DRAFT INFORMATION SHARING POLICY	21 February 2017
CORPORATE POLICY AND RESOURCES COMMITTEE	For Decision

Linkage to Council Strategy (2015-19)	
Strategic Theme	Leader and Champion
Outcome	Establish key relationships with strategic partners to deliver our vision for this Council area
Lead Officer	Head of Policy & Community Planning
Cost: (If applicable)	

1.0 Introduction

1.1 There is a strong government emphasis on the sharing of information across organisations in order to encourage effective co-ordination and integration of services. However, the sharing of information brings within it certain security and confidentiality issues, particularly in relation to the sharing of personal information.

1.2 Information can relate to customers, employees, members of the public or any other identifiable individual and personal information is anything that contains the means to identify a person, eg, name, address, postcode, date of birth.

2.0 Draft Information Sharing Policy

2.1 It is essential the Council has safeguards and protections in place to protect the information that it gathers, creates, processes and discloses in order to comply with the Data Protection Act 1998. This draft policy sets out the requirements placed on employees when sharing personal information within Council and between the Council and other bodies.

2.2 Information Sharing means the disclosure of personal information to a third party. The need to share this type of information can be required for many reasons and the draft policy outlines the factors for staff to consider when deciding to enter into an arrangement to share personal data. This includes setting up an information sharing agreement and undertaking a Privacy Impact Assessment.

3.0 Recommendation

3.1 **It is recommended** that the Corporate Policy and Resources Committee recommend to Council the approval of the draft Information Sharing Policy as set out in **Appendix 1**.

Causeway Coast & Glens Borough Council

Information Sharing Policy
(also known as data sharing policy)

Policy Number	CCG/29/16/P
Version Number	
Author	Linda R McKee

Date of Screening of Policy	
EQIA Recommended?	YES/NO
Date Adopted by Council	
Date Policy Revised	

Version	Review Date	Author / Reviewer	Amendments
0.1	July 2016	Linda R McKee	Draft.
0.2	July 2016	Linda R McKee	Appendices added
0.3	23 August 2016	Elaine Kirk, Solicitor	Staff replaced with workers. 2.2 Personal confidential data definition to remain. Para 16 clarified.
0.4	22 November 2016	ISMG	Typos corrected. To progress to Council Committee stage.
0.5	13 February 2017	Equality and Diversity Officer	Reference inserted to available in other formats

Linkages

The following internal documents will provide additional information:

Freedom of Information Policy
Data Protection Policy and associated guidance to assist with compliance
Records Management Policy and Procedures
A guide to physical, ICT and security policy

The following external documents will provide additional information:

Data Sharing: Code of Practice	Information Commissioners Office
Conducting Privacy Impact Assessment – Code of Practice	Information Commissioners Office
Anonymisation code of practice	Information Commissioners Office
Data Sharing Code of Practice	Information Commissioners Office
Public Sector Data Sharing: Guidance on the Law	Ministry of Justice. http://justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet / staff portal

EVALUATION AND REVIEW OF THE POLICIES

The Policy will, under normal circumstances, be reviewed every three years, and, from time to time, updates and re-issues will be circulated.

However, the policies will be reviewed sooner in the event of any one or more of the following:

- Failure of weakness in the policy is highlighted
- Changes in legislative requirements.
- Changes in Government / Council or other directives and requirements.

SECTION 75 EQUALITY AND GOOD RELATIONS

Causeway Coast and Glens Borough Council is fully committed to meeting its obligations in relation to Equality and Good Relations under Section 75 of the Northern Ireland Act. In this regard this policy will be screened using Section 75 guidelines and will be subject to an Equality Impact Assessment if found necessary as a result of the screening process.

A copy of the Policy can be obtained from the Council in alternative formats, including in large print, in Braille, and on audio cassette.

CONTACT DETAILS

Any issues or queries relating to these policies should be addressed to:

Head of Policy
Causeway Coast and Glens Borough Council
66 Portstewart Road
Coleraine BT52 1EY
Tel: 028 7034 7163
E-Mail: Elizabeth.Beattie@causewaycoastandglens.gov.uk
Textphone 028 7034 7056

(The policy statement should be signed and dated as follows by relevant Council representatives and Trade Union representatives)

Signed: _____ Date: _____

Mayor

Causeway Coast and Glens Borough Council

Signed: _____ Date: _____

Chief Executive

Causeway Coast and Glens Borough Council

Contents

1. Introduction

1.1. Government policy places a strong emphasis on the need to share information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of services.

1.2. The Government has also emphasised the importance of security and confidentiality in relation to personal information and has strengthened the legislation and guidance in this area in particular through the Data Protection Act 1998.

1.3. It is important that Council protects and safeguards person-identifiable information that it gathers, creates processes and discloses, in order to comply with the law, relevant mandatory requirements and to provide assurance to clients and the public.

1.4. An explanation of what is meant by information sharing can be found in section 4.

1.5. All employees to include temporary / agency workers and contractors working in the Council are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 1998 (Appendix B).

1.6. This policy sets out the requirements placed on all Council staff to include temporary / agency workers when sharing personal information within the Council and between the Council and other bodies.

1.7. The Information Commissioner states in the data sharing code of practice "*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 efficient service .... but.... rights under the Data Protection Act must be respected. Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness*."

1.8. Information can relate to clients, staff (including temporary / agency workers), members of the public, or any other identifiable individual, however stored. Information may be held on paper, CD / DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

1.9. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, Council reference number and must not be stored on removable or mobile media unless it is encrypted as per current Guidance. Further guidance is available in relevant procedures.

