Safer Lancashire Community Safety Information Sharing Protocol

Appendices

June 2022

Contents

Appendix 1: Glossary

Anonymised Data	This is data which does not identify an individual, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.
Caldicott Guardian	A senior person in the NHS or Local Authority with responsibility for Public Health and/or Social Care who is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing
Data	Within this Protocol, data could include personal and/or sensitive personal data
Controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	In relation to personal data, means any person (other than an employee of the Controller) who processes the data on behalf of the Controller.
Data Protection Officer (DPO)	Is responsible for overseeing data protection strategy and implementation to ensure compliance with UK GDPR requirements.
Data Recipient	In relation to personal data, means any person to whom the data are disclosed.
Data Source	The source the data was originally obtained from.
Data Subject	Means an individual who is the subject of personal data.
Disclosure	The divulging or provision of access to data.
Explicit Consent	This means articulated agreement and relates to a clear and voluntary indication of preference of choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.
Consent	This means that the individual has provided freely given consent, which is capable of being withdrawn, and they understand what they have consented to. A record of the consent must be kept, and reviewed as necessary.
Information Commissioner	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals **https://ico.org.uk. The ICO has published a Data Sharing Code of Practice and its data sharing hub provides resources to support lawful information sharing: https://ico.org.uk/for-organisations/data-sharing-information-hub/**
Information Governance Toolkit	Is an online system which allows NHS and Social Care organisations and partners to assess themselves against Department of Health Information Governance policies and standards. It also allows members of the public to view participating organisations' IG Toolkit assessments.
Information Sharing Protocol	Is the document setting out the general reasons and principles for sharing data. The protocol will show that all signatory

	organisations are committed to maintaining agreed standards on handling data and will publish a list of senior signatories. It should be underpinned by data sharing agreements between the organisations who are actually sharing the data.
Information Sharing Agreement (ISA)	Is a document which details the organisations approach to data sharing. Agreements will be produced where organisations specifically identify a purpose to share data across organisational boundaries on a regular basis. The agreement should state whether partners are obliged to, or are merely enabled to, share data.
Organisations	Used in the context of this document to relate to the organisations specified within section 12 of this Protocol which details the organisations that are signatories to this Protocol.
Personal Data	Means any information relating to an identified or identifiable natural person ('data subject') who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. UK GDPR Data protection legislation applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
Pseudonymisation	"Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified However, pseudonymisation can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
Personal data breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
Senior Information Risk Owner (SIRO)	Is in Senior Management and is accountable for information risks and incidents for the organisation. The SIRO will foster a culture of protecting and using data and is concerned with the management of all information assets.
Sensitive Personal Data	Means any information relating to an identified or identifiable natural person ('data subject') who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people. For example, information about an individual's: • race

	• ethnic origin • politics • religion • trade union membership • genetics • biometrics (where used for ID purposes) • health • sex life, or • sexual orientation. The UK GDPR refers to sensitive personal data as "special categories of personal data" (click **here** to see Article 9 of the UK GDPR).

Appendix 2: What is data sharing?

By 'data sharing', we mean the disclosure of data or information from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Data 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 data and making it available to each other.
- Several organisations pooling data and making it available to a third party or parties.
- Exceptional, one-off disclosures of data in unexpected or emergency situations.
- Different parts of the same organisation making data available to each other (this type of data sharing could be subject to internal ISAs as defined by your own organisation).

There are two main types of data sharing:

Systematic data 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.

Exceptional data sharing

The majority of data sharing takes place in a pre-planned and routine way and this Protocol sets out the principles for effective information sharing and the establishment of Information Sharing Agreements (ISAs). However, organisations may also decide, or be asked, to share data in situations which are not covered by any routine agreement i.e. one-off decision to share data for a range of purposes. In some cases, this may involve making a decision about sharing in conditions of real urgency, for example in an emergency if a patient lacks the capacity to give consent.

Different approaches apply to these two types of data sharing and this Protocol and resulting sharing agreements reflect this. Some of the good practice recommendations that are relevant to systematic, routine data sharing are not applicable to one-off decisions about sharing. In either case however, the sharing of personal data must comply with the requirements of the legislation.

Appendix 3: Who can we share data with?

Data sharing can be within organisations, with partner organisations either as a '**Controller**' or as a **'Data Processor**' and with third parties as a '**Sub Data Processor**'.

Sharing with a Controller

The Information Commissioners Office (ICO) define a Controller as "a body who determines the purposes and means of processing personal data." The majority of instances where sharing of data occurs under this Protocol and any ISAs are predominantly about sharing personal data between Controllers.

Controllers, under the UK GDPR guidelines have to ensure that all contracts and ISAs comply with the UK GDPR.

For more information, click **here** to see the ICO website.

Sharing with a Data Processor

Where a Controller shares data with another party that is responsible for the processing of personal data on its behalf, the UK GDPR, DPA and ICO identifies these organisations as 'data processors'.

If you are a processor, the UK GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. See **Appendix 9** for more information on the UK GDPR.

A Controller using a data processor must ensure, in a written contract, that:

- The processor only acts on instructions from the Controller; and
- It has security in place that is equivalent to that imposed on the Controller by the sixth data protection principle; see DPA Act Principles **Appendix 9**.

Information sharing is not solely limited to Partners who are party to this Protocol. It may be that there is a need to share information across departments or with national partners or other organisations not in the Partnership. The UK GDPR and the DPA should not hinder the sharing of information but allow secure and lawful processing and management of information flows.

