physical security, security awareness and training, security management, systems development, role based security/practitioner access levels, data transfer and receiving and system specific security policies.

- Wherever 'Common Protective Markings' are used (OFFICIAL-SENSITIVE etc.) then each party organisation should agree and evidence the common meaning of these terms and the associated procedures to ensure that that the transmission/receipt and storage of information thus marked is appropriate to the level of security required.

- The organisations will not transfer, or host information shared under this agreement, outside the UK, European Union and Territories that have received adequacy decisions from the UK and European Union Authorities.

- The organisations will cooperate where necessary to manage data breach incidents and near misses associated with sharing data under this Agreement.

## Freedom of Information

1.11 RWT is a Public Authority and for the purposes of the Freedom of Information (FOI) Act 2000 and the Environmental Information Regulations (EIR)2004.

1.12 Basic information regarding the relationship between the organisations may be disclosed under RWT's publication scheme.

1.13 In addition, RWT may be required to disclose further information about the relationship between the organisations, in response to a FOI request. If this situation arises, RWT will consult with the parties to this agreement prior to disclosure.

## Staff Awareness & Training

1.14 Each organisation has a responsibility to ensure that all relevant staff receive training, advice, and on-going support to be made aware, and understand the implications, of:

- This Information Sharing Agreement (ISA) and any other associated documents (e.g., confidentiality Agreement, the ISA, the 'Operational Arrangement', etc.). This is to include any associated operational requirements arising from the implementation of these.

- The underpinning and organisation specific legislation and associated regulations/guidance in respect of Information Sharing and any express or implied powers arising there from.

- Common Law duties (e.g., Confidentiality).

- Appropriate Codes of Practice and other associated regulations/guidance, where relevant or required (e.g., NHS Confidentiality Code of Practice).

# Appendix 2: Definition of Terms

| Word/Phrase | Definition |
|---|---|
| Agreement | This data sharing protocol/document outlining acceptable practices between the signatory data controllers, for the purpose stated herein |
| Controller | As defined in Article 4 of the UK GDPR. |
| CareCERT | NHS Digital's Care Computing Emergency Response Team.<br>Cyber Security support mechanism for Health and Care |
| Data | as defined within the GDPR and the DPA, including both Personal and Sensitive Data, and also any Data which is not defined by the DPA and which comprises any written information which is provided to or acquired by the Parties which is either (a) commercially sensitive, or (b) confidential, or (c) Special Categories of Personal Data and (d)'information asset' |
| Legislation | The statutes, regulations, codes, and guidance to include (but not limited to) the following:<br><br>i) The UK General Data Protection Regulation (UK GDPR)<br><br>ii) The Data Protection Act 2018 and any subsequent Data Protection legislation (the 'DPA')<br><br>iii) The NHS Act 2006<br><br>iv) The Health and Care Act 2022<br><br>v) Common Law Duty of Confidentiality<br><br>vi) All applicable laws, and regulations relating to the Processing of Data, privacy, health and social care, including (where applicable and without limitation) the guidance and codes of practice issued by the Information Commissioner under the GDPR, DPA and under any subsequent Data Protection legislation.<br><br>This will also include any statutes, regulations, codes, and guidance which may come into force at a future date. |
| Data Subject | The identifiable natural person to whom the Personal Data belongs |
| Fair Processing Notice | Information provided to the individual either when collecting the information, or at the point of receipt of the information from a third party. This notice must comply with the requirements of Articles 12, 13 and 14 of the GDPR and any relevant Data Protection Legislation. |

