Data Sharing Policy

Author	Version	Date	Amendments
Caroline Pegg	**1**	31/01/2018	N/A
Aimee Chambers	**2**	30/01/2019	Added Appendix 3B - flowchart of when to share information Appendix 3 - added seven gold rules of data sharing
Caroline Pegg	**3**	25/03/2021	Updated to reflect ICO new code of practice on information sharing: Addition of sections: 2 Transparency, 6 Children, 7 Data Privacy Impact Assessments and 8 Law Enforcement Purposes Appendix 1-minor changes Appendix 2-Additional minimum requirements for an Information Sharing Agreement. Appendix 4-revised decision record

Responsible Officer: Director of Law and Assurance

CONTENT

1. POLICY STATEMENT

1.1 Under the right circumstances and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more coordinated, and efficient service to customers.

1.2 We recognise that effective partnership working requires information to be shared and that equally there is a need to ensure information sharing takes place within a clear framework to protect the rights of the data subject.

1.3 This document sets out West Sussex County Council's Information Sharing Policy and ensures we share personal data lawfully, fairly, transparently, securely, effectively, and efficiently within the Council and with partner organisations. It includes several checklists, guidance, and templates in the Appendices.

1.4 This Policy applies to all staff and elected members and the Council expects its staff and elected members to comply fully with this Policy. Disciplinary action may be taken against any employee who breaches any of the instructions or requirements forming part of this policy. Elected Members should adhere to this policy to ensure compliance with the Member Code of Conduct and the Council's obligations in relation to confidentiality.

1.5 This policy is associated with the Data Protection Policy and the Data Privacy Impact Assessment Policy

2. TRANSPARENCY

2.1 To be fair and transparent privacy notices are published on WSCC internet. Such notices explain how personal data is being processed by the County Council and contain information about who we share personal data with and why.

3. DATA SHARING

3.1 Data sharing can take the form of a unilateral or reciprocal exchange, several organisations pooling data and making it available to all and/or to other parties, and different parties of the same organisation making data available to each other.

3.2 There are two main types of data sharing:

- systematic, routine data sharing where the same data sets or types of data are shared between organisations for an established purpose; and

- specific, in particular or defined circumstances we share data for any one of a range of purposes.

4. SYSTEMATIC ROUTINE DATA SHARING

4.1 Routine sharing with partners and organisations shall be undertaken in accordance with written Information Sharing Agreements (ISA's) made between the organisations. Prior to entering into such agreement, the organisations involved will each complete the

check list in Appendix 1. Such agreements will contain provisions ensuring that personal data will continue to be protected with adequate security by any organisation that will have access to it.

4.2 Each ISA will, as a minimum, document the matters set out in Appendix 2.

4.3 A summary of key ISAs will be published on the WSCC internet. A copy of every ISA shall be provided to and retained by the Council's data protection team.

4.4 An officer must ensure that he or she has specific authority to sign an ISA with the organisation(s) identified in the ISA.

4.5 The officer signing the ISA for their area of service is responsible for ensuring copies of signed and agreed ISAs are sent to the Council's Data Protection Team who shall retain a log of all ISAs. The Data Protection Team shall be notified of any changes made to or terminations of any ISA.

5. SPECIFIC DATA SHARING

5.1 The County Council will share personal data in an emergency when it is necessary and proportionate to do so. Not every urgent situation is an emergency. An emergency includes:

- preventing serious physical harm to a person;
- preventing loss of human life;
- protection of public health;
- safeguarding vulnerable adults or children;
- responding to an emergency; or
- an immediate need to protect national security.

5.2 The County Council will share personal data without an individual's knowledge or consent in limited circumstances such as where, for example, personal data is processed for:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of tax or duty.

When sharing with police and enforcement agencies we will require a written request detailing the reason why the disclosure is necessary to achieve the purpose in accordance with the limited grounds as set out above.

5.3 We may share personal data without an individual's knowledge or consent at the request of other organisations or proactively where it is required by Law, where it is necessary in an emergency situation to identify and assist vulnerable people or where it is necessary in the interests of safeguarding vulnerable children or adults.

5.4 In relation to a procurement exercise and in relation to any other Council business relating to an individual but where it is not necessary to share or use personal data in full that personal data will be anonymised. Where it is necessary to share personal data as part of a procurement exercise or similar Council business, we will ensure this is done with the protection of a confidentiality agreement or non-disclosure agreement either within the contractual document or as a separate agreement. Any officer dealing with the procurement work shall obtain advice from the Responsible Officer and from Procurement Services in accordance with the Council's Standing Orders on Contracts and Procurement.