Sharing within organisations

Data sharing and the data protection principles also apply to the sharing of information between the different departments of an organisation such as local authority or financial services company. An approach and willingness to share information across departments should be encouraged to support the needs of the wider organisation whilst adhering to the principles and requirements set out within this Protocol. Please see your own organisations procedures for guidance.

Sharing with organisation who are not signatories to this protocol

Any organisation who is not party to this overarching Protocol, but who wishes to share information may do so, providing that there is an existing ISA or contract in

place with the third party. In turn, they agree to comply with the terms of this overarching Protocol and have adequate technical and non-technical security arrangements in place, for example compliance with the Information Governance Toolkit. It may be required for your organisation to adhere to another Information Sharing Protocol/Agreement (set out by another Controller), reviewed and agreed by your own organisation.

Once an identified need to share information between organisations and all Parties have agreed the ISA then all of the organisations are responsible for providing a culture of support to ensure that good practice in information sharing is promoted and supported.

The following range of purposes are agreed as justifiable for the transfer of personal confidential information between the partner agencies as defined within the remit of this Protocol from which organisations aim to establish:

- A culture that supports information sharing between and within organisations including proactive mechanisms for identifying and resolving potential issues and opportunities for reflective practice.
- A systematic approach to explain to service users when the service is first accessed, how and why information may be shared.
- Clear systems, standards and procedures for ensuring the security of information and for information sharing.
- Infrastructure and systems to support secure information sharing, for example, access to secure email or online information systems.
- Effective supervision and support in developing practitioners and managers professionals' judgement in making these decisions.
- Mechanisms for monitoring and auditing information sharing practice.
- Designated source of impartial advice and support on information sharing issues, and for resolution of any difference of opinion about information sharing.
- There is an established information sharing governance framework so that staff are clear about the organisations position on information sharing.
- Information sharing governance framework must always recognise the importance of professional judgement in information sharing at the front line and should focus on how to improve practice in information sharing within and between agencies.

Appendix 4: What data can we share?

The Protocol applies to the following types of data:

Personal data
The UK GDPR and DPA (see **Appendix 9**) identifies two types of data Personal and Sensitive personal data (or special category data), both relate to living people (Data Subjects). However, the Caldicott Information Guardian Review identified a third classification of Personal Confidential Data (PCD), which relates to both living and deceased individuals (see **Appendix 10**).

Personal data means data, which relate to a living individual 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 Controller. Such data could include the data subjects name, address, bank details or IP address. Whilst a name on its own may not be enough to identify an individual when it is linked to other information then it will become identifiable and therefore 'personal data'.

Sensitive personal data or special category data. Certain types of personal information classified as sensitive data, the UK GDPR and DPA (which relates to living individuals only) provides that additional conditions must be met for that information to be used and disclosed lawfully.

The term 'sensitive' data refers to information that provides details of:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade Union membership.
- Physical or mental health.
- Sexual life or orientation.
- Processing of generic biometric data for the purpose of uniquely identifying a natural person, or
- Commission or alleged commission of an offence, criminal proceedings or sentence.

Personal data relating to criminal convictions and offences. Additional safeguards are required when sharing personal data relating to offences and convictions. Personal data collected for a law enforcement purpose may only be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.

Personal confidential data (PCD) describes personal information about identified or identifiable individuals which should be kept private or secret and refers to any information held either as manual and/or electronic records, or records held by means of audio and /or visual technology, about a living or deceased individual who can be personally identified from that information. Examples of identifiable data are name, address, postcode, date of birth, NHS number.

Some data sharing does not involve personal data, for example sharing only statistical data that cannot identify anyone. Neither the UK GDPR, DPA nor this Protocol, apply to that type of sharing if an individual cannot be identified.

Anonymised and Pseudonymised information

Information that falls into this category is data about people that has been aggregated, tabulated or has had unique identifier replaced or removed in ways that make it impossible to identify the details of individuals. This can be shared without the consent of the individuals involved and the processing is outside the provisions of the UK GDPR and DPA. However, care should be taken to ensure that it should not be possible to identify individuals either directly or in summation.

This can happen when anonymised information is combined with other data from different organisations, where the aggregated results produce small numbers in a sample, or where traceable reference numbers are used. Click **here** for further

guidance on anonymised information and requirements (Information Commissioners Office 'Code of Practice on Anonymisation').

Non-personal information

Information that does not relate to people; e.g. information about organisations, natural resources and projects, or information about people aggregated to a level that is not about individuals.
There is a general presumption and expectation that sharing of anonymised and non-personal information will occur, unless there are exceptional reasons for this. These may include:

- Commercial confidentiality.
- Where disclosure may forfeit the organisations duty to ensure safe and efficient conduct of organisational operations.
- Policy formulation (where a policy is under development and circulation would prejudice its development).
- Protect other legal and contractual obligations, and
- Where information is marked protectively (for more information refer to your organisations standards for information classifications).

Appendix 5: When can we share data?

Each of the signatory agencies, their staff and representatives, agree to share information between them, to the extent that is fair and lawful. Sharing of information will be for a specific lawful purpose or where appropriate consent has been obtained. There are six lawful bases to processing personal data and at least one of these **must** apply whenever you process personal data:

1. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. See **Appendix 11** for further guidance on consent.
2. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations), an example would be if the Council needs to use the data for the safeguarding of adults or children. For more information in a safeguarding setting see: Safeguarding Seven golden rules for information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers, HM Government, March 2015 **here**.
4. **Vital interests:** the processing is necessary to protect someone's life.
5. **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.
6. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

When is processing 'necessary'?