| | |
|---|---|
| System | Application, data repository and any means of processing data which is accessible according to specific criteria, whether centralised, de-centralised or dispersed on a functional or geographic basis |
| ICO | Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.<br><br>The UK independent authority for regulating and monitoring activity under all relevant Data protection and information rights legislation. |
| Party/Parties | **The Royal Wolverhampton NHS Trust**, Corporate Services Centre, New Cross Hospital, Wolverhampton. WV10 0QP<br><br>and<br><br>**insert name of organisation** |
| Personal Data/ Personal Information | As defined in Article 4 (1) of the UK GDPR |
| Staff | Employees of the controllers, or its processors and suppliers, contractors, sub-contractors, officers, agents, students on work experience and volunteers who are from time to time employed and/or engaged in connection with processing data on behalf of the data controller or otherwise in relation to the performance of a contract. |
| Processing / Processed / Process | The definition for Processing/Processed/Process within this Protocol shall have the same meaning as Processing within Article (4) (2) of the UK GDPR |
| Processor | As defined in Article 4 of the GDPR |
| Retention | How long data will be held on record |

The Royal Wolverhampton NHS Trust

# Data Processing Agreement

**Between**

**The Royal Wolverhampton NHS Trust**

**(Hereinafter known as the Data Controller)**
**ICO Registration No: Z8441040**

**AND**

***Insert Name of Legal Entity***
**(Hereinafter known as the Data Processor)**
**ICO Registration No: .....**

**In Support of *Insert name of Project or Service Provided***

| | |
|---|---|
| **Version** | 3.0 |
| **Review Date** | _ _/__/202_ |
| **Purpose of Data Processing** | |

## 1.0 Introduction

1.1 This Agreement provides an operating framework to enable lawful disclosure of information under the control of RWT, to the Data Processor working on behalf of the Data Controller taking account of the Data Protection Act 2018/ UK General Data Protection Regulation, and NHS guidance on confidentiality of personal information, the common law duty of confidence and other applicable legislation.

1.2 The terms and conditions of this Agreement shall apply to all NHS Information provided by and on behalf of the Data Controller or obtained by the Data Processor from other sources as part of the delivery of the contracted services or derived from any combination thereof.

1.3 This Agreement between the Data Controller and the Data Processor supports and is specific to *insert name of project or service provided*

## 2.0 Definitions

2.1 **Personal data –** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, or by reference through an identifier.

2.2 **Special categories of personal data (also known as as sensitive personal data) –** The categories of personal information defined in the Data Protection Act 2018/ UK General Data Protection Regulation Article 9(1) and, in this Agreement, information about racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, physical and mental health condition of an individual, sexual life of an individual, the commission or alleged commission of an offence and genetic/biometric data.

2.3 **Confidential (includes business and commercially sensitive) Information –** Information that contains details about an organisation or an individual person, provided with an expectation that confidentiality will be maintained. This includes for example, corporate or technical information that is commercially sensitive, drafts of documents that are not ready for publication, restricted information & documents, etc.

2.4 **NHS Information –** Any information as defined in 2.1 to 2.3 that the Data Controller is responsible for. This includes all information supplied to the Data Processor by and on behalf of the Data Controller and any additional information that the Data Processor obtains during the term of the contract and shall apply equally to original NHS Information including electronic back-ups and hard copies.

2.5 **Data Controller –** As defined in the Data Protection Act 2018/ UK General Data Protection Regulation means the natural or legal person who alone or jointly

with others determines the purpose and means of the processing of personal data.

2.6 **Data Processor –** As defined in the Data Protection Act 2018/ UK General Data Protection Regulation, is an individual (other than an employee of the data controller) or organisation who processes personal information whilst undertaking a business activity or service on behalf of the Data Controller, under contract.

2.7 **Data Processing –** Also defined in the Data Protection Act 2018/ UK General Data Protection Regulation in respect of personal data. For the purpose of this document this includes an operation or set of operations which is performed on personal data, or on sets of personal data, such as:

- collection, recording, organisation, structuring or storage
- adaptation or alteration
- retrieval, consultation, or use
- disclosure by transmission, dissemination or otherwise making available
- alignment or combination; or
- restriction, erasure, or destruction.

