Doncaster Council

www.doncaster.gov.uk

INFORMATION SHARING PROTOCOL

Approving Body	Team Doncaster
Date of Approval	2019
Date of Implementation	2019
Next Review Date	April 2026
Review Responsibility	DMBC Information Governance Team
Version	3.3

REVISIONS/AMENDMENTS SINCE LAST VERSION (IF APPLICABLE)

Date of Review	Amendment Details
1.1	Report to Doncaster Chief Officers Group April 2013.
25/11/2013	Meeting between DMBC/SYP leading to minor amendments
06/06/2014	Amendments incorporated from CCG
22/07/16	Review and Amendment prior to SIRO and Team Doncaster Sign Off
24/01/18 V3	Complete review of the ISP to ensure it is now GDPR compliant ready for sign off by the SIRO and Team Doncaster
20/03/18 V3.1	Amendments incorporated following feedback from SIRO and Team Doncaster.
20/02/2019 V3.2	Review of ISP to Portfolio Group
26/02/19 V3.2	Review of ISP to Team Doncaster
24/04/19 V3.3	Updated Tier 2 Agreement at Appendix II

Contents

DEFINITIONS

Anonymised Information	Information from which no individual can be identified.
Caldicott Guardian	A senior health or social care professional appointed to be the organisation's conscience with regard to all issues relating to health or social care records
Consent & Explicit Consent	An individual's consent should be absolutely clear and a 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. If the information is in relation to special category personal information then explicit consent should be sought unless an exemption under the DPA can be relied on. Privacy notices will ensure that Article 9.2(h) of the General Data Protection Regulation is complied with.
Crime Directive	Refers to the processing of personal data relating to criminal convictions and offences.
Data	Within this agreement this could include personal and/or special category personal information.
Data Controller	The person or organisation who decides the purposes for which and the manner in which any personal data is processed
Data Processor	Any person or organisation (other than an employee of the data controller) who processes data on behalf of the data controller
Data Protection	Processes and polices to protect and oversee the processing and storage of personal data. The legislation and guidance applies universally and not just to public bodies
Data Protection Impact Assessment	A comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data when commencing a new project or updating a system/process.
Data sharing	The disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. This can take the form of systematic, routine data sharing where the same data sets are shared between the same

	organisations for an established purpose, and exceptional one off decisions to share data for any of a range of purposes.
Data Subject	Any living individual to whom personal data relates
Disclosure	The divulging or provision of access to data.
Environmental Information Regulations	Regulations relating to public right of access to information held by a public body which relate to environmental issues such as land, sea, air, emissions, waste, contamination of food etc
Equalities	A range of duties that fall to public bodies to eliminate discrimination, harassment and victimisation and to advance equality of opportunities and facilitate good relations
Freedom of Information	Statute law introduced to support the public's right to request and receive information held by public bodies
General Data Protection Regulation	The GDPR is a regulation which the European Parliament, the Council of the European Union and the European Commission have agreed and implemented from the 25th May 2018 with the intention to strengthen and unify data protection for all individuals within the European Union
Health & Social Care Information Centre	The national provider of information, data and IT systems for health and social care. NHS England has commissioned the HSCIC to deliver the new Data Service for Commissioners (DSC), delivered through Regional Offices (DSCROs). The service will receive and process personal confidential data (PCD) on behalf of Commissioning Support Units (CSUs) and Clinical Commissioning Groups (CCGs).
Human Rights	Legal Rights and duties defined by UK, European and International Law. Article 8 of the Convention on Human Rights sets out obligations for member states on the use of personal data
The Data Security and Protection Toolkit	The Data Security and Protection Toolkit is a NHS online system which also allows organisations to assess themselves. It also allows members of the public to view participating organisation's Toolkit compliance.
Information Sharing Agreement	The Agreement is a more detailed document the intention of which is to spell out how sharing will be carried out between the signatory organisations. The agreement will set out whether partners are 'obliged' or 'enabled' to share information.

Information Sharing Protocol	The Protocol is the high level document setting out the general reasons and principles for sharing data. The Protocol will show that all signatory organisations are committed to maintain agreed standards on handling data and will publish a list of senior signatories. It should be underpinned by Information Sharing Agreements between the organisations who are actually sharing the data.
Interoperability	In relation to electronic systems or software, the ability to exchange and make use of information.
Organisations	Used in the context of this document to relate to the organisations that are signatories to this agreement.
Personal Confidential Data	Personal information about identified or identifiable individuals, which should be kept private or secret. This includes data about deceased individuals.
Personal data	Any data from which a living individual can be identified either from the data or from the data and other information which is in the possession of, or likely to come into the possession of, the data controller
Processing of data	Obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data, including a) organisation, adaptation or alteration of the information or data, b) retrieval, consultation or use of the information or data, c) disclosure of the information or data by transmission, dissemination or otherwise making available, or d) alignment, combination, blocking, erasure or destruction of the information or data.
Senior Information Risk Owner (SIRO)	A role introduced in 2008/9 to ensure board level accountability in public organisations for all risks related to data and information security
Special Category Data	Personal data consisting of information as to a) the racial or ethnic origin of the data subject, b) their political opinions, c) their religious beliefs or other beliefs of a similar nature, d) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), e) their physical or mental health or condition, f) their sexual life or orientation, g) biographical/genetic information
Subject Access Request	Under the GDPR and Data Protection Act, individuals can ask to see the information about themselves that is held on computer and paper records by writing to the person or

	organisation they believe holds it. A subject access request must be made in writing and a reply must be received within 1 month of any necessary checks being carried out.