Many of the lawful bases for processing data depend on the processing being "necessary". This does not mean that processing always has to be essential.

However, it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is a necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.

How do we decide which lawful basis applies?

This depends on your specific purposes and the context of the processing. You should consider which lawful basis best fits the circumstances. You might consider that more than one basis applies, in which case you should identify and document all of them from the start.

You may need to consider a variety of factors, including:

- What is your purpose – what are you trying to achieve?
- Can you reasonably achieve it in a different way?
- Do you have a choice over whether or not to process the data?

Several of the lawful bases relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

If you are a public authority and can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the individual. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the UK GDPR does restrict public authorities' use of these two bases.

Click **here** to see ICO UK GDPR for further information on lawful basis.

The ICO's data sharing hub provides practical tools to help determine whether data can be shared lawfully:
https://ico.org.uk/for-organisations/data-sharing-information-hub/

Appendix 6: Personal Data Breaches

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.

- Alteration of personal data without permission.
- Loss of availability of personal data.

In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

In the event that personal information shared under this Protocol is or may have been compromised, whether accidental or intentional, the organisation making the discovery will, immediately:

- Inform the organisation who provided the data (Controller) of the details.
- Take steps to investigate the cause.
- Take disciplinary action against the person(s) responsible, if appropriate.
- Take appropriate steps to avoid a repetition.
- Take appropriate steps, where possible, to mitigate any impacts.

Upon notification of a breach, the Controller along with the organisation responsible for the breach, and others as appropriate, will assess the potential risks and implications for the individual(s) whose information has been compromised, and if necessary will:

- Notify the individual(s) concerned.
- Advise the individual(s) of their rights.
- Provide the individual(s) with appropriate support.
- Keep a record of any personal data breaches.

Where a breach identified as serious, it will have to be reported to the Information Commissioner's Office (ICO) **within 72 hours** of becoming aware of the breach so notification to the Controller as soon as possible is advisable.

Appendix 7:
Organisational and individual responsibilities

Disclosure of personal confidential information without consent must be justifiable on legal/statutory grounds, or meet the criterion for claiming an exemption under the DPA 2018 (a lawful condition for processing will still be required). Without such justification, both the organisation and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the DPA 2018 or damages for a breach of the Human Rights Act 1998.

Click **here** for a full list of the exemptions on the Information Commissioners Office website.

Organisational responsibilities

Each partner organisation is responsible for making sure that their organisational and security measures protect the lawful use, confidentiality, integrity and availability of information shared under this Protocol.

- Partner organisations will accept the security classifications on information and handle the information accordingly.
- Partner organisations accept responsibility for auditing compliance with the information sharing agreements in which they are involved.
- Partner organisations should make it a condition of employment that its employees will abide by its rules and policies on the protection and use of confidential information and will have relevant training, procedures and checks (such as DBR checks) in place for all staff.
- Partner organisations should make sure that their contracts with external service providers abide by their rules and policies on the protection and use of confidential information.
- The partner organisation originally supplying the information (Controller) should be notified promptly of any breach of confidentiality, or incident, involving a risk or breach of the security of information (**Appendix 6**).
- Partner organisations should have documented policies for records retention, maintenance and secure waste destruction.

Individual responsibilities

Every employee working for the organisations listed in this Partnership Agreement:

- Is personally responsible for the safekeeping of sensitive information they obtain, handle, use and disclose.
- Should know how to obtain, use and share information they legitimately need to do their job.
- Has an obligation to request proof of identity, or take steps to validate the authorisation of another before disclosing sensitive information.
- Must uphold the general principles of confidentiality and data protection as outlined by the UK GDPR (**Appendix 9**), DPA 2018 (**Appendix 9**) and the Caldicott Review 2013 (**Appendix 10**), follow the policies and procedures of their organisation, this Protocol and seek advice when necessary.
- Should be aware that any violation of privacy or breach of confidentiality is unlawful and may be a disciplinary/criminal matter that could lead to dismissal or prosecution.
- Should ensure any information is transferred using an approved, secure method of transportation in accordance with their organisation's policies and procedures.
- Must ensure they follow their own organisation's policies and procedures before releasing any information under this Agreement.

Appendix 8: The Legal Framework

The legal framework within which public sector data sharing takes place is complex and overlapping. There is no single source of Law, which regulates public sector information sharing. The purpose here, therefore, is to highlight the legal framework that affects all types of personal information sharing, rather than serve as a definitive legal reference point. The general legal framework surrounding the sharing of information includes but is not limited to:

United Kingdom Administrative Law (law that governs public bodies actions)	**Crime and Disorder Act 1998**
Human Rights Act 1998 and the European Convention on Human Rights (Article 8.1)	**Education Act 1996, 2002, 2005, 2011**
Health and Social Care (Safety and Quality) Act 2015	**Health Act 1999, 2006, 2009**
General Data Protection Regulation (UK GDPR) 2016	**Care Act 2014**
Data Protection Act 2018	**Mental Capacity Act 2005**
Freedom of Information Act 2000	**Mental Health Act 1983, 2007**
No secrets, Department of Health 2015	**Mental Health (Patients in the Community) Act 1995**
Common Law Duty of Confidence	**NHS Data Security and Protection Toolkit**
Caldicott Principles 2013	**Children and Social Care Act 2017**
Children's Act 1989, 2004	**Computer Misuse Act 1990**
Government Security Classifications April 2014	**Re-Use of Public Sector Information Regulations 2015**

Overall, the law strikes a balance between the rights of individuals and the interests of society. The law is not a barrier to sharing information where there is an overriding public interest in doing so (such as where it is necessary to do so to protect life or prevent crime or harm) provided it is done fairly and lawfully.