**3.0 General**

3.1 The Data Processor shall put in place appropriate technical and organisational measures to ensure the protection of the information subject to this Agreement against the accidental loss or destruction of or damage to NHS Information, having regard to the specific requirements set out in this Agreement, the state of technical development and the level of harm that may be suffered by the Data Controller and/or by a Data Subject whose Personal data is affected, in the event of unauthorised or unlawful processing, or by its loss, damage or destruction.

3.2 All NHS Information referred to in 2.4 and 4.2 will remain under the control of the Data Controller and shall be either returned, reserved at a location determined by the Data Controller, or destroyed by the Data Processor at the instance of the Data Controller, upon completion of the contracted service.

3.3 Under the terms of this Agreement the Data Controller shall provide the Data Processor with the minimum amount of NHS Information necessary to deliver the contracted service and in particular, personal and sensitive information will be accessed on a ‘need to know’ basis only.

3.4 The Data Processor shall only process NHS information as is necessary to perform its obligations under this Agreement and only in accordance with instructions given by the Data Controller under this Agreement and, shall not use or process NHS Information for any purpose other than as directed by the Data Controller for delivery of the contracted service.

3.5 The Data Processor shall not subcontract any of its processing operations performed on behalf of the Data Controller under this Agreement without the prior written authorisation of the Data Controller. Where the Data Processor subcontracts its obligations, with the written authorisation of the Data Controller, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the Data Processor under this Agreement. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data processor shall remain fully liable to the data controller for the performance of the sub-processor's obligations under such agreement.

3.6 Any minor changes to this Agreement that may become necessary from time to time shall be made by the Data Controller to the Data Processor or requested by the Data Processor from the Data Controller, as a written variation.

3.7 In the event of major changes being required, the Data Controller shall terminate this Agreement and replace with an updated version. Such termination and replacement may also be initiated by the Data Processor, subject to prior arrangement with the Data Controller.

3.8 Acquisition, merger, amalgamation, or other form of subsumption of the Data Processor during the contracted service delivery period, will not invalidate the terms of this Agreement.

## 4.0 Description of NHS Information

4.1 The NHS information covered in this Agreement is as detailed in section 4.2 and where relevant is indicated as personal, sensitive, or confidential as defined in sections 2.1, 2.2 and 2.3 respectively. The Data Processor shall not disclose information to any third party without the prior written authorisation of the Data Controller. Disclosure of such data as may contain patient information will require evidence of Caldicott Guardian approval before disclosure for the purpose of delivery of the contracted service. Other data which may be considered 'confidential' or contains information, which is sensitive or otherwise personal information, will require evidence of SIRO and\or Caldicott Guardian approval (as appropriate) before disclosure for the purpose of delivery of the contracted service. In such cases where the signatory to this Agreement, acting on behalf of the Data Controller, is not the Caldicott Guardian or SIRO (as appropriate), copies of such approval should be furnished to the aforementioned signatory before he\she signs this document.

4.2 The NHS information covered in this Agreement is as detailed below:

- *Patient/Employee (delete as appropriate) – Name, Date of Birth and Gender*
- *Patient/Employee (delete as appropriate) – Contact details (telephone/mobile number, email) and Address*
- *Patient/Employee (delete as appropriate) – Hospital number/NHS number*

- *Patient – Medical results/reports/correspondence*
- *Employee – Work history, professional accreditation/training, HR records, Occupational Health, and financial information*
- *Confidential information – Corporate/technical data, commercially sensitive data, document drafts/restricted documents*

## 5.0 Data Protection

5.1 The Data Processor shall comply with all aspects of the Data Protection Act 2018/UK General Data Protection Regulation, Human Rights Act 1998, and common law duty of confidentiality in relation to the processing of personal data and special categories of personal data.

5.2 The Data Processor shall only process data in accordance with the instruction of the Data Controller as specified under this Agreement.

5.3 The Data Processor shall put in place appropriate technical and organisational measures against any unlawful and unauthorised processing of NHS Information and against accidental loss, destruction of and damage to NHS Information.