5.5 Decisions will be proactively taken in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared.

5.6 Decisions will made by appropriate officers having regard to the Information Commissioner's Office checklist, the Caldicott Principles when sharing for the purposes of direct care and the Seven Golden Rules of Data Sharing detailed at Appendix 3.

5.7 A flowchart on 'when to share information' should be followed – appendix 3B will assist the appropriate officer in reaching the decision to share in individual cases.

5.8 All the circumstances of the individual case will be considered when exercising professional judgment in balancing what is required to achieve a legitimate purpose with any interference with the individual's right to respect for private and family life. Any decision to disclose should be justified and proportionate. Applicable professional guidance or ethical rules will be considered. Addressing the questions in the template decision record at Appendix 4 will inform the decision.

5.9 If a decision is made to share personal data, we will share the minimum amount of data required to achieve the aim of the sharing.

5.10 A record will be made of each individual decision to share personal data. The record will include the elements in the template at Appendix 4. This record shall be made and retained by the officer making the disclosure in accordance with arrangements agreed with the Director with responsibility for their service. Such records shall be available for inspection by the Council's Data Protection Officer.

5.11 It may not always be possible to document the sharing in an emergency or time dependent situation however a record will be made as soon as possible.

6. CHILDREN

6.1 Children's vulnerability means that the risks in sharing their data may be higher than in the similar processing of adults' data. We will only share children's data if there is a compelling reason to do so, taking account of the best interests of the child. Compelling reasons will include data sharing for safeguarding purposes and the importance for official national statistics of good quality information about children.

6.2 We will carry out a DPIA in high risk cases to assess and mitigate risks to the rights and freedoms of children, which arise from systematic data sharing. A case is considered to be high risk either because of the particular circumstances of the child in terms of their exposure to risk of significant harm or where the data requested is of particular sensitivity.

6.3 We will carry out due diligence checks on those we intend to share children's data with. If we reasonably foresee that the data will be used in a way that is detrimental to the child, or otherwise unfair, we will not share.

7. DATA PRIVACY IMPACT ASSESSMENT (DPIA)

7.1 When planning systematic data sharing, we will consider carrying out a DPIA. Where the data sharing is being undertaken in circumstances where an individual is at high risk of significant harm s we will carry out a DPIA.

8. LAW ENFORCEMENT PURPOSES

8.1 When data sharing for law enforcement purposes, such as: to prevent, investigate, detect or prosecute criminal offences or execute criminal penalties in relation to trading standards, fire safety risks, matters affecting the highway, planning contraventions, non-school attendance and waste disposal we will comply with Part 3 DPA 2018. We will only share data with consent or where necessary for the performance of the task. Where the data shared is special category data we have a policy in place and will not share data unless we have the individual's consent or the processing is strictly necessary for the law enforcement purpose and a condition in schedule 8 DPA 2018 is met.

9. GIVING EFFECT TO THE POLICY –RESPONSIBILITIES OF OFFICERS

9.1 The Chief Executive, acting through the Council's Data Protection Officer, shall be accountable for the implementation and effectiveness of this policy.

9.2 Where an Elected Member has access to and processes personal information on behalf of the Council the Member does so under the Council's registration and must comply with this policy.

9.3 All Executive Directors and Directors are responsible for implementing safe and sound data sharing procedures within their services and the operation of those services and ensuring the proper security of information held. Directors should have regard to this Policy when formulating any policies or procedures which determine the circumstances in which personal data will be shared.

9.4 The Data Protection Officer has specific operational responsibility for data sharing matters corporately.

10. ENSURING COMPLIANCE

The Council will ensure that:

10.1 Each Directorate documents what personal data is held by the services of that Directorate, where it came from, who it is shared with and that the specification of data management systems operated by the Directorate enables compliance with the Act.

10.2 Legal advice, training and guidance are available to all staff and elected members. Core guidance, practice, procedures and policies shall be held on the County Council's intranet.

10.3 The development and promulgation of best practice in relation to data sharing will be the responsibility of the Data Protection Officer, supported by the Information Governance Group which will include representatives from all Directorates.

10.4 The Council will have in place a compliance programme to monitor data sharing. The status of compliance activities should be monitored by the Council's Information Governance Group or a delegated DPA sub-group.

This is version 3.0

This policy was approved by Tony Kershaw Director of Law and Assurance on 25th March 2021 acting as the Council's Data Protection Officer.

It will be reviewed by the DPO no later than 30th January 2023.