Often personal information can be shared simply by informing people from the outset what purposes their information will be used for and then sharing only for those agreed purposes. There are however special legal considerations around sharing information that is personally sensitive or confidential, because this could have serious consequences for individuals. In deciding whether the law allows personal information to be shared, the following four steps should be considered (as recommended by the Ministry of Justice):

1. Establish whether there is a legal basis for sharing the information (i.e. whether the reason for sharing the information has a statutory basis – e.g. the prevention of crime) or whether there are any restrictions (statutory or otherwise) to sharing the information;
2. Decide whether the sharing of the information would interfere with human rights under the European Convention on Human Rights;
3. Decide whether sharing information would breach any common law obligations of confidence;
4. Decide whether the sharing of the information would be in accordance with the Data Protection Act 2018, in particular the Data Protection Principles, as set out in Appendix 5. In addition, the Freedom of Information Act 2000 gives anyone (an individual or an organisation) a right to request access to information from a public body. Where an exemption applies (e.g. it is third party personal information or commercially sensitive information), disclosure may be refused

Appendix 9: Data Protection Principles

Under the UK GDPR, the data protection principles set out the main responsibilities for organisations. Similar provisions are contained within the Data Protection Act 2018 (DPA) in relation to law enforcement processing. The legislative requirements include that Controllers are **accountable** and able to demonstrate **how** you comply with the six principles.

1. **Lawfulness, fairness and transparency:**
   - **Transparency:** Tell the subject what data processing will be done.
   - **Fair:** What is processed must match up with how it has been described
   - **Lawful:** Processing must meet the tests described in UK GDPR [article 5, clause 1(a)]
     (NB Transparency is not a requirement when processing for law enforcement purposes).
2. **Purpose limitations:** Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent. 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.
3. **Data minimisation:** Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[article 5, clause 1(c)] i.e. No more than the minimum amount of data should be kept for specific processing.
4. **Accuracy:** Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)] Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data i.e. 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.
5. **Storage limitations:** Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed". [article 5, clause 1(e)] i.e. Data no longer required should be removed. However, 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 UK GDPR in order to safeguard the rights and freedoms of individuals.
6. **Integrity and confidentiality:** Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage, using appropriate technical or organisational measures." [article 5, clause 1(f)]

The UK GDPR also creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. The UK GDPR provides the following eight rights for individuals:

1. **Lawfulness, fairness and transparency:** The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

2. **The right of access:** Under the UK GDPR, individuals will have the right to obtain:
   - Confirmation that their data is being processed;
   - Access to their personal data; and
   - Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

   These are similar to existing subject access rights under the DPA.

3. **The right to rectification:** When should personal data be rectified? Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

   If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

4. **The right to erasure:** The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

5. **The right to restrict processing:** Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the UK GDPR is similar.

   When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

6. **The right to data portability:** The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7. **The right to object:** Individuals have the right to object to:
   - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
   - direct marketing (including profiling); and
   - processing for purposes of scientific/historical research and statistics.

8. **Rights in relation to automated decision making and profiling:** The UK GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.

Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the UK GDPR.

Click **here** for further reading on the UK GDPR on the Information Commissioners Office website.

Appendix 10: Caldicott Principles

The Caldicott Review 2013 re-enforced the original principles of 1997 now includes a 7th principle regarding the sharing of information.

Principle 1: Justify the purpose(s)
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: Do not use personal confidential data unless it is absolutely necessary
Person 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 been 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.

Click **here** for more information on the Seven Caldicott Principles July 2013 or **here** for the full Caldicott Review.

Appendix 11: Consent

Consent is one of six lawful bases to process personal data under the UK GDPR.

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller. Recital 43 of the UK GDPR gives the example of where the controller is a public authority.

It is important, therefore, that you consider whether consent is the appropriate lawful basis to process the data or whether another ground should be chosen instead. So, if you would still need to process the data without consent, asking for such consent is misleading and unfair.

An alternative lawful basis cannot be relied upon once consent has been refused; therefore, it might be preferable to identify a lawful basis for processing.

Most lawful bases require that processing is 'necessary'. If you cannot demonstrate the processing is necessary, then you are likely to require the consent of the individual as your lawful basis for processing their personal data.

Consent can only be an appropriate lawful basis if the individual is offered control and choice with regard to accepting or declining the terms offered or declining them without detriment.

When asking for consent you need to assess whether it will meet all the requirements to obtain valid consent. The requirement to establish that valid and explicit consent has been obtained is even more important in circumstances where you are processing special category data, such as data relating to health, racial origin, religious and philosophical beliefs etc.

Article 4(11) of the UK GDPR defines consent as: *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmation action, signifies agreement to the processing of personal data relating to him or her."*

The UK GDPR stipulates that consent of the data subject means any:

- freely given;
- specific;
- informed; and

- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

If the individual has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If consent is bundled up as a non-negotiable part of terms and conditions, or if the individual is unable to refuse or withdraw consent without detriment it will not be freely given.