1.10. 'Confidential' information can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including employee records, occupational health records, etc.

1.11. The Framework for information sharing which forms the key guiding principles of this policy can be found in Appendix A.

2. Scope

2.1. Staff working in or on behalf of Council (including contractors, temporary / agency workers, secondees and all employees). are within the document scope.

2.2. Information includes:

- Person identifiable data / information e.g. employee records (see 1.10)
- Personal confidential data is a term defined in the Health Sector's Caldicott Review. This term describes personal information about identified or identifiable individuals, which should be kept private or secret. 'Personal' includes the DPA definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.

3. Aims of the Policy

3.1. The aim of this policy is to:

- provide a framework for Council and those working on its behalf to:
- provide information to deliver better services
- consider the controls needed for information sharing,
- ensure the expected standards are met (including that partners to information sharing are aware of the obligations of consent or how to take appropriate account of an individual's objection)

3.2. Establish a mechanism for the exchange of information between Council and other organisations.

4. Sharing Information

4.1. Information sharing, in the context of this policy, means the disclosure of personal information from one or more organisations to a third party organisation or organisations. Information sharing can take the form of:

- a reciprocal exchange of data;
- one or more organisations providing data to a third party or parties;
- several organisations pooling information and making it available to each other;
- several organisations pooling information and making it available to a third party or parties;

- exceptional, one-off disclosures of data in unexpected or emergency situations;

4.2. Sharing non personal information with other organisations - Key information is shared with other organisations to: improve client experience; facilitate commissioning of services; manage and plan future services; facilitate quality improvement and leadership; assure and improve the quality of services; statutory returns and requests; train staff / workers; audit performance.

4.3. Sharing personal information with other organisations – where necessary and proportionate, personal information may be shared with other organisations to: Investigate complaints or potential legal claims; protect children and adults at risk; assess need, service delivery and treatment.

4.4. This policy covers two main types of information sharing:

- 'systematic', routine information sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional,
- one-off decisions to share information for any of a range of purposes.

4.5. Different approaches apply to these two types of information sharing and this policy reflects this. Some of the good practice recommendations that are relevant to systematic, routine information sharing are not applicable to one-off decisions about sharing.

4.6. 'Systematic' information sharing - This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes.

4.7. Ad hoc or 'one-off' information sharing - much information sharing takes place in a pre-planned and routine way. As such, this should be governed by established rules and procedures. However, departments / staff / workers may also decide, or be asked, to share information in situations which are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation.

4.8. Factors to consider - When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) you should consider **what is the sharing meant to achieve?** There should be a clear objective, or set of objectives. Being clear about this will identify the following:

- **Could the objective be achieved without sharing the data or by anonymising it?** It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.
- **What information needs to be shared?** You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives. **Use the minimum necessary personal confidential data.**
- **Who requires access to the shared personal data?** You should employ 'need to know' principles, meaning that when sharing both

internally between departments and externally with other organisations individuals should only have access to your data if they need it to do their job, and that only relevant staff / workers should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.

- **When should it be shared?** Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.
- **How should it be shared?** This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.
- **How can we check the sharing is achieving its objectives?** You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.
- **How are individuals made aware of the information sharing?** Consider what to tell the individuals concerned. Is their consent needed? Do they have an opportunity to object? How do you take account of their objections? How do you ensure the individual's rights are respected and can be exercised e.g. how can they access the information held once shared?
- **What risk to the individual and/or the organisation does the data sharing pose?** For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them? The seven golden rules are found at Appendix G.

It is good practice to document all decisions and reasoning related to the information sharing. A decision recording check list for ad hoc and systemic requests are found at Appendix C and D respectively.

4.9. In all circumstances of information sharing, staff / workers will ensure that:

- When information needs to be shared, sharing complies with the law, guidance and best practice;
- Only the minimum information necessary for the purpose will be shared and, if sharing with providers, will only be shared when the contract explicitly permits it;
- Individuals' rights will be respected, particularly confidentiality and security
- Confidentiality must be adhered to unless there is a robust public interest or a legal justification in disclosure;
- Reviews of information sharing should be undertaken to ensure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations

4.10. Some information sharing does not involve personal data, for example where only statistics that cannot identify anyone are being shared. Regard must be

had to the document Information Commissioners Office (ICO) anonymisation code of practice[1]

5. Information Sharing Agreements

5.1. Information sharing agreements – sometimes known as 'Information or data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in an information sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

5.2. An information sharing agreement must, at least, document the following:

- the purpose, or purposes, of the sharing;
- the legal basis for sharing;
- the potential recipients or types of recipient and the circumstances in which they will have access;
- who the data controller(s) is and any data processor(s);
- the data to be shared;
- data quality – accuracy, relevance, usability;
- data security;
- retention of shared data;
- individuals' rights – procedures for dealing with access requests, queries and complaints;
- review of effectiveness / termination of the sharing agreement; and
- any particular obligations on all parties to the agreement, giving an assurance around the standards expected;
- sanctions for failure to comply with the agreement or breaches by individual staff / workers;
- Where organisations are unable to demonstrate the required information governance performance to be classified as 'trusted', routine information sharing continues to require information sharing protocols in order to ensure that the 'rules' are clearly understood and that the requirements of law and guidance are being met. This is not to say that these organisations are failing to deliver effective information governance, rather that there is no agreed means for them to demonstrate that they are doing so in the absence of an agreed protocol.