11. APPENDIX 1

Checklist to be completed by all parties to the Data Sharing Agreement

	REQUIREMENTS LIST/RESPONSIBILITIES	Please tick indicating compliance or the steps you are taking to comply
1.	We have an information security policy	
2.	We have a Data Protection Policy.	
3.	Registration with the Information Commissioners Office is up to date.	
4.	We have a Data Protection Officer	
5.	The Data Protection Officer is widely known within the organisation and across signatory organisations.	
6.	Information Security Training is available to all staff including (permanent, temporary, voluntary, contract, students on placements etc.)	
7.	The organisation is aware that it will remain legally responsible for the information held within the organisation as required by data protection legislation.	
8.	That the organisation we send information to is aware of the purpose for which the information was collected, to ensure that processing does not contravene the Data Protection Act 2018. (If an organisation needs to disclose the information it has received to yet another organisation it must always seek consent from the originating organisation before doing so).	

9.	We will respond to requests for information within a reasonable time scale (as agreed in local /specific agreements and included in legislation e.g. Data Protection Act 2018).	
10.	All staff are issued with or made aware of a Code of Conduct or similar guidance relating to their responsibilities for data and confidentiality,	
11.	The organisation has confidentiality agreements for all staff (including permanent, temporary, voluntary, contract, students on placements, locums, bank staff etc.)	
12.	The organisation has confidentiality agreements with all contractors relating to service user information.	
13.	Service User Records are stored in an appropriate and secure manner.	
14.	Access to information is adequately controlled (for e.g. passwords and network access controls).	
15.	All new information system should be designed to include clear audit trails for all access/ uses of information.	
16.	All information is backed up	
17.	All backups are held securely in fireproof safes, if appropriate.	
18.	All remote accesses to networks are provided by a secure virtual private network or similar.	
20.	We have safe environments for sending and receiving personal information and have procedures for their use.	

21.	Records should be kept in accordance with local and national policies and guidelines	
22.	Person identifiable information will not be sent using insecure email services.	
23.	Staff will not keep person identifiable information on home PCs.	
24.	All portable equipment containing person identifiable service user information is protected against unauthorised access, theft or loss.	
25.	A secure disposal system is available for all person identifiable information no longer required and that all staff have policies and/or procedures to follow (disposal includes paper and electronic information and information on other media such as, hard drives, cds, videos.).	
26.	Adequate security measures are taken to protect all personal information	
27.	All staff using or accessing the data will know about and follow this protocol.	

12. APPENDIX 2

Data Sharing Agreement Required Content

A data sharing agreement shall, as a minimum, document the

following issues:

1. Identity of the data controllers at each stage
2. Where there are joint controllers the responsibilities of each
3. Identity of all parties involved in the sharing including contact data
4. the lawful basis (purpose, or purposes), of the sharing

5. If the lawful basis is consent-provide a model consent form
6. the potential recipients or types of recipient and the

   circumstances in which they will have access
7. the types of data to be shared (data specification)
8. expectations for data quality – accuracy, relevance, usability, formatting.
9. requirements for data security;
10. requirements for staff training and awareness
11. expectations for the retention of shared data;
12. provisions for the protection of individuals' rights including procedures for dealing with access requests, queries and complaints;
13. Confirmation that a DPIA has been considered. Where the data sharing is likely to result in a high risk to individuals the completed DPIA
14. review of effectiveness/termination of the sharing agreement; and sanctions for failure to comply with the agreement or breaches.

13. APPENDIX 3

Caldicott Principles – sharing for the purposes of direct care, extended to social care in 2000.

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

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

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

The Seven Golden Rules of Data Sharing

1. **Remember that the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing** but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. **Be open and honest** with the individual (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** from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