You must pay particular attention to consent forms aimed at children. These should be clearly worded and understandable in order in order to ensure that you can satisfy that you have obtained informed consent.
The following checklist will ensure that your consent form meets the standards required:

1. You have checked that consent is most appropriate lawful basis for processing.
2. You have made the request for consent prominent and separate from terms and conditions.
3. You have asked individuals to positively opt in by clear, affirmative action
4. You have not relied on pre-ticked boxes or any other type of default consent.
5. You use clear, plain language that is easy to understand.
6. You specify why you need the data and what the data will be used for.
7. You give individual or granular options to consent separately to different purposes and type of processing.
8. You name any third party controllers who will be relying on the consent.
9. You tell individuals that they can withdraw their consent at any time.
10. You ensure that individuals can refuse to consent without detriment.
11. You do not make consent a precondition of a service.
12. If you offer online services directly to children, you only seek consent if you have age-verification measures (and parental-consent measures for younger children) in place.

You must ensure that you keep a record of when and how you obtained consent and exactly what the individual was told at the time.

You should regularly review consents to check that the relationship, the processing and the purposes have not changed. You should have processes in place to refresh consent at appropriate intervals, including any parental consents. You must tell individuals that they can withdraw their consent at any time, without detriment, and you must act on withdrawal of consent promptly. It is good practice to use privacy dashboards or other preference-management tools.

You are obliged to inform individuals of their rights under data protection legislation, in addition to other information, such as retention periods and the identity of the Data Protection Officer. Therefore, your consent form should include a link to your Privacy Policy on your website.

Capacity to consent

For a person to have capacity to consent, he/she must be able to comprehend and retain the information material to the decision and must be able to weigh this

information in the decision making process. See guidance as defined in the Mental Capacity Act 2005.

Consent and Children

Until recently section 8 of the Family Law Reform Act entitled young people aged 16 or 17, having capacity, to give informed consent. The courts have held that young people (below the age of 16) who have sufficient understanding and intelligence to enable them to understand fully what is involved will also have capacity to consent. This was augmented by the Fraser (previously Gillick) Competency test. However, if you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent. Click **here** for further information.

It should be seen as good practice to involve the parent(s) or guardian/representative of the young person in the consent process, unless this is against the wishes of the young person. In the case where the wishes of a young person, who is deemed competent to give consent, are opposed to those of their parent/carer, then the young person's wishes should take precedence.

Recording consent - all agencies should have in place a means by which an individual, or their guardian/representative, can record their explicit consent to personal information being disclosed and any limitations, if any, they wish to place on that disclosure.

The consent form should indicate the following:

- details of the agency and person obtaining consent;
- details to identify the person whose personal details may/will be shared;
- the purpose of sharing personal information;
- the organisation(s) with whom the personal information may/will be shared;
- the type of personal information that will be shared;
- details of any sensitive information that will be shared;
- any time limit on the use of the consent;
- any limits on disclosure of personal information, as specified by the individual; and
- details of the person (guardian/representative) giving consent if appropriate.

The individual or their guardian/representative, having signed the consent, should be given a copy for their retention. The consent form should be securely retained on the individual's record and relevant information should be recorded on any electronic systems used, in order to ensure that other members of staff are made aware of the consent and any limitations.

Disclosure without consent

Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the Data Protection 2018 (a lawful basis will still need to be identified). Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability.

There are exceptional circumstances in which a patient's right may be overridden, for example:

- If an individual is believed to be at serious risk of harm, or
- If there is evidence of serious public harm or risk of harm to others, or
- If there is evidence of a serious health risk to an individual, or
- If the non-disclosure would significantly prejudice the prevention, detection or prosecution of a crime, or
- If instructed to do so by a court.

In deciding whether or not disclosure of information given in confidence is justified it is necessary to weigh the harm that would result from breach of confidence against the harm that might result if you fail to disclose the information.

All agencies should designate a person(s) who has the knowledge and authority to take responsibility for making decisions on disclosure without consent. This person(s) should hold sufficient seniority within the organisation with influence on policies and procedures. Within the health and social care agencies it expected that this person will be the Caldicott Guardian.

If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed. A record of the disclosure will be made in the patient's record and the patient must be informed if they have the capacity to understand, or if they do not have the capacity then any person acting on their behalf must be informed.