5.3. Templates for Information Sharing Agreements are available at Appendix E (time-limited, minor projects) and F (systemic, ongoing projects) and can also

[1] http://ico.org.uk/fororganisations/dataprotection/topicguides/anonymisation

be found on the staff portal. The templates cover the sharing of personal identifiable information and the process for signing off any such agreement.

5.4. Where a data sharing agreement is not held and a request is received to release person identifiable information, it should be forwarded to the Information Governance Officer to record on the central database and for follow up action.

6. Privacy Impact Assessment

6.1. Before entering into any new data sharing arrangements, the Information Commissioner recommends undertaking a privacy impact assessment. This will help to assess the benefits that the information sharing might bring to particular individuals or society more widely. It will also help to assess any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals as well as the controls required to manage the associated risks.

6.2. As well as harm to individuals, staff / workers should consider potential harm to the organisation's reputation which may arise if information is shared inappropriately, or not shared when it should be. Further information on privacy impact assessments is available from the Information Commissioners website[2], this includes 'editable annexes[3]' to assist with the privacy impact assessment.

7. Further Advice

7.1. With information sharing there will always be exceptional and difficult circumstances where advice may be needed. The Information Governance Officer should be consulted where there are any concerns about whether the proposed information sharing is appropriate. The issue, subsequent decisions and actions should be documented.

8. Distribution and Implementation

8.1 Distribution Plan

8.1.1. This document will be made available to all Staff / Workers via the Council internet site / staff portal.

8.1.2. A global notice will be sent to all Staff / Workers notifying them of the release of this document.

9. Monitoring

9.1. Compliance with the policies and procedures laid down in this document will be monitored via Information Governance, together with independent reviews by both Internal and External Audit on a periodic basis.

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/
[3] https://ico.org.uk/media/for-organisations/documents/1042836/pia-code-of-practice-editable-annexes.docx

9.2. The Information Governance Officer is responsible for the monitoring, revision and updating of this document.

Appendix A:

Summary of Legal and Council Mandated Frameworks

Council is obliged to abide by all relevant UK and European Union legislation.

The requirement to comply with this legislation shall be devolved to employees and agents of Council, who may be held personally accountable for any breaches of information security for which they may be held responsible. Council shall comply with the following legislation and guidance as appropriate:

Public Sector Data Sharing: Guidance on the Law

1. There is no single source of law that regulates the powers that a public body has to use and to share personal information. The collection, use and disclosure of personal information is governed by a number of different areas of law as follows:

- the law that governs the actions of public bodies (administrative law);
- the Data Protection Act 1998
- the Human Rights Act 1998 and the European Convention on Human Rights;
- the common law tort of breach of confidence;

2. The interrelationship between the above areas of law is quite complex. The starting point is always to determine whether the public body has the power to carry out any proposed data sharing. This will be a matter of administrative law.

3. The relevant legislation will probably define the organisation's functions in terms of its purposes, the things that it must do, and the powers which the organisation may exercise in order to achieve those purposes, the things that it may do. So it is necessary to identify where the data sharing in question would fit, if at all, into the range of things that the organisation is able to do. Broadly speaking, there are three ways in which it may do so:

- **Express obligations** – Occasionally, a public body will be legally obliged to share particular information with a named organisation. This will only be the case in highly specific circumstances but, where such an obligation applies, it is clearly permissible to share the information.
- **Express powers** – Sometimes, a public body will have an express power to share information. Again, an express power will often be designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways".
- **Implied powers** – Often, the legislation regulating a public body's activities is silent on the issue of data sharing. In these circumstances it may be possible to rely on an implied power to share information derived from the express provisions of the legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted. To decide if you can rely on an implied power, you will need to identify the activity to

which the proposed data sharing would be “reasonably incidental”, and then check that the organisation has the power to engage in that activity.

4. The legal framework that applies to private and third sector organisations differs from that which applies to public sector organisations, which may only act within their statutory powers. However, all bodies must comply fully with the data protection principles (See the Data Protection Act below).

5. Whatever the source of an organisation’s power to share information, you must check that the power covers the particular disclosure or data sharing arrangement in question – otherwise, you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place. This might be the case where a Council breaches a duty of confidentiality because an Officer of Council believes that a client has been involved in serious crime. Whilst a disclosure in the public interest may be defensible in a particular case, this does not constitute a legal power to share data.

6. It is also important to ascertain whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions.

7. The next stage is then to consider whether the proposed data sharing might nevertheless be unlawful due to the operation of the Data Protection Act 1998, Human Rights Act 1998, or the common law tort of breach of confidence.

The Data Protection Act 1998[4]

8. The DPA applies to living individuals and gives those individuals a number of important rights to ensure that personal information covered by the Act is processed lawfully. It regulates the manner in which such information can be collected, used and stored, and so is of prime importance in the context of information sharing. Key principles in the DPA that are relevant to information sharing are, personal information must be:

i. Processed fairly and lawfully and, in particular, shall not be processed unless-(a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met”

ii. Processed for specified and lawful purposes.

iii. Adequate, relevant and not excessive.

iv. Accurate and where necessary kept up to date.

v. Not kept longer than necessary, for the purpose(s) it is used.

vi. Personal data are not to be regarded as being processed fairly unless the data subjects are provided with (or have ready access to) certain information, either prior to, or at the time that the processing first takes place, or very soon afterwards. This information includes the identity of the data controller; the purposes for which the data are intended to be processed; and any further information that is necessary in order for the processing to be

[4] http://www.legislation.gov.uk/UKPGA/1998/29/contents

regarded as fair. Usually this requirement is complied with through the provision of 'fair processing notices' which are drawn to the data subject's attention when they supply the personal data to the data controller. Processed in accordance with the rights of the data subject under the Act.

vii. Appropriate technical and organisational measures are be taken to guard against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data

viii. Not transferred to countries outside the European Economic Area (EEA) without an adequate level protection in place.