SECTION A – STRATEGY

1.0. INTRODUCTION & PURPOSE

1.1. An information sharing strategy is crucial for the ethical and legal sharing of information to support partnership working. Information sharing should enable public services to provide seamless services to people and communities driving efficient processes for agencies whilst protecting information appropriately.

1.2. It is equally important that members of the public are confident that their personal information is safe and secure and that it will only be shared in agreed and appropriate circumstances.

1.3. The purpose of this protocol is to provide strategic guidance on the development of information sharing agreements to reflect the needs of any project and each specific information sharing agreement is designed to meet the specific sharing needs of that service.

1.4. In most circumstances there will be a legal or statutory requirement to share data or information but this should still be considered in line with all current Data Protection Legislation, Common Law Duty of Confidentiality, Human Rights Act 1998 and Caldicott principles and it should be proportionate and appropriate.

1.5. Consent to share should be sought if there is no legal or statutory requirement to share and this should be sought at the point of data collection, each organisation's privacy notices must reflect sharing covered in any subsequent Tier 2 Data Sharing Agreements. Data sharing practices and schemes should be published and maintained as required under the Freedom of Information Act 2000. Organisations should publish and regularly update a list of those organisations with which they share and exchange personal information.

1.6. An information sharing agreement will cover the purposes, accountability, restrictions imposed and secure transfer arrangements where data has been shared and each occasion of data sharing of this type will need its own data sharing agreement.

2.0. LEGISLATION AND GUIDANCE

2.1 This strategy does not impose new obligations, but reflects current legislation and regulations. This strategy is informed by the following:

- Access to Health Records Act (1990)
- Caldicott Guardian Manual (2013) DoH
- Children Act (2004)
- Common Law Duty of Confidentiality
- Common Law Powers of Disclosure
- Computer Misuse Act (1990)
- Confidentiality and Disclosure of Health Information Toolkit (BMA 2009)
- Confidentiality Guidance for Doctors (2009) GMC
- Confidentiality: NHS Code of Practice (2003) DoH
- Confidentiality: NHS Code of Practice Supplementary Guidance: Public Interest Disclosures (2010) DoH
- Crime and Disorder Act (1998) (Section 115)
- Criminal Procedures and Investigations Act (1996)

- Data Protection Act 2018
- Data Protection and Sharing – Guidance for Emergency Planners and Responders (HMG 2007)
- Data Sharing Code of Practice Information Commissioner's Office (2011)
- Data Sharing Review Report (Thomas and Walport 2008)
- Environmental Information Regulations (2004)
- Equalities Act 2010
- European Convention for the protection of Human Rights & Fundamental Freedoms (1950)
- European Directive 95/46C (General Data Protection Regulation)
- Freedom of Information Act (2000)
- General Data Protection Regulation 2016
- Health and Social Care Act (2012)
- Homelessness Act 2002
- Housing Act 1985 and 1988 (Schedule 2, Grounds 2 and 14)
- Housing Act 1996 (Section 135, 152 and 153)
- Human Rights Act (1998)
- Information Sharing Guidance for Practitioners and Managers (2008)
- Inspire Regulations (2009)
- Limitation Act 1980
- Management of Police Information Code of Practice (2010)
- Mental Capacity Act (2005) and Code of Practice (2007)
- Mental Health Act 1983
- Multi-Agency Public Protection Arrangements (MAPPA)
- NHS Act (2006)
- NHS Information Governance: Guidance on Legal and Professional Obligations (2007) DoH
- No Secrets: Guidance on developing and implementing multi-agency policies and procedures to protect vulnerable adults from abuse.
- Police Acts (1996) and (1997)
- Protection from Harassment Act 1997
- Records Management Code of Practice for Health and Social Care 2016 NHS Digital
- Regulatory and Investigatory Powers Act (2000)
- Rehabilitation of Offenders Act 1974
- The NMC Code of Professional Conduct: Standards for Conduct, Performance and Ethics (NMC 2004)
- UK Gemini Schematron Schema Guidance (2011)
- Working together to Safeguard Children (2006)

Appendix I provides summary details of the above-mentioned, and related, legislation and guidance.

2.2 The powers and duties identified above, when taken together, create a framework for the sharing of information between different groups of professionals and organisations including the voluntary sector and professionals working across service areas and local authority boundaries. Used proactively, they can facilitate the collection and sharing of information in many of the situations where people are most in need of help and targeted services. These situations are not limited to those where risks have materialised or where the service user is at risk of imminent or serious harm.

Indeed it is a responsibility to share information in order to prevent risk materialisation.

3.0. SCOPE

3.1 This strategy applies to all members of the Team Doncaster Partnership.

4.0. AIMS AND OBJECTIVES

4.1 The primary aim of this strategy is to provide a framework within which information can be shared to support partnership working for the benefit of the people of Doncaster. This strategy is supported by individual information sharing agreements which will outline specific sharing requirements dependent on the required outcome.

5.0 DATA QUALITY

5.1 Shared information / data needs to be of sufficient quality for its intended purpose. This is an essential requirement for all data users and underpins the timely and effective delivery of services. Several characteristics of good data quality have been identified and in summary they are:

- **Accuracy** – Data should be accurate so as to present a fair picture of circumstances and enable informed decision-making at all appropriate levels. Definitions for data should be specific and unambiguous.