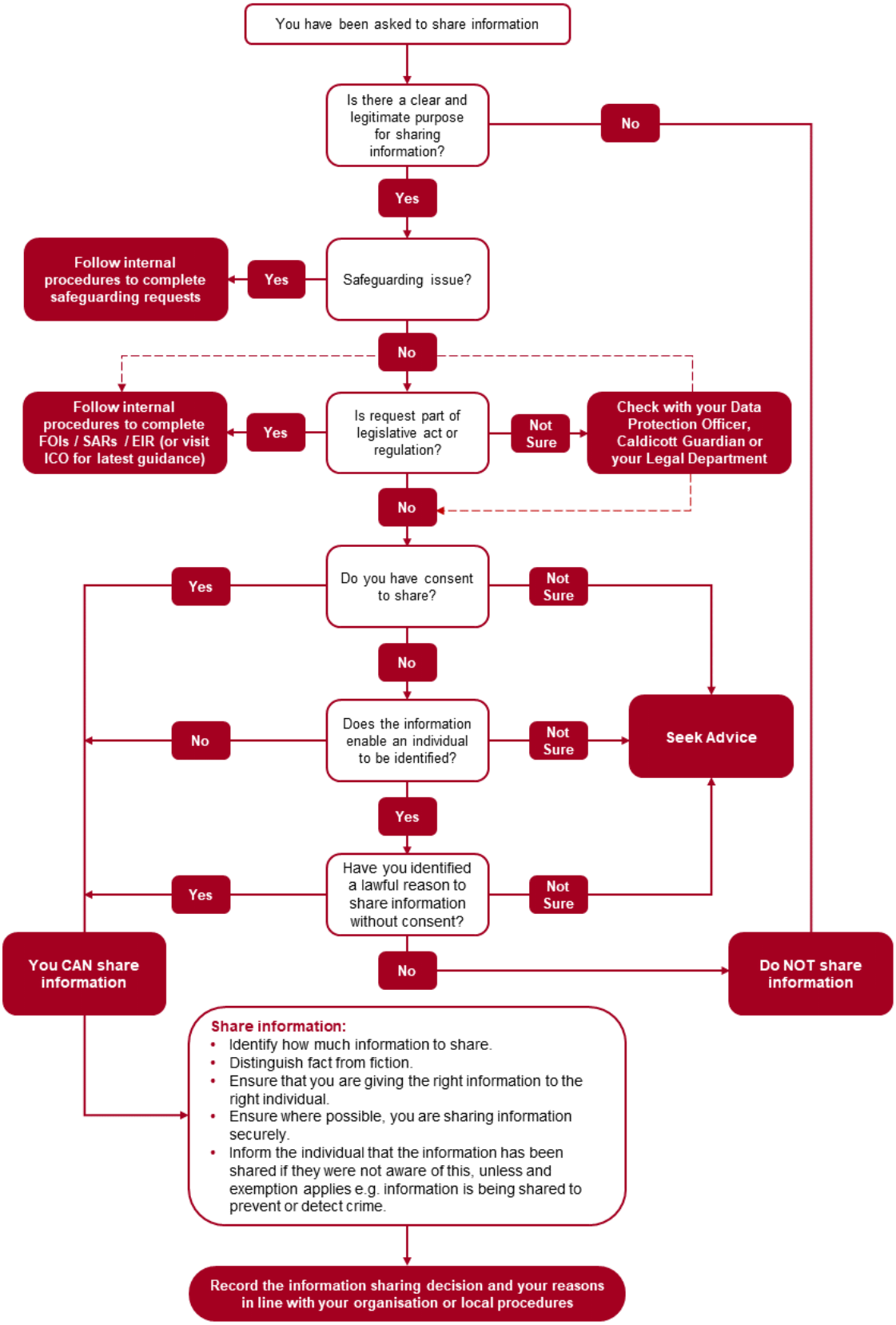
If information is disclosed without consent, there may be some exceptional circumstances (particularly in the context of police investigations or child protection work) where it may not be appropriate to inform the patient of the disclosure of information.

This situation could arise where the safety of a child (or possibly sometimes of an adult) would be jeopardized by informing the patient of such disclosure. In many such situations it will not be a case of never informing the patient, but rather delaying informing them until further enquiries have been made. Any decision not to inform, or to delay informing, should be recorded on the patient's record, clearly stating the reasons for the decision, and the person making that decision.

Further Reading on consent to share information

The Information Governance Review
Information Commissioners Office (ICO)
ICO UK GDPR Consent

Appendix 12: When to Share Information



Appendix 13:
Sample confidentiality declaration sign-in sheet

Name of the meeting:	
Date of meeting:	
Chair:	
Purpose of the meeting:	

Any personal information or sensitive personal information known as special category data disclosed to you during this meeting has been provided to you in strict confidence and for the purpose of:

1. The detection of crime and anti-social behaviour.
2. The prevention of crime and anti-social behaviour.
3. The apprehension of an offender for crime or anti-social behaviour.
4. The prosecution of an offender for crime or anti-social behaviour.

Subject to Section 115 Crime and Disorder Act 1998, the General Data Protection Regulations 2016/679 and Data Protection Act 2018 in particular exemptions to UK GDPR set out at Schedule 2 Part 1 Section 2 Data Protection Act 2018.

- The information shared is done so on a lawful basis. The lawful basis relied upon is to perform a task in the public interest. The lawful basis for processing special category data is in the substantial public interest for the administration of justice. Information should only be shared on a need to know basis and must not be disclosed to any third party, including the data subject and other staff who do not have direct involvement in the original purpose for which it was disclosed.

Further dissemination will only permitted where there is a lawful basis to do so.

- It must be stored securely and permanently deleted when it is no longer required for the purpose for which it is provided.
- Any Lancashire Police information shared is only valid at the time of provision, and should only be used for the purpose as disclosed. It is only disclosed for the specific purpose given at the time of disclosure and should not be used for any other purpose.
- Any information shared will be proportionate and necessary for the purpose for which it is being shared.
- Were possible information shared must be handled and stored in accordance with the Government Security Classifications.
- All persons signing this document are duly authorised to act on behalf of their respective organisation to adhere to the conditions set out.

Please note, by signing this sheet you are agreeing to comply with the requirements of the Lancashire Community Safety Partnership Board Community Safety Information Sharing Protocol and/or the specific Information Sharing Protocol applicable to this meeting.

Name:	Signature:	Organisation Represented:

Appendix 14:
Information Sharing Agreement Template

[Insert Organisational Logo(s)]

[Title of agreement]
Information Sharing Agreement

Based on the ***Safer Lancashire*** Information Sharing Protocol v1.3

Send all Information Sharing Agreements to [**the organisation**] Information Governance or Legal Department for initial review and registration.