9. The DPA imposes obligations upon 'data controllers' when they are 'processing' 'personal data', and gives rights to 'data subjects'.

10. Sections 1 and 2 of the DPA define these concepts:

'Data' includes all automatically processed information as well as some manual records

'Personal data' means data relating to an identified or identifiable living individual. Anonymised data may still be personal data if the data controller can identify who the information relates to.

'Sensitive personal data' are personal data consisting of information as to racial or ethnic origin, political opinions, religious and similar beliefs, trade union membership, physical or mental health, sexual life, and the commission or alleged commission of any offence or criminal proceeding. The DPA imposes additional requirements in relation to the processing (including the sharing) of such data.

The **'processing'** of personal data includes anything which may be done to personal data, such as obtaining, holding, using, disclosing or destroying it. Many types of public sector data sharing will involve information held on computer, so if the information relates to identified or identifiable individuals, it will be clear that the DPA applies.

'Data controllers' are persons who determine the purposes for which, and the manner in which, the personal data are processed.

'Data processors' are persons who process personal data on behalf of a data controller, rather than on their own behalf.

'Data subjects' are the individuals to whom the personal data relate.

Human Rights Act 1998[5]

11. Public authorities must comply with the Human Rights Act 1998 (HRA) in the performance of their functions. The HRA also applies to organisations in the private sector insofar as they carry out functions of a public nature. Where the HRA applies, organisations must not act in a way that would be incompatible with rights under the European Convention on Human Rights.

[5] http://www.legislation.gov.uk/ukpga/1998/42/contents

12. Article 8 of the Convention, which gives everyone the right to respect for his private and family life, his home and his correspondence, is especially relevant to sharing personal data. Article 8 is not an absolute right – public authorities are permitted to interfere with it if it is lawful and proportionate to do so.

13. It is advisable to seek specialist advice if the disclosure or data sharing arrangement you are proposing engages Article 8 or any other Convention right. However, if you disclose or share personal data only in ways that comply with the DPA, the sharing or disclosure of that information is also likely to comply with the HRA.

The Common Law Duty of Confidentiality

14. Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

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

16. In practice, this means that all client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the client.

17. Three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has consented;
- where disclosure is necessary to safeguard the individual, or others, or is in the public interest; or
- where there is a legal duty to do so, for example a court order. Therefore, under the common law, a service provider wishing to disclose a client's personal information to anyone outside the team providing a service should first seek the consent of that client.

18. Where this is not possible, an organisation may be able to rely on disclosure being in the overriding safeguarding interest of the individual or others or in the public interest. However, whether a disclosure is in the public interest is not a decision to be taken lightly. Solid justification is required before individual rights are set aside and specialist or legal advice should be sought before the information is disclosed. Any decision to disclose should be fully documented.

19. Disclosures required by court order should be referred to the organisation's legal advisors as promptly as possible, so that any necessary representations may be made to the court, for example to limit the information requested.

20. If a disclosure is made which is not permitted under common law the client could possibly bring a legal action not only against the organisation but also against the individual responsible for the breach.

Appendix B

Data Protection Act 1998 – Schedule 1, 2 and 3

Data Protection Act

1998 c. 29

SCHEDULE 1

SCHEDULE 1. THE DATA PROTECTION PRINCIPLES
PART 1 THE PRINCIPLES

1Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
(a)at least one of the conditions in Schedule 2 is met, and

(b)in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4Personal data shall be accurate and, where necessary, kept up to date.
5Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6Personal data shall be processed in accordance with the rights of data subjects under this Act.
7Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

SCHEDULE 2. CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1The data subject has given his consent to the processing.

2The processing is necessary—

(a)for the performance of a contract to which the data subject is a party, or

(b)for the taking of steps at the request of the data subject with a view to entering into a contract.

3The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4The processing is necessary in order to protect the vital interests of the data subject.

5The processing is necessary—

(a)for the administration of justice,

[F1(aa)for the exercise of any functions of either House of Parliament,**]**

(b)for the exercise of any functions conferred on any person by or under any enactment,

(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d)for the exercise of any other functions of a public nature exercised in the public interest by any person.

SCHEDULE 3. CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1The data subject has given his explicit consent to the processing of the personal data.

2(1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2)The **[F1** Secretary of State**]** may by order—

(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

Appendix C– Data Sharing Checklist – ad hoc request

Data Sharing Checklist – one off request. Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Reference Number:	Record your considerations. Where appropriate refer to the legislation and Data Protection principles.
Is the sharing justified? Key points to consider:	
• Do you think you should share the information?	
• Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?	
• Do you have concerns that an individual is at risk of serious harm?	
• Do you need to consider an exemption in the DPA to share?	
Do you have the power to share? Key points to consider:	
• The type of organisation you work for.	
• Any relevant functions or powers of your organisation.	
• The nature of the information you have been asked to share (for example was it given in confidence?).	
• Any legal obligation to share information (for example a statutory requirement or a court order).	
If you decide to share Key points to consider:	
• What information do you need to share? Only share what is necessary. Distinguish fact from opinion.	
• How should the information be shared? Information must be shared securely. Ensure you are giving information to the right person.	
• Consider whether it is appropriate / safe to inform the individual that you have shared their information.	
Record your decision. Record your data sharing decision and your reasoning – whether or not you shared the information. If you share information you should record:	
• What information was shared and for what purpose	
• When it was shared.	Date:
• Your justification for sharing.	
• Whether the information was shared with or without consent.	Discussed with 3rd Party – YES / NO

Name:	
Job Title:	
Date	
Countersigned by Line Manager / IGO	
Date	

Guidance:

Data Protection Principles.