- **Validity** – Data should represent clearly and appropriately the intended result and should be used in accordance with the correct application of any rules or definitions.

- **Reliability** – Data should reflect stable and consistent data collection processes that need to be fit for purpose and incorporate controls and verification procedures.

- **Timeliness** – Data input should occur on a regular ongoing basis rather than being stored to be input later. Verification procedures should be as close to the point of input as possible.

- **Relevance** – Information collected should comprise the specific items of interest only. Sometimes definitions need to be modified to reflect changing circumstances in services and practices, to ensure that only relevant data of value to users is collected, analysed and used.

- **Completeness** – All the relevant data must be recorded. Missing or invalid data can lead to incorrect judgement and poor decision-making.

6.0 PRINCIPAL CONSIDERATIONS FOR INFORMATION SHARING

6.1 Information is provided in confidence when it appears reasonable to assume that the provider of the information believed that this would be the case, or

where a person receiving the information knows, or ought to know, that the information is being given in confidence. It is generally accepted that most (if not all) information provided by service users is confidential in nature. All organisations which are party to this framework accept the duty of confidentiality and will not disclose such information without the consent of the person concerned, unless there are statutory grounds or an overriding justification for doing so (see below). In requesting release and disclosure of information from members of partner organisations, staff in all organisations will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that information is not disclosed illegally or inappropriately. This includes third party disclosures.

6.2 As is required by the fair processing requirements of the Data Protection Act and the GDPR, individuals in contact with organisations will be fully informed about information that is to be obtained, held or disclosed about them. The individual also has the right to:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights related to automated decision making or profiling.

6.3 Individuals' rights to confidentiality are not absolute and may be overridden if evidence that disclosure for specific purposes is necessary in exceptional circumstances. Such as:

- Where it is required by statute.
- Where not to share the information poses a public health risk.
- In the vital (life or death) interests of the data subject or another person and consent cannot be obtained.
- Where sharing is required to prevent, detect or prosecute a serious crime such as treason, murder, manslaughter, rape, kidnapping, hostage-taking, causing an explosion likely to endanger life or property and hijacking (this list is not exhaustive).
- Safeguarding of children or vulnerable adults where a lack of information sharing may lead to unjustified delay in making enquiries about allegations of serious harm.

6.4 There must be a clear and justifiable purpose for sharing information such as:

- Supporting the delivery of care
- Improving quality standards
- Effective partnership working
- Monitoring public health
- Audit and research

- Managing incidents, risks and complaints
- Contracting and service planning
- Education and training
- Protecting the vulnerable
- Investigating serious crime and fraud
- Bringing offenders to justice
- Protecting Life and Property
- Preserving Order
- Preventing the commission of offences
- Reducing Crime
- Reducing anti-social behaviour
- Improving confidence and satisfaction with the work of the partnership
- Tackling Substance Misuse
- Protecting the public against extremism and civil emergencies.
- Reducing risk and increasing the safety of victims.

6.5 Consideration should be given as to whether individuals can be identified from the data and if so whether explicit consent can or should be obtained.

- Consider whether some or all of the information can be shared anonymously or in a redacted format
- Patient consent must be obtained wherever it is necessary or appropriate
- Identify a methodology for allowing individuals to be excluded
- In circumstances where identifiable personal data is required and consent cannot be obtained whether a referral to the National Information Governance Board is appropriate.

6.6 The parties to any information sharing agreement must be stated

- Consider who needs to be involved in the sharing of information
- Take into account common or differing rules of confidentiality depending on the information being shared and its source.
- If external contractors are involved the contracts must be specific on the confidentiality of information and any permitted secondary use.
- Ensure all parties sign up to the agreement at the appropriate level (e.g. Caldicott Guardian in health and social care and Chief Information Officer in police forces).

6.7 The actual information to be shared must be defined along with storage and retention criteria;

- Define at the outset the information to be shared and any information that is excluded
- Ensure there is agreement on the responsibilities for managing the shared information, allowing access and re-use and investigating any breaches or inappropriate use

- For each agreement identify a retention period for the shared data and monitor compliance through a reporting system to the Ethics and Governance Group

6.8 The security arrangements for the data in storage and transit must be considered

- Make sure there are clearly defined rules for the way in which information is passed between individuals and teams
- Keep records of information shared and where it is stored
- Identify responsibilities and methods for safe disposal of data
- Ensure access controls have been agreed between all parties

6.9 Mandatory information governance training, support and guidance must be available to all signatories to agreements.

- Ensure all parties to an agreement have received training, appropriate to specific projects and meeting the minimum standards for each partner providing data
- Agree how support and advice will be provided where necessary.

6.10 All information sharing agreements must reflect Partner's Information Governance Strategies, Policies and Procedures including:

- Data Protection Policy
- Information Governance Policy
- Internet and E mail Policy
- Password Management & Access Controls Policy
- Records Management Policy
- Confidentiality Code of Conduct

6.11 Appendix III sets out an easy read process to support decision making with regard to information sharing.

7.0 ACCOUNTABILITY AND RESPONSIBILITIES

7.1 Overall accountability for information held across the organisations lies with each Data Controller who has responsibility for establishing and maintaining effective policies and procedures for meeting all statutory requirements and guidance relating to the processing and sharing of all types of information and data.

7.2 The provision and development of information sharing agreements will be the responsibility of the Local Authority or the Lead partner.