Document Status

Version	[insert…Latest version number of the ISA]
Document Owner	[insert…Organisation name]
Document author and enquiry point	[Name] [Job Title] [Contact Details]
Document authoriser	[Name and Job Title of whomever has approved this ISA i.e. Director, Head of Service, DPO, Caldicott Guardian etc.]
Document agreed date	[insert…date all parties have agreed and signed up to the ISA]
Document classification	[insert…Public / Controlled / Restricted]
Document distribution	[insert…list partners organisations]
Document retention period	[insert…for example: 3 years from document review/end date]
Next document review/end date	[insert… date appropriate for this ISA which may depend on your data, 1 or 2 years or change to data and or data processors and sub processors in which case a whole document review may be required and possibly a revised Privacy Impact Assessment]

Version History

Version:	Date:	Contributor / Author:	Description of Change:

1. Introduction

Insert a brief introduction (examples below) - set out any terms and abbreviations.

1.1	This Information Sharing Agreement (Agreement) is to facilitate partnership working between the partners identified in **Section 2.1**. This Agreement identifies the legal powers and methods of sharing information in order to achieve common goals for the benefit of Lancashire.
1.2	This Agreement outlines the need for [**insert**] to work together to [**insert**] etc.
1.3	All Parties to this Agreement should ensure that all of their staff affected by it are aware of its contents and the obligations it creates between the Parties signed up to it.

2. Partner and partner responsibilities

2.1	**The Parties committed to this Agreement are:** *Who are the intended Partners to this Agreement and what are their responsibilities? Including Controller, Data Processor and Sub Data Processors (third parties).* [DELETE THE ABOVE TEXT FROM FINAL ISA] • [Name of organisation] who has the role of Controller • [Name of organisation(s)] who has the role of Data Processor(s) • [Name of organisation(s)] who has the role of Data Sub-processor(s) *Remove if not applicable*
2.2	**It will be the responsibility of these Parties to ensure that they:** • Have realistic expectations from the outset. • Maintain ethical standards. • Have a process to control the flow of information. • Provide appropriate training. • Have adequate arrangements to test compliance with the agreement. • Meet Data Protection Act 2018 (DPA), General Data Protection Regulation (UK GDPR) and other relevant legislative requirements.

3. Background and scope of the Agreement

3.1	*What is the purpose of the agreement? What is the specific business need/objective for information sharing? What are the benefits to sharing these data? Carry out a Data Privacy Impact Assessment (DPIA) on this business process, starting with your organisations DPIA screening questions.* [DELETE THE ABOVE TEXT FROM FINAL ISA] In order to…
3.2	The Agreement covers the sharing of personal data about data subjects for the purpose of [**Enter here**] and the Agreement covers sharing for any of the purposes listed in **Section 5**: **Purposes and legal basis for Sharing Information.**

4. Information to be shared

4.1	*What specific information is required for the purpose of this agreement? List fields of information shared. Do these cover special categories of data, personal data? Consider the identifiability of individuals. (See section 4 of the Protocol for more information on types of data). Could list in a table…* [DELETE THE ABOVE TEXT FROM FINAL ISA] Data to be shared
4.1.1	The Parties have identified that the following fields of data are required to fulfil the purpose and scope of the Agreement as identified in **Sections 3.1 and 3.2.**
4.1.2	These data are to be provided by [**enter Party one here**] and are to be received by [**enter other Party / All remaining Parties**]. If any third party processing via a sub processor, detail it here also.
4.2	**Data Processing** *Detail any processing of data carried out by any of the Parties. In particular, document processing of any special categories of personal data.* [DELETE THE ABOVE TEXT FROM FINAL ISA] Enter text here
4.3	**Terms of use of the information** *Add a clear statement of how the information is used and restrictions that may apply. Consider the enhanced rights of the individual, take Consent and the 'right to be forgotten' into consideration. Is there a Privacy Notice in place for this data? Does the Agreement fit with the agreed terms of re-use (if any)? Could also specify named individuals who would be the responsible for processing the data etc.* [DELETE THE ABOVE TEXT FROM FINAL ISA] Enter text here
4.4	**Exchange of Information** *State explicitly how and what information is to be shared, consider methods such as encrypted email, mail, secure file transfers and how regularly these are to take place.* [DELETE THE ABOVE TEXT FROM FINAL ISA] Enter text here

5. Purposes and legal basis for information sharing

5.1	**Purpose for sharing information** *How will services be improved, what value does the data have, what value will be added by any data processing activity?* [DELETE THE ABOVE TEXT FROM FINAL ISA] The main purpose for sharing information is to…
5.2	**Legal Basis for Sharing Information** *State Legal basis for information sharing. What are the specific lawful powers/obligations for the processing of information?* *What considerations apply to make the processing fair under the terms of the Data Protection Act 2018 or UK GDPR? (Appendix 4 and 5 of the **Safer***

	Lancashire *Partnership Information Sharing Protocol.* [DELETE THE ABOVE TEXT FROM FINAL ISA] The legal basis for sharing information between the Parties is…
5.3	**Other legislation which has an impact on the Agreement** *Could include a brief description of the main impact of relevant legislation and can have an appendix to list all relevant legislation (if applicable), see* ***Appendix 8*** *of the* ***Safer Lancashire*** *Information Sharing Protocol for examples of other legislation.* Enter text here