Personal data must be:

- Processed fairly and lawfully.
- Processed only for one or more specified and lawful purpose.
- Adequate, relevant and not excessive for those purposes.
- Accurate and kept up to date - data subjects have the right to have inaccurate personal data corrected or destroyed if the personal information is inaccurate to any matter of fact.
- Kept for no longer than is necessary for the purposes it is being processed.
- Processed in line with the rights of individuals - this includes the right to be informed of all the information held about them, to prevent processing of their personal information for marketing purposes, and to compensation if they can prove they have been damaged by a data controller's non-compliance with the Act.
- Secured against accidental loss, destruction or damage and against unauthorised or unlawful processing - this applies to you even if your business uses a third party to process personal information on your behalf.
- Not transferred to countries outside the European Economic Area - the EU plus Norway, Iceland and Liechtenstein - that do not have adequate protection for individuals' personal information, unless a condition from Schedule four of the Act can be met.

Further advice and help:
Section 29 considerations: Crime and Taxation
https://ico.org.uk/media/for-organisations/documents/1594/section-29.pdf

Appendix D– Data Sharing Checklist for system sharing

Data Sharing Checklist – systemic sharing. Scenario: You want to enter into an agreement to share personal data on an ongoing basis. This checklist should be used in association with the statutory ICO Code of Practice on Data Sharing.

Reference Number:	Record your considerations. Where appropriate refer to the legislation and Data Protection principles.
Is the sharing justified? Key points to consider:	
• What is the sharing meant to achieve?	
• Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?	
• Is the sharing proportionate to the issue you are addressing?	
• Could the objective be achieved without sharing personal data?	
Do you have the power to share? Key points to consider:	
• The type of organisation you work for.	
• Any relevant functions or powers of your organisation.	
• The nature of the information you have been asked to share (for example was it given in confidence?).	
• Any legal obligation to share information (for example a statutory requirement or a court order).	
If you decide to share. It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:	
• What information needs to be shared?	
• The organisations that need to be involved.	
• What you need to tell people about the data sharing and how you will communicate that information.	
• Measures to ensure adequate security is in place to protect the data	
• What arrangements need to be in place to provide individuals with access to their personal data if they request it	
• Agreed common retention periods for the data	
• Processes to ensure secure deletion takes place	
• Any other considerations	

Guidance:

Data Protection Principles.

Personal data must be:

- Processed fairly and lawfully.
- Processed only for one or more specified and lawful purpose.
- Adequate, relevant and not excessive for those purposes.
- Accurate and kept up to date - data subjects have the right to have inaccurate personal data corrected or destroyed if the personal information is inaccurate to any matter of fact.
- Kept for no longer than is necessary for the purposes it is being processed.
- Processed in line with the rights of individuals - this includes the right to be informed of all the information held about them, to prevent processing of their personal information for marketing purposes, and to compensation if they can prove they have been damaged by a data controller's non-compliance with the Act.
- Secured against accidental loss, destruction or damage and against unauthorised or unlawful processing - this applies to you even if your business uses a third party to process personal information on your behalf.
- Not transferred to countries outside the European Economic Area - the EU plus Norway, Iceland and Liechtenstein - that do not have adequate protection for individuals' personal information, unless a condition from Schedule four of the Act can be met.

Appendix E – Information sharing agrement – for minor, time-limited projects

This Information Sharing Agreement (ISA) defines the arrangements for processing data between …….. and ……. and sits underneath the overarching Information Sharing Protocol (ISP) / Partnership Agreement. The appendices provide further information and guidance should this be needed.

1. Parties to the agreement: Full name and address of the organisations or businesses

2. Why is the information being shared?

3. What information being shared?

4. What is your legal justification for sharing? Has consent been gained if required?

5. How will the information be shared? (e.g. data transfer - include any security measures)

6. How will the information be stored? (e.g. secure server - include any security measures)

7. Who will handle the information – name and job title?

8. How long will the information be kept?

9. How will the information be destroyed?

10. What date will the information be shared? Initial date must be later that the date of the signatures below and should give an indication of subsequent dates for regular sharing.

11. What are the names, roles and contact details of any members of staff who will make sure that the required information is shared at the appropriate time?

12. When will this agreement be reviewed and by whom?

This agreement must be formally approved and signed by both parties before any information sharing takes place. Both parties will ensure that the ISA and any associated documents are known and understood by all staff involved in the process.

Originating organisation

Name of organisation: …….

Name: …….

Position: ……..….

Signature: …… Date: ……..…

Partner organisation

Name of organisation: …….

Name: ……..

Position: ……..

Signature: …… Date: ……

Appendix F – Information Sharing Agreement – template for systemic sharing

INFORMATION SHARING AGREEMENT
[INSERT PURPOSE] BETWEEN THE FOLLOWING [XXXX], [XXXX], [XXXX]
SUMMARY SHEET

Title of Agreement	
Agreement Reference	
Purpose	To facilitate the sharing of xxxx information between the organisations listed below. The purpose of the information sharing is to xxxxx
Partners	
Date agreement comes into force	
Date of agreement review	
Agreement owner	
Agreement drawn up by:	
Location of agreement in force	
Protective Marking (Government Classification)	

VERSION CONTROL

Version Number	Date	Amendments Made	Authorisation

1. INTRODUCTION

1.1. This information sharing agreement has been drawn up under the umbrella of the Information Sharing Framework, which sets out the core information sharing principles which have been agreed by its signatory organisations.