7.3 All signatories have a responsibility to ensure they are familiar with the requirements of this strategy and for ensuring partners are familiar with and

understand the need for robust processes to support working with partners and sharing information.

7.4 All partners are responsible for the safety and confidentiality of information and for ensuring that they comply with the specific Information Sharing Agreement, relevant legislation, guidance and policies and procedures at all times.

SECTION B – PROCEDURE FOR INFORMATION SHARING AGREEMENTS

8.0 STYLE AND FORMAT OF INFORMATION SHARING AGREEMENTS

8.1 All agreements should be written in a style which is concise and clear using unambiguous terms and language. A template for use is attached at Appendix II.

- Purpose of Information Sharing
- Partners – all agencies involved
- Date of Agreement
- Review period
- Relevant legislation and guidance
- Process for sharing including transfer methods
- Types and scope of information to be shared
- Constraints or restrictions on the use of information including consent
- Roles, responsibilities and accountabilities
- Specific issues for the agreement including excluded parties and data
- Review, retention and deletion of information
- Storage of data
- Signature of all relevant parties including Caldicott Guardians where health and social care information is to be shared
- Process for subject access requests under Data Protection Act
- Process for handling Freedom of Information and Environmental Information requests
- Arrangements for access

9.0 DEVELOPMENT AND APPROVAL PROCESS FOR INFORMATION SHARING AGREEMENTS

- **STEP 1:** The need is identified, in line with Article 25 – Privacy by Design of the GDPR, for an information sharing agreement within a service, operational or strategic group or to support a work area.

- **STEP 2:** Draft an agreement to suit the authority using the pre-approved template (APPENDIX II).

- **STEP 3:** Ensure all agencies and departments support and understand the agreement through their respective SIRO Board or other authorising Board.

- **STEP 4:** Seek advice as required from the Caldicott Guardian and/or Information Governance Lead for each authority.

- **STEP 5:** Obtain the formal approval and signatures from organisations and departments depending on the information and functions involved.

- **STEP 6:** Pass a copy of the completed agreement to the Information Governance lead within each authority who will ensure that it is publicly available as appropriate and that it is noted by any relevant committees for each Partner organisation.

SECTION C FORMAL AGREEMENT

THE UNDERSIGNED PARTIES AGREE TO:

- Promote good practice in the sharing of personal, non-personal and depersonalised information by ensuring compliance with the principles, purpose and processes given within this Protocol.
- Take necessary action to identify and rectify and breaches of this Protocol and any associated information sharing agreements, and to have established policies and practices for dealing with complaints about the sharing of information.
- Facilitate the exchange of information where necessary to promote good quality information.
- Ensure that data subjects are informed of their rights in respect of personal information, including right of access and relevant complaints procedures.
- Develop systems of implementation, dissemination, guidance, training and monitoring to ensure that the Protocol is known, understood and followed by all professionals who need to share personal information.
- Establish processes to review the use of the Strategy, in order to ensure that practice is in accordance with the requirements of the Strategy, and to take corrective action as needed.
- Develop and amend the Strategy on an annual basis, taking into account changes in the law or future national guidance.
- Develop information processing systems that ensure collected data is complete, accurate, timely and relevant, leading to effective Data Quality.
- Ensure that collected data is stored and transmitted securely.

SIGNATURES

By signing this Strategy, all signatories accept responsibility on behalf of their organisation for its execution and agree to ensure that their staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purpose of this agreement.

Signatories must also ensure that their organisation and its staff comply with all relevant legislation.

Organisation	Name	Signature
The Mayor of Doncaster	Ros Jones	
Chair, Health and Well Being Board	Councillor Rachael Blake	
Chair, Doncaster CCG	David Crichton	
Doncaster College	Anne Tyrrell	
Doncaster Chamber & Chair, Enterprising Doncaster	Dan Fell	
Chair, Children and Families Forum	Nuala Fennelly	
South Yorkshire Fire and Rescue Services	Helen Hartland	
Chief Executive, Doncaster Council	Jo Miller	
South Yorkshire Police	Shaun Morley	
Chief Executive, Doncaster Children's Services Trust	Paul Moffat	
Chief Officer, Doncaster CCG	Jackie Pederson	
Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust	Richard Parker	
Rotherham, Doncaster & South Humber NHS Foundation Trust	Kathryn Singh	
Department for Work and Pensions	Sharon Thorpe	
Doncaster Voluntary & Community Sector		

Organisation	Name	Signature
The Mayor of Doncaster	Ros Jones	
St Leger Homes of Doncaster	Julie Crooks	
Assistant Director, Commissioning & Business Development, Children & Young People, Doncaster Council	Leanne Hornsby	

APPENDIX I

SUMMARY OF KEY LEGISLATION AND GUIDANCE
(Detailed guidance should be available in all agencies for staff)

Access to Health Records Act 1990

This Act provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements. The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 apart from the sections dealing with access to information about the deceased

Data Protection Act/General Data Protection Regulation

The legislation and regulation applies to personal data. This means any information relating to an identifiable person who can be directly or indirectly identified by referring to a particular identifier.

There are 6 principles that are legally enforceable, these are:

Personal data should be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and where necessary kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.
- Processed in a manner that ensures appropriate security of the personal data.

Organisations, who are Data Controllers, are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the ICO.

Data subjects also have the following rights under the legislation and regulation:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right related to automated decision making including profiling

Crime Directive

Article 10 of the GDPR relates to the processing of personal data relating to criminal convictions and offences.