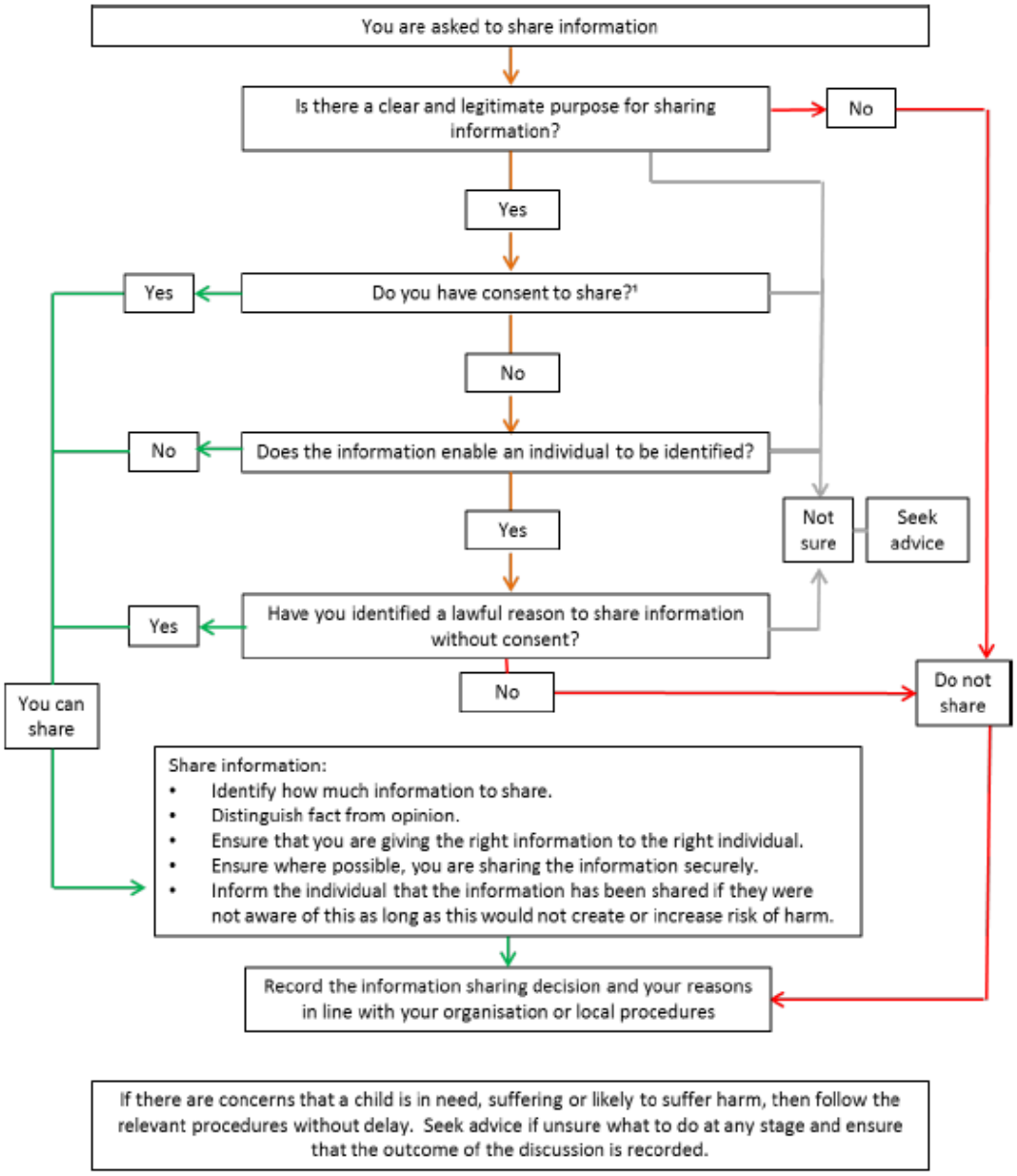
4. **Where possible, share information with consent**, and where possible, respect the wishes of those who do not consent to having their information shared. Under the UK GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

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

6. **Necessary, proportionate, relevant, adequate, 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 individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).

7. **Keep a record of your decision** and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose. – Appendix 4.

14. APPENDIX 3B – FLOWCHART OF WHEN TO SHARE INFORMATION



HM Government:

- Information Sharing – Advice for practitioners providing safeguarding services to children, young people, parents and carers' (July 2018)

15. APPENDIX 4 SPECIFIC DATA SHARING FORM

West Sussex County Council	
Name of organisation and name and position of requestor	
Date of request	
Description of data	
Purpose of the sharing	
State the lawful basis for sharing (personal data a condition in GDPR Art 6, special category data an additional condition in Art 9, criminal offence data Part 3 DPA 2018)	
If the lawful basis for sharing was the data subjects consent how was this recorded?	
Is the data accurate/up to date/ historic	
What are the risks to individuals of sharing and of not sharing	
Seriousness of risk and likelihood of harm	
Are there other means of achieving the purpose	
What is the minimum which can be shared to achieve the purpose	
Where applicable summarise any advice received	

Decision	
Reason for sharing	
Any specific arrangements re: Secure method of sharing Retention/deletion of data	
Whether or not safe to inform data subject	
Any other organisations likely to have access to the data	
Date of disclosure	
Decision taken by (name and position):	
Dated	Signed