1.2. [Outline overall objectives and any specific legislation you are working under]

1.3. In order to meet this objective it is necessary for partners to share selected information.

2. POLICY STATEMENTS AND PURPOSE

Explain why the proposed data sharing is necessary, the aims you have and the benefits this will bring to the participating organisations, to individuals or to society more widely. This should be documented in precise terms so that all parties are clear as to the purposes for which data may be shared and shared data may be used.

2.1. The purpose of this agreement is to enable information to be shared between the below-named organisations in support of the following objective(s),

- [Objective]

2.2. [What are the benefits?]

2.3. [What are the limits? What is not covered? Are there any agreements in related areas that will operate in parallel?]

3. PARTNERS

Your agreement should identify clearly all the organisations that will be involved in the data sharing and include contact details for both a lead officer in the area concerned and the organisation information sharing lead. It should also contain procedures for including additional organisations in the data sharing arrangement and for dealing with cases where an organisation needs to be excluded from the sharing.

3.1. This agreement is between the partners listed in Appendix 1, from the following organisations:

- [Organisation 1] [Organisation 2]

3.2. If a new partner joins the agreement, a new version of the information sharing agreement will be issued as soon as possible, certainly within one month, and circulated to all participating parties.

3.3. If a partner leaves the agreement, a new version of the information sharing agreement will be issued as soon as possible, certainly within one month to all participating parties. Partners must refer to section 5.9 regarding retention and deletion of information that has been shared.

4. BASIS FOR SHARING

You need to explain your basis for sharing data. If you are a public sector body, you may be under a legal duty to share certain types of personal data. Even if you are not under any legal requirement to share data, you should explain the legal power you have which allows you to share. If you are a private or third sector organisation then you may not need a specific legal power to disclose personal data, but your agreement should still explain how the disclosures will be consistent with the Data Protection Act. If consent is to be a basis for disclosure, then your agreement could also provide a model consent form. It should also address issues surrounding the withholding or retraction of consent. Remember that even if your sharing has a consent basis, you must still ensure that you comply with the Data Protection Act's requirements for ensuring accurate and up to date information and destroying in a timely manner.

4.1. This agreement fulfils the requirements of the following **[delete/add as appropriate]:**

- The Data Protection Act 1998 (sections 29(3) & 35(2)).
- The Data Protection Act 1998 (Principle 1) Schedules 2 and 3
- The Data Protection (Processing of Sensitive Personal Data) Order 2000/417
- The Human Rights Act 1998 (article 8)
- The Freedom of Information Act 2000
- Common Law Duty of Confidentiality

4.2. Any information shared and the processes used to share such information on will be compliant with the relevant Human Rights legislation.

5. PROCESS

5.1. This agreement has been formulated to facilitate the exchange of xxxx information between the signatories. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of the agreement. The balance, between an individual's Human Rights and the need to disclose information, must be assessed to ensure the information shared between agencies is proportionate to the purpose. Anyone in doubt should consult their Information Sharing Lead before proceeding.

5.2. INFORMATION TO BE SHARED

Say how you determined which information would be shared. Then specify the information to be shared - which documents or data and in what circumstances? Are all the items to be shared between all participants or are there more restricted information flows?

Is information shared as and when necessary via individual conscious decisions, or is there ongoing shared access to a common data platform or pool? This section needs the most detailed thinking.

- Information providers: It would be useful to ask each participating organisation to identify the information they would potentially share under the agreement.
- Information receivers: Then work together to review which organisations should receive what information.
- Scope of information to be shared: Then consider, for each set of information that is in scope, whether at or part of it should be provided. The Data Protection Act requires that the information shared should be relevant and not excessive. Therefore, where datasets are being shared, it may be necessary to identify which specific fields will be shared (e.g. Name, Date of Birth, Address (not Email), Religion, Sexual Orientation). Where case file information is being shared, it may be necessary to identify the circumstances which mean a case is in scope for sharing. Is there anything that should specifically not he shared?

5.2.1. [How did you work out what data would be shared?]

5.2.2. [What will this data be shared?]

5.2.3. [What happens if information not specified here needs to be shared to achieve the aims set out — on a one-off basis?] If there is a need to share additional information on a one-off-basis, the parties concerned should consider

whether the sharing is necessary to the agreement and document their considerations/findings, including any additional consents sought (and if not sought, an explanation as to why).

5.2.4. [What happens if information not specified here needs to be shared to achieve the aims set out — on a continued basis?] 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 should agree an addition to the sharing agreement, ensuring that the new information meets the same legislative or consent basis as the original. This addition should be added to the agreement and all parties should sign up to it.

5.3. CONSENT [only include if personal data is involved]

If relevant, confirm how the consent of the data subjects has been / will be secured for the proposed sharing and use of the information that is in scope. There are two key exceptions to the need to obtain consent: (1) where there is a legislative mandate to share the information without consent or (2) where needing to obtain consent may place an individual at risk of harm. Sharing can happen in these circumstances without consent. You can state this in the paragraphs below if this is useful to establish the context behind your actions. Where consent is needed, there must be some form of active communication when information is collected where individuals knowingly indicate consent for the intended use of their data. Have the data subjects given their consent to their information being shared, or do they have access to fair processing notices covering this. There may be different arrangements for each party or a joint arrangement. Privacy notices or fair processing notices are often used to secure consent, in which case, check that they are sufficient for the planned use and provide links to them below. Notices may need to be revised to cover the planned data use or specific consent may need to be obtained relating to the planned activities. If in doubt, refer to the ICO's Privacy Notice Code of Practice. You must make provision to deal with individuals withdrawing or not providing their consent for the use of their data which is anticipated by the sharing agreement. In certain defined circumstances sharing can proceed without consent. Specify here if this is likely to apply.