The Crime Directive 2016 aims to protect the data of data subjects being processed by 'competent authorities' for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data.

Digital Economy Act 2017

Part 6, Sections 108-111 relate to charges payable to the Information Commissioner's Office, these charges replace those set out in the Data Protection Act 1998.

The charges have been agreed and are as follows:

Tier 1 – micro organisations

The organisation has a maximum turnover of £632,000 for a financial year or no more than 10 members of staff. The fee for tier 1 is £40.

Tier 2 – small and medium organisations

The organisation has a maximum turnover of £36 million for a financial year or no more than 250 members of staff. The fee for tier 2 is £60.

Tier 3 – large organisations

If an organisation does not meet the criteria for tier 1 or tier 2, the organization has to pay the tier 3 fee of £2,900.

Crime and Disorder Act 1998

The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area. Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power but only where it is necessary and expedient for the purposes of the Act. However, whilst all organisations have the power to disclose, Section 115 does not impose a requirement on them to exchange information and responsibility for the disclosure remains with the organisation that holds the data. It should be noted, however, that this does not exempt the provider from the requirements of the 2nd Data Protection principle.

The Criminal Procedures and Investigations Act 1996 require the police to record in durable form any information that is relevant to an investigation. The information must be disclosed to the Crown Prosecution Service, who must in turn disclose it to the defence at the relevant time if it might undermine the prosecution case. In cases

where the information is deemed to be of a sensitive nature then the CPS can apply to a judge or magistrate for a ruling as to whether it should be disclosed.

Human Rights Act 1998

Article 8.1 of the Human Rights Act 1998 provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. This is however, a qualified right i.e., there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights and Article 8.2 provides “there shall be no interference by a public authority with the exercise of this right as it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others”.

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

- That it has taken these rights into account
- That it considered whether any breach may result, directly or indirectly, from the action, or lack of action
- If there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights
- Whether one of the permitted grounds for interference could be relied upon
- Whether there was proportionality

The Act also requires public bodies to read and give effect to other legislation in a way that is compatible with these rights and makes it unlawful to act incompatibly with them. As a result these rights still need to be considered, even when there are special statutory powers to share information.

Common Law duty of Confidentiality

All staff working in both the public and private sector are aware that they are subject to a common law Duty of Confidentiality and must abide by this. The duty of confidence only applies to identifiable information and not to aggregate data derived from such information or to information that has otherwise been effectively anonymised i.e., it is not possible for anyone to link the information to a specified individual.

The Duty of Confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g., to protect others from harm). Whilst it is not entirely clear under law whether or not a common law Duty of Confidence extends to the deceased, the Department of Health and professional

bodies responsible for setting ethical standards for health professionals accept that this is the case.

Unless there is a sufficiently robust public interest justification for using identifiable data that has been provided in confidence then the consent of the individual concerned should be gained (deceased individuals may have provided their consent prior to death). Articles 6 and 9 of the General Data Protection Act and the Data Protection Act 2018 apply whether or not the information was provided in confidence.

Where it is judged that an individual is unable to provide consent (for example due to mental incapacity or unconsciousness) other conditions in Articles 6 and 9 of the General Data Protection Act and the Data Protection Act 2018 must be satisfied (processing will normally need to be in the vital interest of the individual).

Whilst under current law, no-one can provide consent on behalf of an adult in order to satisfy the common law requirement, it is generally accepted that decisions about treatment and the disclosure of information should be made by those responsible for providing care and that they should be in the best interests of the individual concerned

.

All organisations are subject to their own codes or standards relating to confidentiality.

Caldicott Report 1997 – And the Caldicott 2 Review 2013

In December 2011 the Government announced that it wanted to allow patients' records and other NHS data to be shared with private life science companies, to make it easier for them to develop and test new drugs and treatments. Concerns were raised about what that might mean for patient confidentiality. This and other issues prompted the instigation of Caldicott 2, in which Dame Fiona was asked to review information issues across the health and social care system.

Dame Fiona first investigated issues surrounding confidentiality when she chaired a similar review in 1996-7 on the use of patient data in the NHS. That review recommended that the NHS adopt six principles (see below) for the protection of confidentiality, which became known as the "Caldicott principles". The review also recommended that NHS organisations appoint someone to take responsibility for ensuring the security of confidential information. These people became known as "Caldicott Guardians".

The reach of Caldicott 2 is far wider than the 1997 report. Its recommendations affect all organisations working in the health and social care sector – including local authorities. Its recommendations, if adopted, will have a significant impact on the way that local authorities operate.

1. **Justify the purpose(s) for using confidential information** - Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

2. **Only transfer/use patient-identifiable information when absolutely necessary** - Patient-identifiable information 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.

3. **Use the minimum identifiable information that is required** - Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. **Access should be on a strict need to know basis** - Only those individuals who need access to patient-identifiable information should have access to it. They should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

5. **Everyone with access to identifiable information must understand his or her responsibilities** - Action should be taken to ensure that those handling patient-identifiable information, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect an individual's confidentiality.

6. **Understand and comply with the law** - Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality** - Professionals should in the patient's interest share information within this framework. Official policies should support them doing so.

Only the NHS and Social Care are required to apply these principles and to nominate a senior person to act as a **Caldicott Guardian** responsible for safeguarding the confidentiality of patient information.