5.4 The Data Processor shall not cause or allow NHS Information to be transferred to any territory outside the UK, European Economic Area and territories granted adequacy decision by the European Union or UK. This clause remains binding on the Data Processor and any Sub processors acting on instruction from the Data Processor, in the event the Data Processor becomes subsumed by acquisition or merger with another legal entity not currently a Party to this Agreement.

## 6.0 Policies and Procedures

6.1 The Data Processor shall have confidentiality, information security, data protection, records management policies or equivalent. These will describe individual responsibilities for handling the categories of information documented in clauses 2.1-2.3 of this Agreement.

6.2 The Data Processor shall provide the Data Controller with copies of the policies referred to in 6.1 above on request or as part of the process for approval of this Agreement.

## 7.0 Data Processor's Employees

7.1 The Data Processor shall undertake all reasonable background checks to ensure the reliability of all employees who are likely to have access to NHS Information.

7.2 The Data Processor shall include appropriate confidentiality clauses in employment contracts, including details of sanctions against any employee acting in a deliberate or reckless manner that breaches confidentiality or the non-disclosure provisions of this Agreement, or causes damage to, or loss of NHS information.

7.3 The Data Processor shall ensure that all employees are aware of and act in accordance with the policies referred to in 6.1 above.

*7.4* The Data Processor shall ensure that all employees are adequately trained to understand and comply with their responsibilities under this Agreement, and the common law duty of confidence, and shall provide the Data Controller with evidence of that training on request or as part of the process for approval of this Agreement.

7.5 Subject to clauses 7.1 – 7.4, the Data Processor shall ensure that only those employees involved in delivery of the contracted service, have access to NHS information on a strict 'need to know' basis and shall implement appropriate access controls to ensure this requirement is satisfied.

7.6 The Data Processor shall ensure that any employees involved in delivery of the contracted service, who do not specifically need to use NHS Information as part of their role, have restricted access to NHS Information or redacted extracts only.

**8.0 Security – General**

8.1 The Data Controller will not contract services from Data Processors unable or unwilling to comply with the terms of this Agreement and reserves the right to terminate the contract if either Party is unable to agree necessary amendments in the future.

8.2 The Data Processor shall not under any circumstances share, disclose or otherwise reveal NHS Information (in whole or in part) to any individual, business, or other organisation (3rd party) not directly involved in delivery of the contracted service, without the prior written authorisation of the Data Controller.

8.3 The Data Processor shall notify the Data Controller immediately, of any data security incidents or activities that suggest non-compliance or a breach of any sections or the entirety of the terms in this Agreement. These include incidents categorised as near misses, where there is no loss or unauthorised disclosure of NHS Information.

8.4 The Data Processor shall indemnify the Data Controller and compensate for any loss (financial or otherwise) that the Data Controller sustains due to any failure by the Data Processor their employees or sub-contractors, to act in accordance with the terms of this Agreement and relevant legislation.

## 9.0 Security – Physical

9.1 The Data Processor shall ensure that all NHS information is physically protected from accidental or deliberate loss or destruction arising from environmental hazards such as fire or flood.

9.2 The Data Processor shall ensure that all NHS information is held on premises that are adequately protected from unauthorised access. Adequate deterrent measures should be deployed to forestall theft or sabotage, using for example burglar alarms, security doors, ram-proof pillars, controlled access systems, etc.

## 10.0 Security – IT Systems

10.1 The Data Processor shall hold electronically based NHS information on secure servers unless otherwise authorised in writing by the Data Controller.

10.2 NHS information will, under no circumstances, be stored on portable media or devices such as laptops or USB memory sticks, unless agreed in writing and subject, as a minimum, to those constraints detailed in section 10.2 and sub-sections.

10.3 The Data Processor shall ensure that:

10.4 All portable media used for storage or transit of NHS information are fully encrypted in accordance with NHS Guidelines on encryption to protect personal information.