5.3.1. [How has consent been obtained/how will it be obtained?]

5.3.2. [Arrangements for each partner.]

5.3.3. [Arrangements if consent for sharing is denied by an individual.]

5.3.4. [Arrangements if consent for sharing is withdrawn by an individual.]

5.3.5. [Notes re: the likelihood of need to share without consent if relevant.]

5.4. RIGHT TO SHARE NON-PERSONAL INFORMATION [delete if not relevant]

Some non-personal information is subject to a sharing agreement to control its circulation as it is protected by copyright or licensing arrangements. If this is relevant to you, indicate here what the constraint is, what restricted sharing is allowed and on what basis. Are notifications needed e.g. to a copyright holder, that the information sharing is taking place? Is this conditional e.g. on all parties having a current licence to a given software platform or dataset? If so, what are the arrangements if this ceases to be the case?

5.4.1. [Set out any special basis for restricting the information shared.)

5.4.2. [Any conditions that need to be met, notifications made, etc.]

5.4.3. [Arrangements if conditions are no longer met.]

5.5. RIGHT TO SHARE ANONYMISED AND PSEUDONYMISED INFORMATION [delete if not relevant]

Personal information can be altered so that it is no longer person-specific through aggregation, anonymization or pseudonymisation. While this type of data is no longer person-identifiable in theory, there is sometimes a risk that parts of a dataset could be deanonymised, depending on the size of the involved population and how different datasets are combined. The means that care still needs to be taken in the treatment and management of these datasets to protect the privacy of individuals.

If data is e.g. aggregated, so that the situation of an individual could not be extracted, then individuals could not ask for their information to be removed. If, however, individuals are still represented as lines in the data, although anonymised or pseudonymised, then they could withdraw consent. Paragraphs here will be informed by the materials to be shared.

5.5.1. [Set out any special basis for restricting the information shared.]

5.5.2. [Any conditions that need to be met, notifications made, etc.]

5.6. HAS A PRIVACY IMPACT ASSESSMENT I RISK ASSESSMENT BEEN DONE?

If the data sharing includes personal data a Privacy Impact Assessment (PIA) may be warranted. This is a process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data. It is valuable where a new process or system could poses significant risks to the privacy of individuals. For the sharing of other types of information, a more generic risk assessment may be done. Include details of any assessments which have been done and how their findings have influenced the design of the sharing arrangement. Identity any risks which need to be kept under review during the lifetime of the agreement.

5.6.1. [Was a privacy impact assessment relevant? If so, details. What changed as a result?]

5.6.2. [How will risks be kept under review?]

5.6.3. [Was a risk assessment relevant? If so, details. What changed as a result?]

5.6.4. [How will risks be kept under review?]

5.6.5.

5.7. HOW WILL THE INFORMATION BE TRANSFERRED

Indicate how electronic and hard copy information which is shared under this agreement will be transferred between participating organisations / individuals. If sent electronically, also indicate whether the information will be encrypted? Consult with ICT if necessary. If relevant, also indicate any means of transit which are not acceptable under the agreement. Confirm that decisions to share information must be documented and state how/where this is to be done. Confirm what protective markings you will use to ensure that sensitivity of information is understood.

5.7.1. The Information Sharing Framework provides details of the overall security standards required of participating organisations to manage the information they receive from other parties under this agreement. These must be respected by all signatories.

5.7.2. [Set out requirements specific to this sharing arrangement. What transit mechanisms are acceptable?)

5.7.3. [What transit mechanisms are not acceptable?]

5.7.4. [Active decision making and audit trail for the information shared — specify what is expected.] There must be a record made of each decision to share information. This is to be recorded as follows:

[Organisation 1 – file location or approach]/ [Organisation 2 – file location or approach.]

5.7.5. [Ensuring level of sensitivity is understood – protective marking. If different organisations have different standards, identify them here.] Before being shared, information should be protectively marked as follows:

[Mark 1] [Mark 2]

5.7.6. [Ensuring ownership is understood.] Information that is shared should be labelled with the name of s originator, so that obligations around withdrawal of consent, updating to maintain accurate records and reporting any breaches etc can be fulfilled.

5.8. ENSURING DATA QUALITY

Who is responsible for for data quality? What is the process for ensuring that the data shared is accurate? How will you ensure that the meaning of data is understood so that it is not inadvertently misused once shared? How will you ensure that datasets that have been shared will be kept updated? What will the process be for responding to any complaints about accuracy of personal data?

5.8.1. [Responsibility.] Everyone sharing data under this agreement is responsible for the quality of the data they are sharing

5.8.2. [Accuracy.] Before sharing data, officers will check that the information being shared is accurate and up to date to the best of their knowledge. If sensitive data is being shared which could harm the data subject if it was inaccurate, then particular care must be taken.

5.8.3. [Ensuring meaning is understood.] Where a dataset" is being shared (i.e. structured data), it will be accompanied by a table providing definitions 01 the data fields.

5.8.4. [Ensuring out of date data is not used once shared.] If personal data has been held for longer than [time period...], an updated version must be obtained before [...action...]