Freedom of Information Act 2000

This Act provides clear statutory rights for those requesting information together with a strong enforcement regime. Under the terms of the Act, any member of the public will be able to apply for access to information held by bodies across the public sector. The release of personal information remains protected by current Data Protection legislation and the GDPR.

The Children Act 2004

The Act provides a legislative spine for the wider strategy to improve children's lives. This covers the universal services which every child accesses, and more targeted

services for those with additional needs. The overall aim is to encourage integrated planning, commissioning and delivery of services as well as improve multi-disciplinary working, remove duplication and increase accountability. There is a duty to cooperate between relevant partners in the making of arrangements to improve the well being of children.

Health and Social Care Act 2012

The Health and Social Care Act 2012 underpins wide ranging reforms of the NHS since it was founded in 1948. Changes include the establishment of a National Health Service Commissioning Board and Clinical Commissioning Groups, as well as Health and Wellbeing Boards. The changes became operational on 1st April 2013. The Act sets out provision relating to public health in the United Kingdom; public involvement in health and social care matters; scrutiny of health matters by local authorities and co-operation between local authorities and commissioners of health care services. The Act establishes a National Institute for Health and Care Excellence, and establishes the provision for health and social care.

The clinical commissioning organisations established by the Act must have a secure legal basis for every specific purpose for which they wish to use identifiable patient data. Where there is no such statutory legal basis either the consent of the patient is required to process personal confidential data or the data must be fully pseudonymised.

Care Act 2014

This Act incorporates a wide range of provisions relating to adult social care, including Safeguarding and most provisions come into force on 1 April 2014.

The sections with most relevance to information sharing are:

Ss 6&7: Duties to cooperate with other persons in the exercise of functions relating to adults with needs for care and support, and to carers.

S37: Duty to notify receiving LA when an adult receiving care and support moves.

S45: Duty to comply with request for information by Safeguarding Adults Board to enable or assist the SAB to exercise its functions. This could include information about individuals.

S67: Involvement of independent advocate in assesments, plans etc.

Statutory guidance is available on all parts of this Act.

Other relevant legislation
Criminal Justice Act 2003
Criminal Procedures and Investigations Act 1996
Civil Contingencies Act 2004
Regulation of Investigatory Powers Act 2000
Homelessness Act 2002

Safeguarding Vulnerable Groups Act 2006
Education Act 2002
Mental Capacity Act 2005
Local Government Act 2000
Mental Health Act 1983
Common Law Duty of Confidentiality

There are statutory restrictions on passing on information linked to:
NHS (Venereal Disease) Regulations 1974
Human Fertilisation and Embryology Act 1990
Abortion Regulations 1991

Further Guidance
HM Government Publications:
Information Sharing: Guidance for practitioners and managers
Information Sharing: Pocket Guide
Available at www.education.gov.uk/publications to download

ICO Publications
Anonymisation Code of Practice
Data Sharing Code of Practice
Subject Access Code of Practice
Guide to Data protection

Available from - http://ico.org.uk/

Doncaster Council

www.doncaster.gov.uk

APPENDIX II

Tier 2 Information Sharing Agreement (ISA)

This Information Sharing Agreement (ISA) defines the arrangements for processing personal, identifiable information between Doncaster Borough Council (DBC) and the organisation stated below.

Data Share Name/Identifier: *For example, Safe and Well*

Between *Doncaster Borough Council* (ICO Registration Number Z7522039)
Providing Information (Data flow)

And: *Enter Organisation Name(s) and ICO Registration Number*
Receiving Information (Data flow)

For what purpose is the information being shared?

Is there a Privacy Notice in place, covering the information to be shared?

☐ Yes - please supply a copy
☐ No – please consider the need to create a notice

Are you:

☐ Collecting new personal data items that have not been collected/shared before?
☐ Introducing new or changing identity authentication requirements which may be intrusive?
☐ Introducing new privacy invasive technologies?
☐ Updating current or providing new links with data in other collections?
☐ Changing the medium for publically available information to enable data to be more readily acceptable?
☐ Converting transactions from anonymised/pseudonymised data to identifiable transactions?
☐ Changing a data delivery method that may be unclear or intrusive?
☐ None of the above

If you have ticked any boxes above, there is a requirement for the host organisation to update/amend their Privacy Notice.

Please provide details below:

What is the legal gateway for sharing?

If relying on consent to share, please specify "Not applicable".

A legal gateway is any piece of legislation which requires or allows the movement of information from one organisation to another. It may place a statutory duty on the organisation or powers on behalf of the individuals concerned.

What information is being shared?

- ☐ Personal
- ☐ Special category
- ☐ Criminal offence data
- ☐ Statistical data

What is the lawful basis for processing (Article 6, GDPR)?

- ☐ Not applicable (statistical data only)
- ☐ Consent
- ☐ Contractual necessity
- ☐ Legal obligation
- ☐ Vital interests
- ☐ Public task
- ☐ Legitimate interests

What is the lawful basis for processing (Article 9, GDPR)?

Special category data **only**: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, and sexual orientation.

- ☐ Not applicable (personal data or statistical data only)
- ☐ Consent
- ☐ Obligations in connection with employment
- ☐ Vital interests
- ☐ Legitimate activities of a not for profit body or association
- ☐ Information has been made public by the data subject
- ☐ Necessary in relation to legal rights
- ☐ Necessary for public functions
- ☐ Necessary for medical purposes
- ☐ Necessary for reasons of public interest in the area of public health
- ☐ Necessary for archiving purposes

What is the lawful basis for processing criminal offence data (Article 10, GDPR)?