10.5 Portable media are not left unattended at any time (e.g., in parked cars, in unlocked and unoccupied locations, etc.).

10.6 When not in use, all portable media are stored in a locked area and issued only when required to authorised employees, with a record kept of issue and return.

10.7 The Data Processor shall not allow employees to hold NHS information on their own personal computers or other personal peripherals.

10.8 The Data Processor shall ensure adequate back-up facilities to minimise the risk of loss of or damage to NHS information and that a robust business continuity plan is in place in the event of restriction of service for any reason.

10.9 The Data Processor shall not transmit NHS information by email except as an attachment encrypted to 256-bit AES or TLS 1.2 and above standards or within NHS mail.

10.10 The Data Processor shall only make printed paper copies of NHS information

if this is essential for delivery of the contracted service.

10.11 The Data Processor shall store printed paper copies of NHS information in locked cabinets when not in use and shall not remove from premises unless this is essential for delivery of the contracted service.

10.12 The Data Processor shall provide the Data Controller with a signed Information Governance Statement of Compliance (IGSoC) (as confirmation of achieving level 2 (satisfactory) in respect of the NHS Information Governance Toolkit) OR evidence of compliance with another credible Information Security Management System (ISMS), before the Data Controller can allow access to networked IT systems (e.g. N3, Summary Care Record, etc).

## 11.0 Secure Destruction

11.1 The Data Processor shall ensure that NHS information held in paper form, regardless of whether as originally provided by the Data Controller or printed from the Data Processor's IT systems, is destroyed using a crosscut shredder or subcontracted to a confidential waste company that complies with European Standard EN15713.

11.2 The Data Processor shall ensure that electronic storage media used to hold or process NHS information is destroyed or overwritten to current CESG standards as defined at www.cesg.gov.uk

11.3 In the event of any bad or unusable sectors that cannot be overwritten, the Data Processor shall ensure complete and irretrievable destruction of the media itself.

11.4 The Data Processor shall provide the Data Controller with copies of all relevant overwriting verification reports and/or certificates of secure destruction of NHS information at the conclusion of the contract.

## 12.0 Monitoring & Audit

12.1 The Data Processor shall permit the Data Controller to monitor compliance with the terms of this Agreement, by:

12.1.1 Allowing Data Controller employees or nominated representatives to enter any premises where NHS information is held, at all reasonable times and with or without prior notice, for the purpose of inspection.

12.1.2 Completing and returning a Data Processing Monitoring Form at the request of the Data Controller.

12.1.3 Provide independent assurance of the self-audited Information Governance Toolkit performance measures where the Data Processor is required to comply.

## 13.0 Freedom of Information

13.1 The Data Processor acknowledges that the Data Controller is a public authority for the purpose of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).

13.2 Basic details of the contract shall be included in the appropriate log under the 'Data Controllers Publication Scheme'.

13.3 In addition, the Data Controller may be statutorily required to disclose further information about the contracted service or the contract itself in response to a specific request under FOIA or EIR, in which case:

13.3.1 The Data Processor shall provide the Data Controller with all reasonable assistance and co-operation to enable the Data Controller to comply with its obligations under FOIA or EIR.

13.3.2 The Data Controller shall consult the Data Processor regarding commercial or other confidentiality issues in relation to this contract, however the final decision about disclosure of information or application of exemptions shall rest solely with the Data Controller.

## 14.0 Legal Jurisdiction

14.1 This Agreement is legally binding and is governed by and shall be interpreted in accordance with the law of England and Wales.

14.2 In the event of a dispute, the parties to this Agreement agree to attempt to resolve such issues according to NHS dispute resolution procedures. If agreement cannot be reached, the parties agree that the courts of England and Wales shall have exclusive jurisdiction to hear the case.

14.3 The Data Processor's lawful basis for processing shall be as stated in the UK GDPR Article 6(1)e and Article 9(2) h.