6. Data Quality

6.1	*Explain what standards will apply for data quality and handling of errors. Taking the UK GDPR principles and rights for individuals into consideration as well as principles 3 and 4 of the DPA 2018 (see* ***Appendix 4 and 5*** *of the* ***Safer Lancashire*** *Information Sharing Protocol), for example:* [DELETE THE ABOVE TEXT FROM FINAL ISA] Information shared under this Agreement must be fit for purpose, meaning that it must be adequate, relevant and not contain excessive detail beyond that required for the agreed purpose.
6.2	*Appropriate records will record sources of information and any methodologies applied when processing the data.* Where information received by any partner is insufficient to achieve the agreed purpose, i.e. inaccurate, out-of-date or inadequate for the stated purpose clarify with the Controller before acting on the information. Partner's receiving such queries will act promptly to resolve them, ensuring documenting corrections and cascading to all Parties immediately.

7. Retention, Storage and Disposal

7.2	*Explain information retention, purpose, storage, and any specific security, review or disposal arrangements that apply.* *State explicitly how long the data is to be held for by all Parties if the Controller intends for the Data Processors to only keep these data for a specified period in accordance with the Controllers retention policy, otherwise could say in line you're your organisations retention policies. How the Parties will dispose of the data at the end of the retention period?* [DELETE THE ABOVE TEXT FROM FINAL ISA] All Parties must ensure that they have appropriate measures in place to ensure the secure storage of all the information subject to this Agreement will be kept as follows: • Physical copies of information provided held in a lockable storage area, office or cabinet.

	• External parties must protect electronic files against illicit internal use or intrusion.

8. Access and Security

8.1	*Explain the standards and conditions, which are required to protect the information concerned. Include any special arrangements, which might apply. For example access to files will be restricted – operate a clear desk policy, employees given access on a need to know basis. Is there any specific training needed or is a basic or enhanced Disclosure and Barring Service (DBS) check required?* [DELETE THE ABOVE TEXT FROM FINAL ISA] Enter text here

9. Handling of complaints, information requests or breaches of the Agreement

9.1	**Handling of data breaches** Data processors, in the event of a personal data breach or breach of confidentiality take steps to notify the Controller and relevant organisations Data Protection Officer(s) (DPO) as soon as possible. The Controller has the responsibility to notify the ICO of a serious breach within 72 hours of any signatory organisations becoming aware of the breach. *Detail the relevant DPO contact information. Organisation will be required to record all information about any personal data breaches.* [DELETE THE ABOVE TEXT FROM FINAL ISA] Enter text here
9.2	**Handling of complaints** Any party, on receipt of a complaint, must immediately…
9.3.1	**Handling of requests for information under Data Protection / FOI** Where the [**non Controller**], in response for [**insert**] information made under the Freedom of Information Act 2000, or the Environmental Information Regulations 2004 or a Subject Access Request, as applicable is considering disclosing [**insert**] information obtained via this Agreement it will consult with [**Controller**] before doing so.
9.3.2	The [**non Controller**], in fulfilling obligations under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004, or Subject Access Request, as applicable, comply with the Data Protection Act 2018 and the General Data Protection Regulation (UK GDPR) where the [**insert**] information includes personal and/or special category data.

10. Commencement and Termination of the Agreement

10.1	**Commencement of the Agreement** This Agreement shall take effect from the date that the Parties fix their ***signatures below*** and shall continue in force for as long as the pilot phase continues or until the termination of this Agreement under **Section 10.2** below.

10.2.1	Any Party may terminate this Agreement at any time provided they give a minimum of 30 days' notice in writing to the other Parties.
10.2.2	If any Party suspects a security breach, this agreement can be suspended for 30 days. Such suspension arrangements allow the affected Party the opportunity to seek a resolution and cause any remedial actions to be completed. In the event that agreement cannot be reached, the Agreement will be terminated in writing with full explanation to the Parties concerned.
10.2.3	The obligations of confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

11. Monitoring, review and dissemination of the Agreement

11.1	**Monitoring of the Agreement** *Detail the procedures and process for monitoring the application of the ISA including who will be responsible for the review process (normally the document author). Detail the responsibilities for monitoring of all Parties. The Controller to review procedures, methods and data during the life of the Agreement i.e. the Audit team review the measures, training, security etc. If the process, methodology or data quality are not what the Controller expects…* [DELETE THE ABOVE TEXT FROM FINAL ISA] Enter text here
11.2	**Review of the Agreement** *Review every two years or when there is any major change to the data, process, relevant legislation or Parties to the Agreement. The Parties agree to notify a representative of the Controller of any requirements to review the Agreement and it will be the responsibility of the Controller to instigate the review.* [DELETE THE ABOVE TEXT FROM FINAL ISA] Enter text here
11.3	**Dissemination of the Agreement** All Parties will disseminate copies of this Agreement to all relevant staff and, on request, to the data subjects of the Agreement process and will ensure that appropriate training is provided to all relevant staff.

12. Signatories

12.1	*Ensure all organisations have agreed to and signed the Agreement **before** information sharing takes place. Check your organisations approval procedures as it may require your Data Projection Officer (DPO), Caldicott Guardian, Senior Information Risk Officer (SIRO), Information Governance lead officer or Director to agree and sign this Agreement.*

Controller: Insert Organisation name

Name and Title/Role	Signature	Date

Data Processor: Insert Organisation name

Name and Title/Role	Signature	Date

Data Processor: Insert Organisation name

Name and Title/Role	Signature	Date