Criminal allegations, proceedings or convictions **only**.

- ☐ Not applicable (personal data or special category data or statistical data only)
- ☐ Legal authorisation
- ☐ Official capacity

What are the benefits to sharing the information?

Which data fields/items will be shared?

Please list, for example name, address, telephone number, date of birth, etc.

In what format is the data being transferred and how?

- ☐ Electronic data – accessed on site by staff working for partner organisations
- ☐ Electronic data – by email
- ☐ Electronic data – via automated system to system
- ☐ Electronic data – via manual system transfer
- ☐ Electronic data – via text
- ☐ Information delivered by voice
- ☐ Paper – courier
- ☐ Paper – hand delivered by data subject
- ☐ Paper – hand delivered by staff
- ☐ Paper – standard post
- ☐ Paper – transferred by fax
- ☐ Removable media – hand delivered by staff
- ☐ Removable media – standard post

Further notes on the above:

What is the frequency of the transfer?

- ☐ Instant
- ☐ Daily
- ☐ Weekly
- ☐ Monthly
- ☐ Quarterly
- ☐ Annually
- ☐ Ad hoc
- ☐ Other – please specify:

Further notes on the above:

How many records are being transferred?

Who are the data subjects?

Where will the information be stored by the receiving organisation after transfer?

- ☐ Server – personal or shared drive
- ☐ Server – system on organisation premises
- ☐ Off site server – UK based
- ☐ Off site server – EEA based
- ☐ Off site server – outside of EEA
- ☐ Secure storage on organisations premises
- ☐ Secure storage off organisations premises
- ☐ Other – please specify:

Further notes on the above:

How will the information be secured by the receiving organisation?

- ☐ Area access by key/key pad/access card
- ☐ Password protection
- ☐ Smartcard/system password
- ☐ Other – please specify:

Further notes on the above:

How will the information be accessed by the receiving organisation?

- ☐ Log book
- ☐ Key allocation
- ☐ Key issue log
- ☐ System login
- ☐ Other – please specify:

Further notes on the above:

Who will access the information being shared in the receiving organisation?

- ☐ Employees – professional qualified staff
- ☐ Employees – all staff
- ☐ Volunteers
- ☐ Third parties – other partners
- ☐ Third parties – trusted partners
- ☐ Other – please specify:

Further notes on the above:

How will the information be kept up to date and checked for accuracy and completeness by the providing organisation? Select all that apply.

- ☐ Assurance in place (e.g. IGT, PSN)
- ☐ Staff aware of responsibilities when working with data
- ☐ Clear retention schedules
- ☐ Integrity checks maintained
- ☐ Other – please specify:

Further notes on the above:

Describe your management of the retention and disposal of data by the providing organisation: Select all that apply.

- ☐ Assurance in place (e.g. IGT, PSN)
- ☐ Policies and procedures in place which state/define retention schedules
- ☐ Policies and procedures in place which state/define disposal methods and criteria
- ☐ Other – please specify:

Further notes on the above:

Describe how you deal with Subject Access Requests for individual records and how you rectify / block / erase / destroy as necessary by individual request or court order by the data controller (host organisation): Select all that apply.

- ☐ Assurance in place (e.g. IGT, PSN)
- ☐ Clearly defined procedures in place for Subject Access Requests for individuals
- ☐ Clearly defined procedures in place to handle rectification and blocking of data
- ☐ Other – please specify:

Further notes on the above:

Describe the receiving organisation's policies, processes and standard operating procedures: Select all that apply.

- ☐ Assurance in place (e.g. IGT, PSN)
- ☐ Clearly defined
- ☐ Up-to-date
- ☐ Readily available
- ☐ Understandable (in plain English) for staff to use
- ☐ Other – please specify:

Further notes on the above:

Describe the receiving organisation's management of incidents: Select all that apply.

- [ ] Reviewed, including any root cause analysis and action plans
- [ ] Other – please specify:

Further notes on the above:

Describe the receiving organisation's training for both the system and data: Select all that apply.

- [ ] Assurance in place (e.g. IGT, PSN)
- [ ] Users are aware of their responsibilities when using the asset
- [ ] Regularly trained and tested on their understanding
- [ ] Understand what to do in the event of a breach or incident
- [ ] Other – please specify:

Further notes on the above:

Describe the receiving organisation's security of the asset: Select all that apply.

- [ ] Assurance in place (e.g. IGT, PSN)
- [ ] Secure storage (e.g. locked cabinet)
- [ ] Secure connection (e.g.https:)
- [ ] Secure access (e.g. password protected)
- [ ] Secure encrypted device (e.g. data stick)
- [ ] Managed so only authorised persons can access and access routinely checked
- [ ] Audit trail of interactions
- [ ] Other – please specify:

Further notes on the above:

Describe the receiving organisation's business continuity arrangements:
Select all that apply.

- ☐ Assurance in place (e.g. IGT, PSN)
- ☐ Clear business continuity arrangements
- ☐ Users are aware of arrangements and appropriately trained
- ☐ Regularly reviewed and updated (at least annually)
- ☐ Other – please specify:

Further notes on the above:

Describe the receiving organisation's disaster recovery arrangements:
Select all that apply.

- ☐ Assurance in place (e.g. IGT, PSN)
- ☐ Regularly reviewed and updated (at least annually)
- ☐ Electronic part of a disaster recovery testing regime, regularly tested
- ☐ Other – please specify:

Further notes on the above:

Does the third party/supplier agreement/contract(s) contain all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?

- ☐ Yes
- ☐ No
- ☐ Not applicable

Further notes on the above:

Review cycle:

- ☐ 1 year
- ☐ 2 years
- ☐ 3 years
- ☐ Other – please specify:

Date of agreement:

Date review due:

DBC contact name:

Email address:

Phone number:

Role:

Signed:

contact name:

Email address:

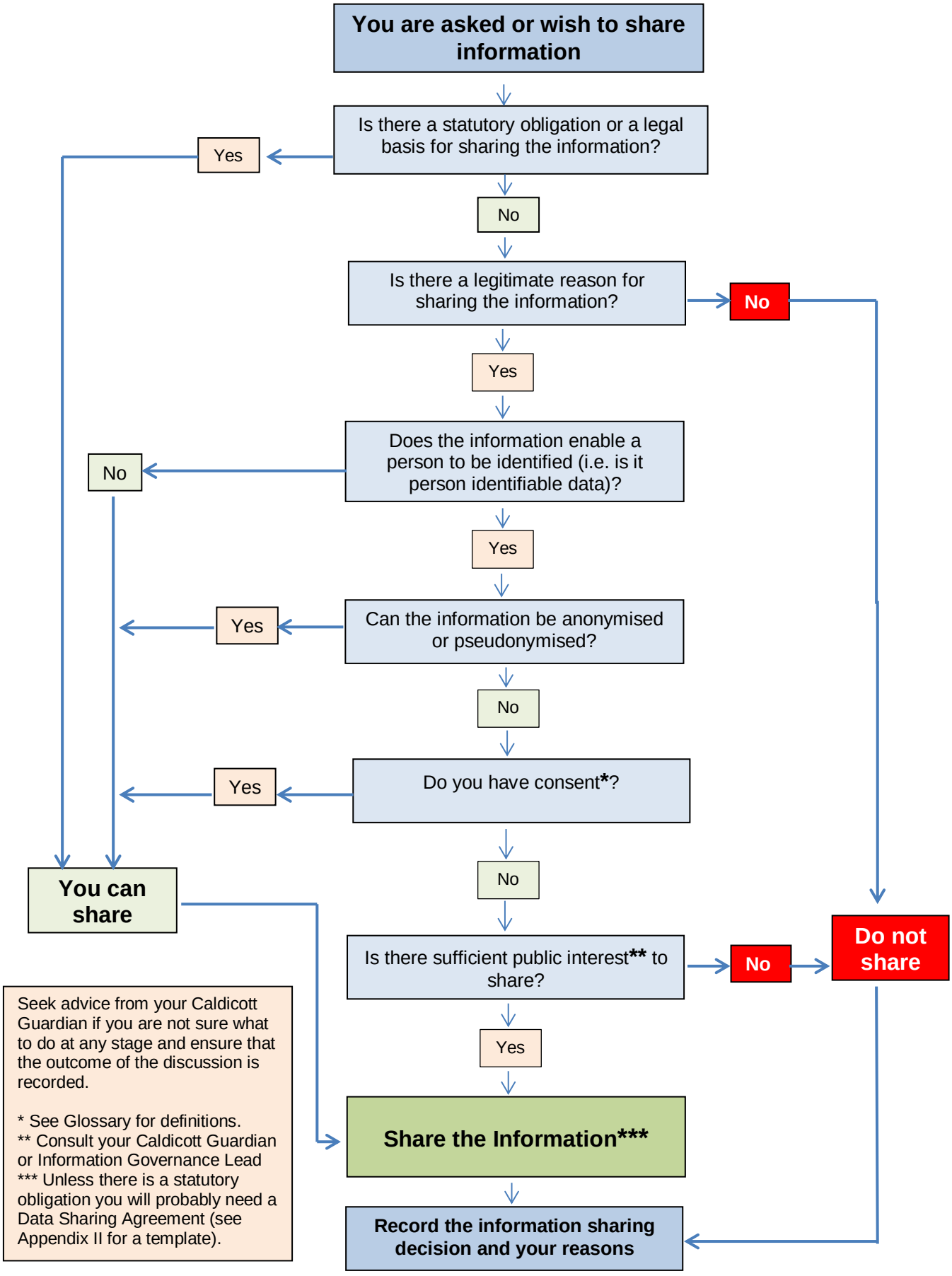
Phone number:

Role:

Signed:

Change Management

Name	Position	Organisation	Version	Comments	Date
Information Governance Team	DPO	DMBC	1.0	Replacement to previous T2 Agreement	24/04/19


You are asked or wish to share information
Is there a statutory obligation or a legal basis for sharing the information?
Yes
No
Is there a legitimate reason for sharing the information?
No
Yes
Does the information enable a person to be identified (i.e. is it person identifiable data)?
No
Yes
Can the information be anonymised or pseudonymised?
Yes
No
Do you have consent*?
Yes
No
You can share
Is there sufficient public interest** to share?
No
Do not share
Yes
Share the Information***
Record the information sharing decision and your reasons
Seek advice from your Caldicott Guardian if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.
* See Glossary for definitions.
** Consult your Caldicott Guardian or Information Governance Lead
*** Unless there is a statutory obligation you will probably need a Data Sharing Agreement (see Appendix II for a template).