## Data Processing Agreement between the Data Controller and the Data Processor

On behalf of the Data Controller

Signed…… Date……

Name: …… Position: ……

(Print name & position of authorised signatory)

On behalf of the Data Processor

Signed…… Date……

Name…… Position……

(Print name & position of authorised signatory)

This form must be returned to [*insert name of Data Controller's representative here]* prior to release of any data identified in Section 4.2

**Appendix 6**

| Level of agreement | What does the agreement cover? | When should it be used and by who? |
|---|---|---|
| Tier 1 – Wolverhampton Overarching Information Sharing Protocol. | This document is a high-level policy document common to all organisations delivering health, social and community services, across an area.<br><br>The Trust has already signed up to a Wolverhampton City wide agreement which can be viewed here<br><br>It describes a common set of principles and defines the general parameters within which the signatory organisations will share information with each other.<br><br>This document establishes ownership and transparent agreement to the spirit of information sharing in the best interests of service users and their families and carers, and it commits those who sign it to sharing information lawfully, ethically and effectively at all levels of their organisation.<br><br>This Tier One document provides the context for the underlying tiers in the model. | This is a high-level strategic agreement that will be reviewed and signed by the Chief Executive or other member of the board of directors.<br><br>Other members of staff would not be asked to fill in an agreement at this level in their day-to-day duties. |
| Tier 2 – Information Community Agreements | These documents are high-level agreements common to organisations delivering health, social and community services.<br><br>They satisfy the Tier 2 level of the 3-Tier Model for Information Sharing and focuses on the collective purposes underlying the sharing of information within the 'Information Community'.<br><br>Tier Two documents describe common contexts and shared objectives between agencies delivering services of a similar scope for example safeguarding adults or children, school nursing. To carry out these activities a number of organisations will be involved and will need to input/view a patient or service user's record. | Information Community Agreements are to be signed by Service Directors or the equivalent functional leads who have responsibility for the area of sharing, for example safeguarding.<br><br>If circumstances arise where a tier 2 agreement is needed please contact the Information Governance Lead. |

| | | |
|---|---|---|
| | Tier 2 documents reference the relevant underpinning legislation and the associated duties and powers that enable legally justifiable exchanges of information within the same Information Community.<br><br>They also provide context for a supporting set of individual information sharing agreements (Tier 3) that determine at a detailed level, how personal information can be shared amongst organisations with the same information community. | |
| Tier 3 – Purpose Specific Information Sharing Agreements (PSISA) | Where information is shared with another organisation for them to use to carry out a business function of their own, they store and use the data we are sharing then a PSISA need to be used.<br><br>These documents are the lowest level or third element of the Three-Tier model. This is the template that all staff should use to detail;<br>• What information is to be shared<br>• Why it is being shared (for what specific purposes)<br>• Who it is being shared with (between which agencies)<br>• When it is being shared (the times, the frequency etc)<br>• How it is being shared (format)<br><br>These documents are aimed at an organisation's "operational management/practitioner" level and will define the relevant processes which support the information sharing between two or more agencies for a specified purpose. | Purpose Specific Information Sharing Agreements (PSISA) should be used by any member of staff involved in the process of information sharing with another organisation. Attachment 4<br><br>Once filled in review by the Information Governance Steering Group or IG Lead is needed before being signed by IG lead / Caldicott Guardian.<br><br>Heads of relevant services who have the devolved local and/or operational responsibility for delivery. |
| Tier 3 – Purpose Specific Data Processing Agreements (PSDPA) | Where information is accessed by organisation for them to process the data on our behalf to carry out one of the Trust business function, they are not storing the data then a PSDPA is needed.<br><br>For example if a company accesses | Purpose Specific Data Processing Agreements (PSDPA) should be used by any member of staff involved in the process of allowing access to the Trusts |

| | | |
|---|---|---|
| | personal data on the Trusts systems for maintenance of systems, testing, scanning etc. | information. Attachment 5 |

## Information Sharing Policy – Flowchart which sharing template to use