5.8.5. [Complaints.] If a complaint is received about the accuracy of personal data which affects datasets shared with partners in this agreement, an updated replacement dataset will be communicated to the partners. The partners will replace the out of date data with the revised data.

5.9. INFORMATION USE, REVIEW, RETENTION AND DELETION

Confirm that information should only be used for the purposes that the agreement was designed to enable. Confirm which organisation is the primary record keeper for the information shared. The information that is shared should not be kept indefinitely. Instead, a retention schedule needs to be defined for it, setting out how long it should be kept before being deleted 'The retention schedule for the master copy of information held by the originating organisation may be different from the retention schedule applied to the copies of that information that have been shared for the purposes of this sharing agreement. What happens to the information that has been shared when the agreement ends e.g. because a project finishes or there is a policy change? What happens to the information that has been shared if a partner leaves the agreement?

5.9.1. Partners to this agreement undertake that information shared under the agreement will only be used for the specific purpose for which it was shared, in line with this agreement. It must not be shared for any other purpose outside of this agreement.

5.9.2. [Record ownership — adapt as appropriate.] In each case, the originating organisation remains the primary information owner and record keeper for the information that is shared. Where information is edited by the receiver, they must make it clear this is an altered copy.

5.9.3. [Retention period — different subsets of information may need to be kept for different lengths of time. If this is the case, draw up a table. If you have an Appendix of information to be shared, add the retention periods to this for ease of reference.] The retention period for the information shared is xxxx from the date of xxxx.

5.9.4. The recipient will not release the information to any third party without obtaining the express written authority of the partner who provided the information.

5.9.5. [Destruction — cover paper and electronic files if appropriate.] The following destruction process will be used when the information is no longer required: [paper] [electronic]

5.9.6. If a partner leaves the agreement, decisions must be taken and followed through on what happens to:

- The information that has already been shared with the signatories by the departing organisation.
- The information that has already been shared with the departing organisation by the other signatories.

5.10. ROLES AND RESPONSIBILITIES UNDER THIS AGREEMENT

Who can share information under this agreement? If it is a finite number of individuals, roles or teams, list them. What information needs to be recorded, if any, about the sharing, that takes place to provide an audit trail? Consider where a template should be set up straight to log sharing. Can shared information be passed on by the received to a third party?

5.10.1. The [people/roles/teams] who will have access to information provided under this Agreement are:

Organisation 1 [Name role, team] [Name, role, team]

Organisation 2 [Name, role, team] [Name, role, team]

5.10.2. All partners to this agreement must appoint Specific Points of Contact (SPOC) — see Appendix 1.

5.10.3. [Responsibility of the SPOC] The SPOC's within each organisation will be the first port of call for questions about the agreement. If there is a problem such as a potential information security breach, relevant SPOCs must be contacted.

5.10.4. It is the responsibility of everyone sharing information and accessing and using the information that has been shared to take appropriate decisions, then hold the information securely, in accordance with the standards set out in the overall Framework and this agreement. Any person who is not sure of the requirements on them should read the Framework and this Agreement, then, if necessary, contact their SPOC.

5.10.5. [Indicate limits on who can share information under this agreement.] Only appropriate and properly 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.

5.10.6. Information shared between partners must not be disclosed to any third party without the written consent of the partner that provided the information. For the purposes of this Agreement, approval for such sharing lies with the SPOC of the originating organisation.

5.11. REVIEW OF THE INFORMATION SHARING AGREEMENT

Confirm when the Information Sharing Agreement will be reviewed and who is responsible for initiating this. What happens if that person leaves their role?

5.11.1. [Review.] This Information Sharing Agreement will be reviewed xxxx months after its launch and xxxx thereafter. The person responsible for initiating this process is: xxxx.

5.11.2. [Exceptional review.] 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.

5.11.3. [Ongoing ownership.] If the lead person departs their role, an alternative lead must be nominated as soon as possible.

5.12. INDEMNITY

5.12.1. xxxx, xxxx and xxxx as receivers of information covered under this Agreement will accept total liability for a breach of this Information Sharing Agreement should legal proceedings be served in relation to the breach.

6. SIGNATURES

6.1. 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.

6.2. Signatories must also ensure that they comply with all relevant legislation

Signed on behalf of xxxx…….

Title: .....

Rank/ Position: .....

Date: .....

Signed on behalf of xxxx…….

Title: .....

Rank/ Position: .....

Date: .....

Appendix 1: Partners, signatories and leads

Organisation	Departments	Lead Signatory NB: Indicate if Specific Point of Contact (SPOC)	Information Sharing Lead NB: Indicate if Specific Point of Contact (SPOC)

Appendix G – Seven golden rules for information sharing[6]:

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. The exceptions to this are where telling the person concerned would put that child, young person or others at increased risk of significant harm (or an adult at risk of serious harm) or if it would undermine the prevention or detection of a serious crime.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

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 for 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, then record what you have shared, with whom and for what purpose. If you decide not to share, record the reason for not sharing.

The *seven golden rules* and the following questions will help support your decision making so you can be more confident that information is being shared legally and professionally. If you answer *not sure* to any of the questions, seek advice from your supervisor, manager, nominated person within your organisation or area, or from a professional body.

Key questions to support decision making:

- Is there a clear and legitimate purpose to share the information?
- Does the information enable a living person to be identified?
- Is it confidential?
- If confidential, do you have consent to share?
- Is there sufficient public interest to share without consent?
- If you decide to share, is it shared appropriately and securely?
- Have you recorded the decision to share or not to share properly?

6 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf