

Doncaster Multi-Agency Information Sharing Agreement



Date Agreement came into force	January 2021
Date of Agreement review	January 2024
Agreement Owner/s	Doncaster Safeguarding Childrens Partnership and Doncaster Safeguarding Adults Board
Version	2.0

This agreement is for frontline staff, practitioners and managers to enable effective decision making when sharing information between agencies.

Every inquiry into a child's death in the UK has found that effective sharing of information within and between agencies is fundamental to improving the protection of children and young people.

The various inquiries all showed that no single service had a full, clear picture about what was going on in the child's life. In all cases, early indications of a threat to wellbeing had been missed, or hadn't been responded to at the earliest opportunity.

This is also true of when dealing with adults at risk. Safeguarding Adult reviews frequently highlight missed opportunities between safeguarding partners (local authorities, GPs and health, the police, housing, care providers) to communicate and work jointly.

**In care settings the reviews of residents care should be holistic and include information sharing from all agencies involved.
Such failures can lead to serious abuse and harm and in some cases, even death.**






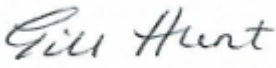

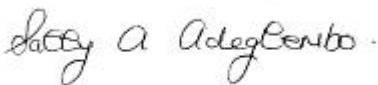

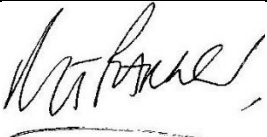
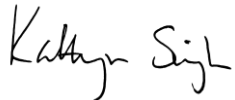
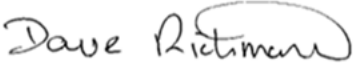
"There can be no justification for failing to share information that will allow action to be taken to protect children"

Government Letter issued to all Local Authorities March 2015

"Poor information sharing between multi-agency partnerships¹ has been identified as a compounding factor that can lead to the serious harm, abuse or death of a child.² This has been well documented through Serious Case Reviews and national policy, which state that there is a clear need for effective multi-agency working and information sharing in order to secure improved safeguarding outcomes."

Information sharing to protect vulnerable children and families, Department for Health, July 2016

The signatories below have agreed that their agency will work within the guidelines set out in this Information Sharing Agreement; the most senior officer should sign this agreement.

Name	Organisation/Agency	Signature	Date
John Goldup	DSCP and DSAB Independent Chair		17.03.2021
Damian Allen	Doncaster Metropolitan Borough Council		11.02.2021
Jackie Pederson	Doncaster Clinical Commissioning Group		15.02.2021
Simon Wanless	South Yorkshire Police		18.03.2021
James Thomas	Chief Executive, Doncaster Childrens Services Trust		12.02.2021
Gill Hunt	NHS England		01/03/2021
Dawn Peet	South Yorkshire Fire and Rescue	D S Peet	15.2.2021
Kirsty Knivett	Doncaster College and University Centre		18.02.21
Sally Adegbembola	South Yorkshire National Probation Service		17/02/21
Luke Shepherd	South Yorkshire Community Rehabilitation		24/02/21
Richard Parker	Doncaster and Bassetlaw Teaching Hospital Foundation Trust		11/02/2021
Kathryn Singh	Rotherham Doncaster and South Humber NHS Foundation Trust		10/03/2021
Dave Richmond	St Leger Homes		11/02/2021

Introduction and Scope

Information sharing can be complex and sometimes confusing for practitioners, however practitioners sharing information should be able to do this with confidence and with the best intentions of safeguarding children and adults at risk.

Appropriate and timely sharing of relevant information is a vital part of any early intervention approach that is adopted by organisations that work with children and adults at risk within Doncaster.

Sharing appropriate information at the right time improves outcomes for all and can help prevent situations escalating into tragedies.

Practitioners should not wait until a situation has reached crisis point before sharing information. They should also share when there are smaller changes. This allows patterns to emerge – and these can often point to more serious concerns, allowing appropriate help to be offered at an early stage.

No professional should assume that someone else will pass on information which they think may be critical to keeping a child or adult at risk safe. If a professional has concerns then they should share the information with the Multi-Agency Safeguarding Hub or contact the Adults Contact Team. Please note that the Multi-Agency Safeguarding Hub has separate information sharing document specific to the service. However it reflects principles of this document.

Please refer to the appendix for contact details.

This protocol has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information between themselves and with the Doncaster Safeguarding Children Partnership and Adults Board (DSCP and DSAB);
- Set out the legal gateway through which the information is shared, including reference to the Human Rights Act 1998 and the common law duty of confidentiality;
- To support the Making Safeguarding Personal agenda within Adult Safeguarding
- Describe the security procedures necessary to ensure compliance with responsibilities under the Data Protection Act 2018 and agency specific security requirements;
- Describe how this arrangement will be monitored and reviewed.
- Ensure compliance with Working Together to Safeguard Children 2018 and the Care Act 2014

Why information sharing is important

Sharing information as part of early intervention and preventative services

- There is an increasing emphasis on integrated working across services with the aim of delivering more effective intervention at an earlier stage. Early intervention aims to prevent problems escalating and increase the chances of achieving positive outcomes. In some areas there is increased use of multi-agency services, for example: in Children's Centres to support children's health and development; through EPIC (Encouraging Potential Inspiring Change) to help young people move away from involvement in crime and anti-social behaviour; and through use of the Safeguarding Adults Hub (SAH) in adult services and the Early Help Assessment (EHA) in children's services, both intended to promote a more coordinated and person-centred approach to the provision of care.
- Whether integrated working is through specific multi-agency structures or existing services, success for those at risk of poor outcomes depends upon effective partnership working and appropriate information sharing between services.
- Sharing information about individuals between public authorities is often essential if adults at risk are to be kept safe or to ensure they receive appropriate services. The sharing of information must only happen when it is **legal** and **necessary** to do so and **adequate safeguards** are in place to protect the security of the information. Furthermore, where a death of an adult at risk has occurred due consideration should be taken in respecting the dignity of an individual and their family.
- Sharing information at an early stage helps to identify trends and patterns of concern for vulnerable children or adults at risk. For example children at risk of CSE or quality within care home settings.

If in any doubt please refer to your

- LADO (Local Authority Designated Officer)
- Safeguarding Adult Manager or Designated Safeguarding Adults Professional Lead

Sharing Information between the Multi-Agency Safeguarding Hub and South Yorkshire (SY) Police

- In addition to the above SY Police and DCST Multi-Agency Safeguarding Hub acknowledge there is a duty to share information in relation to cases that may be initially screened as high risk cases, and/or where there are potential Child Protection issues. Joint screening of certain Police Vulnerable Person's Assessments also takes place to ensure that the Police and the Multi-Agency Safeguarding Hub share information in cases where there is an initially identified lower tariff of risk, and where the welfare of the child is of concern.
- This process ensures that the welfare needs of the child are being prioritised, and key agencies share relevant information about the child and carers.

Sharing information between adult and children's services

- Staff in adults' services are aware that problems faced by clients who have parenting responsibilities are often likely to affect children and other family members. However, this information is not always shared and opportunities to put preventative support in place for the children and family are missed. Where an adult receiving services is a parent or carer, sharing information where appropriate with colleagues in children's services could ensure that any additional support required for their children can be provided early.

Sharing information to support transitions

- There are many transition points in the life of an individual. Transitions include a child moving from nursery into primary school; from primary to secondary school; and moving into adulthood. Significant transitions can also occur when an individual leaves long-term care, hospitalisation or prison. In all of these cases, information sharing is important to ensure that the person gets the support that they require, through and after the transition.

Sharing information where there are concerns about significant harm to a child or young person

- It is critical that where you have reasonable cause to believe that a child or young person may be suffering or may be at risk of suffering significant harm, you should always refer your concerns to Children's Social Care or the Police, in line with your Local Safeguarding Children Partnership procedures.
- In some situations there may be a concern that a child or young person may be suffering, or at risk of suffering significant harm, or of causing significant harm to another child or serious harm to an adult. However, you may be unsure whether what has given rise to your concern constitutes 'a reasonable cause to believe'. In these situations, the concern must not be ignored. You should always talk to someone to help you decide what to do – a lead person on safeguarding, a Caldicott guardian, your manager, an experienced and trusted colleague or another practitioner who knows the person. You should protect the identity of the child or young person wherever possible until you have established a reasonable cause for your belief.
- Significant harm to children and young people can arise from a number of circumstances – it is not restricted to cases of deliberate abuse or gross neglect. For example faltering growth (also known as failure to thrive) of an infant for no known reason could indicate the infant is suffering significant harm but equally the child could have an undiagnosed medical condition. If the parents refuse consent for further medical investigation or an assessment, then you are still justified in sharing information. In this case, the information sharing would be to help ensure that the causes of the faltering growth are correctly identified.

Sharing information where there are concerns about serious harm to an adult

- You may be sharing information about an adult as part of your aim to deliver more effective intervention at an earlier stage to prevent problems escalating and to increase the chances of achieving positive outcomes. However there

may also be situations where you may want to share information because you are concerned about serious harm to an adult.

- If you believe the adult you are dealing with is an adult at risk and is unable to make informed decisions then you will need to take this into consideration when making your decision. Where harm, or risk of harm, to an adult at risk is suspected appropriate action should be taken in accordance with your local codes of practice. You should contact the Local Authority Safeguarding Adults Hub for advice and support.

Sharing Information between Safeguarding Adults Hub and South Yorkshire (SY) Police?

- In addition to the above SY Police and the Local Authority Safeguarding Adults Hub acknowledge there is a duty to share information in relation to the suspected or potential adult abuse or neglect in line with the Care Act 2014 and South Yorkshire Principles for Safeguarding Adults. Joint visits between the Safeguarding Adults Hub and the Police also takes place to ensure information is shared and screening is informed in cases where there is concern for the welfare of the adult.

Sharing information where there are concerns about significant harm or serious harm to third parties

- Where you have concerns that the actions of some may place children at risk of significant harm or adults at risk of serious harm, it is possible to justify sharing information with or without consent for the purposes of identifying people for whom preventative interventions are appropriate. Significant harm to children and serious harm to adults is not restricted to cases of extreme physical violence. For example, the cumulative effect of repeated abuse or threatening behaviour may well constitute a risk of serious harm to an adult.

Sharing information where you have a statutory duty or a court order

- Where you have a statutory duty or court order to share information you must do so unless, in the case of a court order, your organisation is prepared to challenge it.

Sharing information in an emergency situation (terrorist-related action, natural disaster and other incidents)

- The nature of emergency situations will vary but information sharing is always a vital part of providing services to the people affected by them. Whilst the principles and legislative basis underpinning the sharing of information are broadly the same in an emergency situation, it is more likely than not that it will be in the interests of the individuals for personal data to be shared.
- Timeliness is a key consideration in emergency situations. It may not be appropriate to seek consent for information sharing if delays could incur as a result. You should always consider how much information needs to be shared to achieve the objective and the most appropriate way in which to do so given the urgency of the situation. Security of information sharing must still be considered but should be proportionate to the sensitivity of the information and the circumstances.

Please refer to **PREVENT** and **WRAP (Workshop to Raise Awareness of Prevent)**

Key messages - Adult safeguarding: sharing information

- Making Safeguarding Personal and the Care Act 2014 reiterates that adults have a right to independence, choice and self-determination including control over information about themselves. In the context of adult safeguarding these rights can be overridden in certain circumstances. (Care Act 2014).
- All staff should know that the duty to share information can be as important as the duty to protect confidentiality.
- When the adult at risk lacks capacity and it is felt that they do not have the ability to make decisions for themselves, the use of an advocate should be promoted.
- Emergency or life-threatening situations will usually warrant the sharing of relevant information with the relevant emergency services without consent.
- The law does not prevent the sharing of sensitive, personal information within organisations. If the information is confidential, but there is a safeguarding concern, sharing it will usually be justified.
- The law does not prevent the sharing of sensitive, personal information between organisations where the public interest served outweighs the public interest served by protecting confidentiality – for example, there is a serious overriding public interest if the information relates to:
 - Serious crime
 - Danger to a person's life
 - Danger to other people
 - Danger to the community
 - Serious threat to others, including staff
 - Serious infringement of the law
- The Data Protection Act 2018 enables the lawful sharing of information.
- There should be a local agreement or protocol in place setting out the processes and principles for sharing information between organisations.
- An individual employee cannot give a personal assurance of confidentiality.
- Frontline staff and volunteers should always report safeguarding concerns in line with their organisation's policy.
- It is good practice to try to gain the person's consent to share information.
- As long as it does not increase risk, practitioners should inform the person if they need to share their information without consent.
- Organisational policies should have clear routes for escalation where a member of staff feels a manager has not responded appropriately to a safeguarding concern.
- All organisations must have a whistleblowing policy.
- The management interests of an organisation should not override the need to share information to safeguard adults at risk of abuse.
- All staff, in all partner agencies, should understand the importance of sharing safeguarding information and the potential risks of not sharing it.
- All staff should understand when to raise a concern and who to raise it with.

- The seven golden rules for information sharing should underpin all safeguarding practice (see appendix).

The Legal Framework

There is a wealth of legal frameworks and government guidance that sets out how information is exchanged. These include:

- The Human Rights Act 1998
- The Data Protection Act 2018
- The Children Act 1989 & 2004
- The Education Act 1996 & 2002
- The Learning and Skills Act 2000
- The Mental Capacity Act 2005 & DoLS (Deprivation of Liberty Safeguards)
- Working Together to Safeguard Children 2018
- The Care Act 2014
- Serious Crimes Act 2015 – S76 Coercion and Controlling Behaviour
- The NHS Act 2006
- Police and Criminal Evidence Act 1984
- CQC—(Health and Social Care Act 2008)

The main legal gateway (or statutory power to share information) for the purposes of this protocol is section 10 of the Children Act (2004) and The Care Act 2014 that places a duty on all Local Safeguarding Children's Partnership member agencies to make (information sharing) arrangements to promote cooperation.

In applying section 10 of the Children Act (2004), all LSCB member agencies and the LSCP must also adhere to the arrangements outlined in the Data Protection Act (2018) and Human Rights Act (1998).

To help agencies determine and decide where information shared, between agencies and with the DSCP and DSAB, fulfils all legal requirements, the flowchart on page 15 should be used to help inform decision making.

In addition to the legal power under section 10 of the Children Act (2004), individual member agencies and their partners also have other responsibilities to share information that satisfies the public interest test outlined in the flowchart on page 15.

The list below is not exhaustive but covers the main DSCP and DSAB member agencies:

- Section 27 of the Children Act (1989) places a duty on a variety of agencies to share information with children's social care; where the information is shared to immediately protect a child suffering significant harm, or is likely to suffer significant harm (under section 47 of the Children Act 1989) then it is likely to meet the public interest test to share without consent;
- Section 82 of the NHS Act (2006) places a duty to co-operate upon NHS bodies and local authorities to secure and advance the health and wellbeing of the population;

- Section 251 of the NHS Act 2006 replaced section 60 of the Health and Social Care Act 2001. It provides powers to the Ethics and Confidentiality Committee of the NIGB to ensure that patient identifiable information needed to support essential NHS activity can be used without the consent of patients.
- Section 17 of the Crime and Disorder Act (1998) sets out the power for a range of agencies to share information for the purposes of preventing crime and disorder;
- MARAC arrangements cover sharing information for multi-agency provision of services for victims of domestic abuse to help reduce their victimisation ;
- The 2008 Entry Regulations duty to allow entry to local Healthwatch. The Legislation in Section 225 of the 2007 Act requires the Secretary of State for Health to make regulations to require certain persons to allow authorised representatives to “enter and view”, and observe the carrying-on of activities on premises owned or controlled by the service provider.
- The Mental Capacity Act (2005) and associated Code of Practice (2007);
- The Care Act 2014 Section 45 requests a person or body to supply information to enable or assist the SAB to exercise its functions. Clauses 5.33; 10.60 and 14.146 specifically refer to information sharing.

Adults at risk have the right to refuse, or withhold consent, for organisations to share information in relation to suspected abuse. Wherever possible the views and wishes of the adult will be respected. However, if it is thought that they are in a situation that will result in the abuse of further adults at risk i.e, in care home settings/ sheltered housing etc., or if they may be abusing another person, the duty of care overrides the individual’s refusal.

The need to protect the individual or the wider public outweighs their rights to confidentiality. Decisions to share information about an adult at risk must be made by the organisation and not that member of staff acting on their own. **This, however, should not cause unnecessary delay in the disclosure process.**

There may be meetings that you attend that will have their own information sharing protocols which stipulate how and when you can share and/or record information relating to that individual. **Please ensure you are guided by the relevant protocol in place.**

Data Sets to be Shared

What types of information will be shared?

- There are several distinct classifications of data covered by the Data Protection Act 2018 detailed below- includes data relating to a living individual who can be positively identified from the data, or from the data and other information which is at the disposal of other individuals or is in the public domain. Personal data includes obvious identifiers such as names, addresses, dates of birth, as well as NHS or National Insurance numbers. Facial photographs and CCTV footage are also regarded as personal data, as are descriptions or photographic records of unique scars, tattoos or other markings.

- Special categories of personal data includes data relating to racial or ethnic origins, religious or philosophical beliefs, political opinions , trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or sexual life or sexual orientation.
- Data relating to criminal convictions and offences.

Information relating to children or adult safeguarding may involve a wide range of both personal data, special categories of personal data and criminal data, in circumstances relating to many types of abuse and neglect (further descriptions can be found within the Children Act (1989) – section 27, for Children and the Care & Support Statutory Guidance – issued under the Care Act 2014 - section 14.17 for adults, and local authorities are advised not to limit their view of what constitutes abuse or neglect, as they can take many forms and the circumstances of the individual case should always be considered):

- Physical abuse
- Domestic violence
- Sexual abuse
- Sexual exploitation
- Psychological abuse
- Financial or material abuse
- Modern slavery
- Discriminatory abuse
- Organisational abuse
- Neglect and acts of omission
- Self-neglect
- Radicalisation

Risks and Mitigation

It is impossible to cover all potential scenarios in this agreement. The guidance is therefore to:

1. Share as much as, but no more than, is necessary.
2. Always document the reasons for sharing personal data and sensitive personal data.
3. Record why it is believed the data shared is relevant and proportionate.

Should any member of staff or volunteer working for a partner organisation feel that the letter and spirit of this agreement is not being honoured, or that barriers to legitimate sharing of information are being raised, this should be communicated to their organisation's representative on the Doncaster Safeguarding Childrens Partnership or Safeguarding Adults Board, who will in turn follow this up with their counterparts and Data Protection leads in the Member organisation.

Safeguarding adult meetings that involve/or are about an adult at risk

In order to safeguard an adult at risk or other vulnerable people, it may be necessary to share confidential information at safeguarding adults meetings. It is the responsibility of the Chair of that meeting to request any relevant information and to secure the agreement of the relevant parties to sharing this information.

The Chair of the safeguarding meeting will ensure that a mechanism is in place to ensure that a confidentiality statement is made at the start of the meeting and all parties understand their responsibilities in respect of confidentiality. Exchange may be verbal or written however data protection principles must still apply with attendees only being present where it is appropriate for them to share the information.

Attendees at safeguarding adults meetings will be asked to sign an attendance list which will confirm their individual compliance with the protocol.

Notes taken at safeguarding meetings will be marked 'CONFIDENTIAL'. Only those people who have been invited to the meeting will receive copies of the notes and they must be filed in the confidential / safeguarding adults section of any case file / electronic record.

In all circumstances consent to use and disclose copies of notes / minutes of meetings must be sought from the chair of the meeting.

Any requests for access to the notes of safeguarding adult meetings must be considered on a case by case basis under the Freedom of Information Act 2000 and / or the Data Protection Act 2018, but information will only be disclosed if it is appropriate to do so. For further advice, contact should be made with the Data Protection officer or Freedom of Information officer from the relevant organisation or contact can be made with the Information Commissioner.

If an organisation wishes to disclose confidential information, permission i.e. consent, must be obtained in writing from the initial owner of the information (unless there is a legal obligation to share). If this may not be appropriate, then prior advice should be sought from above the Data Protection / Freedom of Information officer from the relevant organisation or, contact can be made with the Information Commissioner.

It is recommended that information relating to safeguarding adult issues should be retained on case files / electronic records according to local policy. Information should then be reviewed and if agreed only then securely disposed.

The Seven Golden Rules of information sharing

By following these '7 Golden Rules' of information sharing, practitioners can work with families and other professionals to ensure that the best outcome is made.

1

Remember that the Data Protection Act 2018 are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

2

Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3

Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4

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

5

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

6

Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles). Ask *“how will providing the information help further enquiries and how will failing to provide it hinder them?”*

7

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

Record the time, date and decisions that have been made.

Working Together to Safeguard Children 2018 expressly states that “fears about sharing information **must not be allowed** to stand in the way of the need to promote the welfare and protect the safety of children”

The Care Act Guidance emphasises the need to share information about safeguarding concerns at an early stage. Adult Safeguarding Reviews have highlighted how significant gaps in the sharing of information can lead to poor outcomes for adults at risk.

The Caldicott Principles

The Caldicott principles apply to health and social care organisations' use of personal information; these organisations are required to observe the following principles when using personal information.

The original Caldicott Review was published in 1997. It included six principles governing the sharing of information. A further review was undertaken by Dame Fiona Caldicott in 2013 and included an additional principle to emphasise the need to give greater focus to information sharing. The revised list of Caldicott principles are as follows:

- 1 Justify the purpose(s) for needing the personal confidential information
- 2 Do not use personal confidential information unless it is absolutely necessary
- 3 Use the minimum necessary of personal confidential information
- 4 Access to personal confidential data should be on a strict need- to- know basis
- 5 Everyone with access to personal confidential data should be aware of their responsibilities
- 6 Comply with the law
- 7 The duty to share information can be as important as the duty to protect patient confidentiality

Data Security and Management

It is important that information is shared safely and only shared with the intended recipient. The information should show the originator's details, including organisation name (where applicable) and date.

Email – this is by far the most widely used method to exchange information therefore care should be taken to anonymise any identifying information, e.g. by using initials. The risks in relation to using email is acknowledged, however, its use has been agreed to ensure timely exchange of information to those recipients who are not in possession of a secure encrypted email account or do not have email encryption software.

Where an organisation has access to Government Connect / GCSX (or equivalent), this facility must be used. It is a secure network between central government and every local authority in England and Wales. It is part of the wider Government Secure Intranet (GSI) and provides connectivity to nearly all central government departments as well as the NHS and the police. If you use other secure email methods such as Egress you need to check if the recipient can access the information you send.

Check the intended recipient is the actual person!

The full list of secure Government email systems are below. They have email addresses ending:

- .cjsm.net (Criminal and Justice)
- .gov.uk (Local Government/Social Services)
- .gse.gov.uk (Central Government)
- .gsi.gov.uk (Central Government including Department of Health)
- .gsx.gov.uk (Central Government)
- .hscic.gov.uk (The Health and Social Care Information Centre)
- .mod.uk (Military)
- .nhs.net (NHSmail)
- .pnn.police.uk (Police)
- .scn.gov.uk (Criminal and Justice)

Egress should only be used if you are sure the recipient can access this method, the preference should be to use the above secure email domains.

Other methods

Fax - is only secure if the person who requires the information is waiting by the receiving fax machine to receive the document immediately or the fax machine is located in a secure place. Faxes should only ever be used as last resort.

Scanning - this is usually where you scan a document to your own email or to a location in your data collection system, ensure you enter the correct email address.

Text Messaging - this method of communication is often preferred by people staff work with, however, staff should be aware that no confidential information is shared when texting and that any language used is professional and courteous

Postal or Courier Services - can never be fully secure and are not recommended unless secure email is not possible. If post is to be used, ensure that you use an envelope that will show if it has been tampered with (preferably inside another envelope), and is marked 'Private and confidential addressee only'.

Personal exchange - Paper copies of information can be exchanged in person provided that both the information holder and the recipient take appropriate measures to ensure that it cannot be read by anyone who does not have a legitimate reason to do so. Paper copies should be kept secure at all times.

Verbal Exchange - this is only secure if it is not repeated to anyone who is not authorised to hear it, or overheard when exchanged or discussed e.g. in a busy office or during a conference phone call. If information is exchanged verbally in a manner where it is not recorded at the time, the exchange should be validated and confirmed in writing as soon as possible.

Disposal of Data/information - at the end of its use (for copy information) or agreed retention period information should be securely disposed of in line with internal procedures. Where information has been shared, and the receiving organisation is not the data controller, authority of the originating organisation should be sought before destruction takes place.

Storage - all organisations must ensure that reasonable steps are taken to ensure the security of data – this includes the management of data when in transit between organisations. Each signatory to this agreement is expected to have an information security framework that documents how information will be kept secure. This will be made available on request.

Security Breaches - in addition to compliance with the Golden Rules (see above), once the individual recipient has been verified and validated then the information shall be disclosed securely.

Any concern or allegation of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data will be a personal data breach under the Data Protection Act 2018 and must be reported immediately using the relevant internal reporting channels within the appropriate organisation. Any level 2 breach (as defined in the Information Governance Toolkit Reporting Tool) will be reported to the Healthcare and Social Care Information Centre (HSCIC) and the Information Commissioners Office (ICO).

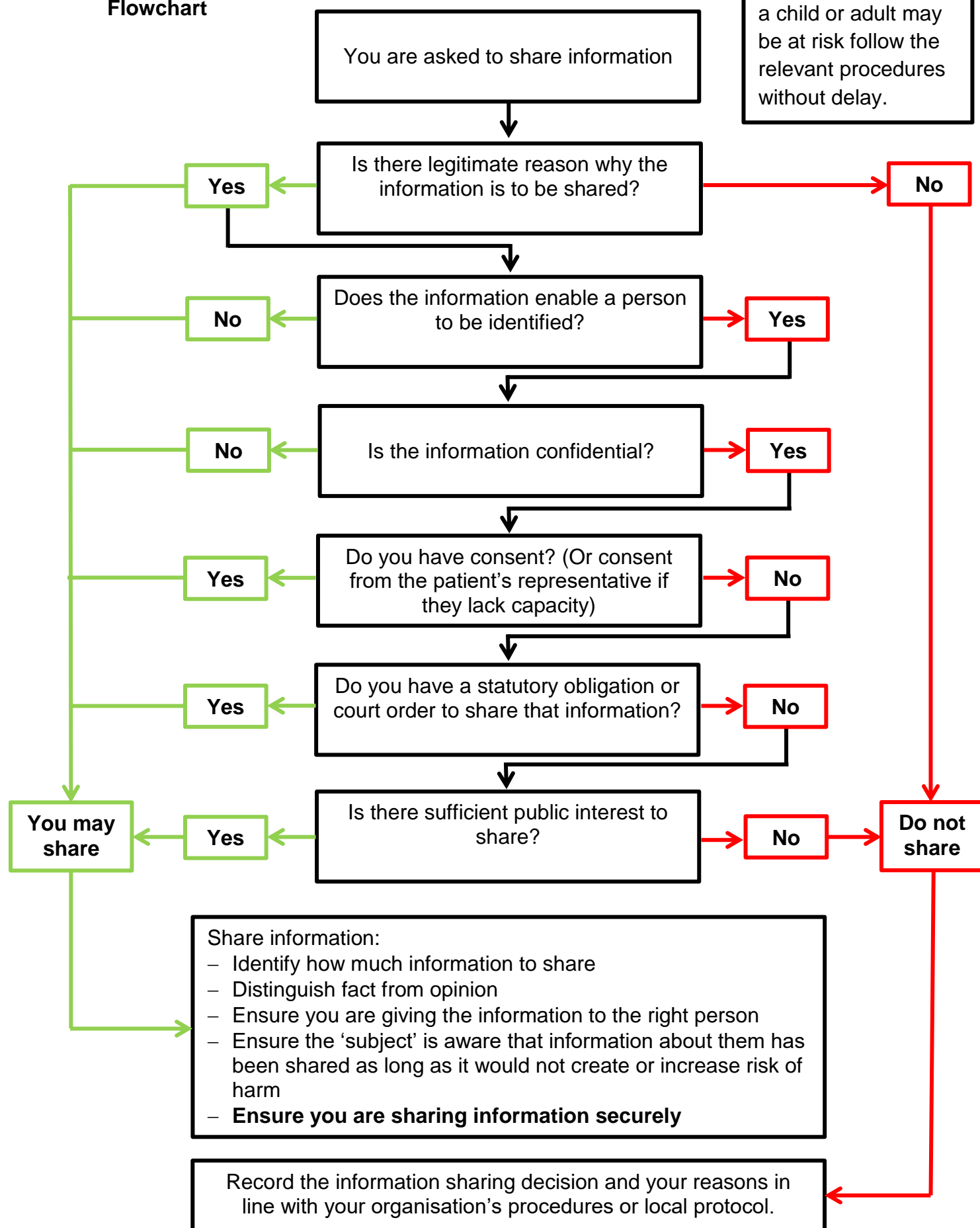
Staff should be aware of their own organisations' policy on using social media such as Facebook/Twitter and any future social media that comes into being. The general line should be that your personal social media account is not used for sharing any account of the work you are engaged in. No identifiable information should be shared.

If your organisation contracts services to other providers then it is essential that contracts ensure compliance with this information sharing agreement.

Flowchart

NOTE:

If there are concerns a child or adult may be at risk follow the relevant procedures without delay.



APPENDIX

The 6 safeguarding principles that underpin safeguarding adults at risk

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215591/dh_126770.pdf

Multi-Agency Safeguarding Hub

This is the 'Front Door' for access to services, support and advice for Children and their Families, from Early Help and Support through to Safeguarding and Child Protection.

Social workers are available to discuss your concerns and agree the next steps to be taken.

Tel: 01302 737777 (Between 8:30am and 5pm, Monday to Friday)

Out of hours Tel: 01302 736000

Email: ChildrenAssessmentService@dcstrust.co.uk

Adult Services Social Care

If you have any concerns about the welfare or safety of an adult you can report it online here:

<https://www.doncaster.gov.uk/doitonline/reporting-a-safeguarding-concern>

For general information, advice and guidance about safeguarding adults call the Safeguarding Adults Hub on: 01302 737063

SMS/Text Number (for people from the deaf community): 0797 903 1116

PREVENT and WRAP

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

Letter issued to Chief Executives of local authorities, Directors of Children's Services, Police and Crime Commissioners, Local Safeguarding Children's Boards, Health and Wellbeing Boards and GPs in relation to information sharing

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/408843/info_sharing_letter5.pdf

Information Governance Toolkit

<https://www.igt.hscic.gov.uk/resources/IG%20Incident%20Reporting%20Tool%20User%20Guide.pdf>