INFORMATION SHARING AGREEMENT

Teeswide Safeguarding Adults Board

Contents

Appendices

Revision Number	Date Approved by the Board	Change Record	Links to Other Policies	Review Date:
5	Sept 2018	Refreshed in line with the introduction of the GDPR.	Inter-Agency Safeguarding Adults Policy and Procedure and Communication and Engagement Strategy	
5.1	Jan 2019	Further amendments after receiving further legal advice regarding GDPR and the Data Protection Act 2018	Inter-Agency Safeguarding Adults Policy and Procedure and Communication and Engagement Strategy	
5.2	Sept 2020	Minor review, only amendment required to update the title of the Think Family Guidance.	Inter-Agency Safeguarding Adults Policy and Procedure and Communication and Engagement Strategy	Mar-21

1. Summary of the Key Points

Information sharing is vital to safeguarding and promoting the welfare of *Adults, and is an intrinsic part of any front line practitioner's job when working with Adults. The decision is how much information to share, with whom and when. Information sharing can have a profound impact on individuals' lives.

* The adult experiencing, or at risk of abuse or neglect will hereafter be referred to as the **Adult** throughout this document.

Fears about information sharing cannot be allowed to stand in the way of the need to safeguard and promote the welfare of Adults. The aim of this section is to give all staff in every partner organisation under the Teeswide Safeguarding Adults Board (Board) umbrella, key points to keep in mind when making information sharing decisions. If you need more information when making your information sharing decision, you should read the rest of this document, speak with your manager and consult the Inter-Agency Safeguarding Adults Policy and Procedure. When making your information sharing decision, you should keep the following points in mind:

1.1 Seven golden rules for information-sharing

- **Remember that the General Data Protection Regulation** (GDPR) **and Data Protection Act 2018 is not a barrier to sharing information** but provides a framework to ensure that personal information about a natural person is shared appropriately.
- **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be, shared, by another lawful reason.
- **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.
- **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is a lawful reason to do so such as where safety may be at risk. You will need to base your judgement on the facts of the case.
- **Consider safety and wellbeing:** base your information-sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions.
- **Necessary, proportionate, relevant, accurate, timely and secure:** ensure that information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in timely fashion, and is shared securely, and in accordance with any organisation policy in handling personal information.
- **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share and then record what you have shared, with whom and for what purpose.

1.2 Some information sharing won't involve personal data or special categories of personal data. If information is:

(a) fully anonymised or is otherwise non-identifiable; or
(b) wholly statistical in nature, then it is not necessary to apply this agreement.

Care must be taken however to establish that information is either anonymised, as the obvious fields of person-identifiable data may not be the only positive identifiers within shared material.

1.3 What is personal data and special categories of personal data?
There are two distinct classifications of data covered by the GDPR and Data Protection Act 2018:

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Information relating to adult safeguarding may involve a wide range of both personal data and special categories of personal data. The GDPR and Data Protection Act 2018 sets out the circumstances in which personal and special categories of personal data can be shared. Understanding these circumstances is key to sound information sharing decisions.

For further guidance on these circumstances, you should consult your organisations' practitioner guidance/information governance lead.

1.4 How do I decide whether to share information?

Consent from individuals to share their personal information
Staff and volunteers need only seek consent from individuals before sharing their personal data and or special categories of personal data if there is *no legal basis for doing so. If required, they should record the consent, when given, on their organisation's standard consent documentation. Where it is not possible to obtain consent this could be because:

- The individual does not have the mental capacity to consent
- It may not be safe to seek consent
- It may not be possible to seek consent for some other reason.

* Also see Making Safeguarding Personal Guidance (page 9).

Sharing personal and special categories of personal information without consent
In cases where it has not been possible to seek or obtain consent it may be possible to share information in one of the ways explained below. Staff or volunteers should **always record the rationale** for sharing the information, and how this decision was arrived at.

- If the individual does not have the mental capacity to consent, staff or volunteers should record this using their agency's Mental Capacity Assessment recording tool
- One of the reasons from Article 6 (1) of the GDPR is required to justify the lawfulness of processing of personal data, whilst a reason from Article 9 (2) is required to share special categories of personal data.

Those reasons with particular relevance to this agreement are included below:

Article 6 (1) – Lawfulness of processing personal data:

- Compliance with the legal obligations of partner organisations
- Protecting the vital interests of the subject or of another natural person
- Carrying out tasks or duties substantially in the wider public interest or in the exercise of official authority vested in the controller
- Pursuing the legitimate interests of the partner organisation.

Article 9 (2) – Justifications for the processing of special categories of personal data:

- Compliance with employment law obligations
- Protecting the vital interests of the subject or of another natural person, only where the person lacks capacity to consent (GDPR Article 9 (2) (c))
- Legal advice and establishing or defending legal rights
- Public functions (including the administration of justice) and where necessary to carry out statutory duties
- Medical purposes and the provision of healthcare
- Necessary for provision of health or social care (only amongst professionals subject to professional confidentiality) (GDPR Article 9 (2) (h) + 9(3) + Data Protection Act 2018 s.11 (1))
- Detection of unlawful activity
- Protection of the public
- Police processing.

Emergency or life-threatening situations may warrant the sharing of relevant information with the relevant emergency services without consent.

As long as it does not increase risk, practitioners should inform the person if they need to share their information without consent.

1.5 What else should I keep in mind?

Once you have decided you can share the data, you should keep the following points in mind:

- Be proportionate with the information that is shared
- Ensure the correct information is given to the correct individual
- Distinguish fact from opinion
- Always document the reasons for sharing personal data and special categories of personal data
- Record why it is believed that the data shared is relevant and proportionate.

1.6 Consider risks to others - 'Think Family'

Consideration must also be given as to whether anyone else is at risk, including children or other adults with care and support needs. Whilst actions may be limited in relation to the individual themselves, there may be a duty to take action to safeguard others. Should there be a concern that a parent may be neglecting children in their care, concerns must be reported to Children's' Social Care. See: Think Family Guidance.

2. Information Sharing Agreement

2.1 Purpose

The purpose of this agreement is to protect Adults from harm by facilitating the sharing of information between the partner organisations described below (section three). The following statement should guide all information sharing with the partners of the Board, as well other organisations who may be asked to share information with the Board:

"Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution, as they are by carelessness".
Christopher Graham, Information Commissioner, May 2011

2.2 Introduction

This agreement is written to provide advice and guidance on the sharing of **personal,** and or **special categories of personal data,** as defined by the GDPR and Data Protection Act 2018 and in the specific context of Adult safeguarding. It sets out the core information sharing principles which have been agreed by its signatory partner organisations. It describes:

(a) the information which will be shared between the partner organisations listed and
(b) the arrangements for assisting compliance with the relevant legislation, including the GDPR, Data Protection Act 2018 and the Care Act 2014.

This agreement may also need to be read in conjunction with higher level data protection, information security and or information sharing policies within individual partner organisations, and the Board's requirement to maintain an annual registration **as a Data Controller** with the Information Commissioners Office (ICO).

The Board recognises the need to provide clear guidance to staff in partner organisations on when and how to share information, in order to both:
(a) establish the truth about allegations of abuse or neglect of Adults, and
(b) prevent abuse or neglect of Adults.

Information sharing agreements do not in themselves make the sharing of personal data and special categories of personal data legal or ethical. The GDPR and Data Protection Act 2018 sets out the context in which information may be used legally, with this agreement and echoes the legislative framework and promoting best practice and co-operation across partner organisations.

The Care Act 2014 set out a clear legal framework for how local authorities and other parts of the safeguarding system should protect Adults at risk of abuse or neglect. Local authorities have safeguarding duties. They must:

- **lead a multi-agency local adult safeguarding system** that seeks to prevent abuse and neglect and stop it quickly when it happens
- **make enquiries, or request others to make them,** when they think an Adult with care and support needs may be at risk of abuse or neglect and they need to find out what action may be needed
- **establish Safeguarding Adults Boards**, including the local authority, NHS and police, which will

develop, share and implement a joint safeguarding strategy
- **carry out Safeguarding Adults Reviews** when someone with care and support needs dies as a result of neglect or abuse and there is a concern that the local authority or its partners could have done more to protect them
- **arrange for an independent advocate** to represent and support a person who is the subject of a safeguarding enquiry or review, if required.

Any relevant person or organisation must provide information to Safeguarding Adults Boards as requested (see below). Local Authorities must **co-operate** with each of its relevant partners in order to protect Adults experiencing or at risk of abuse or neglect.

3. Partner Organisations

Catalyst (Voluntary Sector Development Agency in Stockton-on-Tees)	Middlesbrough Voluntary Development Agency
Cleveland Police	National Probation Service: Cleveland
Cleveland Fire Brigade	North Tees & Hartlepool NHS Foundation Trust
Community Rehabilitation Company: Durham Tees Valley	Redcar & Cleveland Borough Council
Healthwatch Hartlepool	Redcar & Cleveland Voluntary Development Agency
Healthwatch South Tees	South Tees CCG
Healthwatch Stockton-on-Tees	South Tees Hospitals NHS Foundation Trust
Hartlepool Borough Council	Stockton-on-Tees Borough Council
Hartlepool and Stockton on Tees CCG (Clinical Commissioning Group)	Tees, Esk & Wear Valleys NHS Foundation Trust
HMP Prison Service (Holme House & Kirklevington Grange)	Thirteen Housing Group
Middlesbrough Borough Council	

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

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

4. Purpose of the Information Sharing

4.1 What are the aims of data sharing?

- To prevent death or serious harm
- To protect an Adult experiencing, or at risk of abuse or neglect
- To prevent or detect a crime, or support the prosecution of offenders
- To make a referral to a partner organisation for immediate action to protect an Adult
- To help people access the right kind of support to reduce risk and promote wellbeing
- To seek advice about a specific adult safeguarding situation, or to establish grounds for an Adult safeguarding investigation
- To establish the potential need for involvement of partner organisations in adult safeguarding work (investigation, prosecution or protection arrangements)
- To plan or initiate an Adult safeguarding investigation
- To identify low-level concerns and patterns that may reveal people at risk of abuse
- To make a referral to organisations for the purposes of requesting or amending services to persons at risk of abuse or neglect, or those suspected of perpetrating abuse
- To make a referral to the Disclosure and Barring Service (DBS) or to provide information to DBS for the purposes of them coming to a barring decision
- To notify the Care Quality and or Charity Commission(s) who may need to take action relating to alleged malpractice

- To notify employers who may need to take action against perpetrators who are thought to pose a risk in respect of the nature of their work
- To notify service providers of a risk posed by a service user
- To inform the development and review of multi-agency policies and strategies for protecting Adults at risk of abuse
- To conduct Safeguarding Adult Reviews (SAR's)
- To deal with complaints, grievances and professional and administrative malpractice.
- To monitor and review Adult safeguarding referrals and the impact of Adult safeguarding policies and procedures, including both the equalities (race, ethnicity, gender, sexuality, age, disadvantage and disability) impact of the policies and the outcomes for individuals. This may include both quantitative and qualitative information, personal data and sensitive personal data, the personal views of individual and expressions of relevant professional opinion.

4.2 What types of information can be shared?
This agreement has been formulated to facilitate the exchange of information between the partner organisations. This includes systematic, routine information sharing and information sharing in response to unexpected or emergency situations. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of the agreement.

The balance, between an individual's rights and the need to disclose information, must be assessed to ensure the information shared between agencies is proportionate to the purpose. Anyone in doubt should consult their information sharing lead before proceeding.

Information relating to Adult safeguarding may involve a wide range of both personal data and special categories of personal data (see explanation above) in circumstances relating to many types of abuse and neglect (further descriptions can be found within the Care & Support Statutory Guidance issued under the Care Act 2014 (section 14.17). 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.

4.3 Who requires access to the personal data or special categories of personal data?
The partners will ensure that 'need to know' principles are observed when its staff and volunteers are deciding who information can be shared with. Partners will advise their staff and volunteers to consider:

- Is it necessary for the requestor to know the information and
- If so, how much information is relevant to the request to share information
- What amount of information is proportionate to share in order to fulfil the safeguarding outcome?

Key roles of individuals within the safeguarding process will govern whether they need to know the information about alleged victims, alleged perpetrators, witnesses and other information pertaining to incidents. Staff within partner organisations should only have access to data if they need it. At all times it is essential to be certain of the reasons why an individual or a meeting needs access to the information.

4.4 How should the decision to share data be recorded?
The rationale for sharing the information should always be documented on the Data Sharing Decision and Update Form (Appendix B). The decision should record why it's believed that information sharing is relevant and proportionate, and whether the data sharing is ongoing, or has taken place in response to particular events.

4.5 How should data be shared?
Where a decision to share data has been made that data must be shared securely between partner organisations. Partner organisations have agreed the following common rules for establishing data security.

The operational aspects of data sharing will be dealt with in accordance with the partner organisation's own data sharing policies. Partner organisations will:

- Ensure appropriate monitoring and audit procedures are in place
- Ensure good quality access control systems in its premises
- Ensure technical security is appropriate to the data processing activities
- Ensure that the encryption of personal data is implemented and managed

- Ensure that common security risks have been identified and a plan is in place for mitigating against them
- Ensure that you set privileges to information based on people's need to know
- Ensure effective measures are in place for the security of information in transit
- Ensure level of sensitivity is understood through commonly understood protective marking
- Ensuring ownership of information is understood by labelling information with the name of its originator, so that obligations around withdrawal of consent, updating to maintain accurate records and reporting any breaches etc can be fulfilled.

In the event that a recipient receives information by an unsecured route, it is incumbent on the recipient to advise the sender and agree a secure route for future transfers of information.

In all transfer scenarios, the onus is on the **SENDER** to ensure that:

- Information is transferred securely
- The chosen method is acceptable to and workable by the recipient
- Information has reached the required recipient.

4.6 Empowering Communities and Neighbourhood Management System (ECINS)
Some partner organisations across Tees are now using ECINS, which is a cloud based information hub and sharing system, which allows practitioners to task each other, speeding up the way in which support is offered to Adults. The use of this system and the general principles for making an information sharing decision would be identical to any other, and covered by the guidance set out in this agreement.

4.7 What is the legal basis for sharing information?
The legal basis for sharing information to safeguard Adults at risk, or to cooperate with other individuals or organisations that are working to protect Adults at risk, is a Local Authority duty under sections (6), (7) (9) (42) & (45) of the Care Act 2014.

Furthermore, the principles guiding the sharing of information to safeguard Adults at risk are described in more detail within the key information for staff above/each partner organisation's information sharing policies/the Inter Agency Safeguarding Adults Policy and Procedure.

Legal basis:
Article 6 (c) GDPR: "processing is necessary for compliance with a legal obligation to which the controller is subject";
Article 6 (d) GDPR: "processing is necessary in order to protect the vital interests of the data subject or of another natural person;
Article 6 (e) GDPR: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller";
Article 6 (f) GDPR: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

Under Part 1 of the Care Act 2014, Local Authorities have a statutory duty to:

- cooperate with other persons in the exercise of functions relating to adults with needs for care and support, and to carers (Sections 6 & 7)
- notify receiving Local Authority when an adult receiving care and support moves (Section 37)
- comply with request for information by Safeguarding Adults Board (SAB) to enable or assist the SAB to exercise its functions. This could include information about individuals (Section 45 – see below)
- involvement of independent advocate in assessments, plans etc. (Section 67)
- Involvement of independent advocate in safeguarding (Section 68).

It is necessary for Adult Social Care departments of Local Authorities to share the personal information outlined within this agreement in order that the Authority to fulfil its statutory duties under the Care Act 2014. Statutory guidance is available on all parts of this Act.

4.8 Reluctance to share information (applying Section 45):
In the event that an organisation declines to share information considered necessary to enable the Board to exercise its functions, consideration should be given to whether the concern warrants the Board exercising Section 45 of the Care Act.

The prescribed conditions for making a request under s45 are:

1. the request is made for the purpose of enabling or assisting the SAB to exercise its functions; and
2. request is made to a person whose functions or activities the SAB considers to be such that the person is likely to have information relevant to the exercise of a function by the SAB.
3. is that the information relates to —

(a) the person to whom the request is made,
(b) a function or activity of that person, or
(c) a person in respect of whom that person exercises a function or engages in an activity, or

4. the information —

(a) is information requested by the SAB from a person to whom information was supplied in compliance with another request under this section, and
(b) is the same as, or is derived from, information so supplied.
(c) information may be used by the SAB, or other person to whom it is supplied under subsection (1), only for the purpose of enabling or assisting the SAB to exercise its functions.

A 'Supply of Information' request made by the Board, under Section 45 of the Act, must be complied with by the recipient organisation, unless it would be 'incompatible with their own duties or have an adverse effect on the exercise of their functions'.

Such supply of information requests may concern, but are not necessarily limited to, Safeguarding Adults Reviews and the undertaking of safeguarding enquiries. Requests for the Board to exercise Section 45 must be made in writing to the Chair of the Safeguarding Adults Board by the partner organisation's Board member, detailing how the relevant criteria is met.

Wherever practicable, the Chair of the Board will seek the views of statutory members of the Board, before reaching a decision as to whether to exercise Section 45. This may not always be possible for example, where such a delay would place an individual at further risk.

4.9 Freedom of Information Requests (FOI)
All signatories to this agreement are Public Authorities and therefore subject to the Freedom of Information Act 2000.

The Freedom of Information Act 2000 grants a right of access to any information held by Public Authorities, unless there are valid legal reasons why this information should not be disclosed. It is intended to promote a culture of openness and to facilitate a better public understanding of how public authorities carry out their duties, the reasoning behind their decisions, and how public money is spent.

The Freedom of Information Act 2000 does not interfere with the Public Authority's obligation to protect personal or confidential data, nor does it inhibit an individual's right to access their own personal information, as prescribed under the General Data Protection Regulation.

Public Authorities have an obligation under the Freedom of Information and Data Protection Acts to consider requests from any person or organisation for access to any information that they hold. This may include safeguarding adult information, including the minutes of meetings and information shared by any other party in connection with safeguarding adult investigations.

Public Authorities will not release information if any of the exemptions defined in the Freedom of Information Act 2000 or General Data Protection Regulation apply. The exemptions include personal information, information supplied in confidence, information for which a claim to legal professional privilege can be maintained, and information where disclosure would prejudice the effective conduct of social work.

There may be circumstances where information relating to safeguarding adult investigations is released, but only where it is appropriate to do so. A situation where information may be released would be where a case has been concluded with no concerns regarding the safety of those involved, and where permission

has been received from all relevant parties for the disclosure of the information. However, advice should always be sought from Legal, Data Protection, Information Governance and a Caldicott Guardian as appropriate.

The Board proactively publishes the minutes of their meetings, and under the statutory duty, an Annual Report which provides a detailed account of the work of the Board and the partner agencies. This report outlines all of the relevant data and Teeswide information in relation to safeguarding adult work.

4.10 Compliance with the Human Rights Act
The partner organisations understand that any informational shared and the processes used to share such information must be compliant with the relevant Human Rights legislation. The Information Commissioner's view on sharing information and data is that provided the sharing complies with the GDPR and Data Protection Act 2018, it is "also likely" to comply with the Human Rights Act 1998/ECHR – Information Commissioner's Code of Practice on Information Sharing.

5. Information Governance and Retention

The GDPR requires that personal data and special categories of personal data is not retained for longer than necessary. Partner organisations may have their own organisational, legal or procedural requirements for records retention and disposal. These retention schedules should be observed and applied at all times. Where no such organisational procedure exists, it is essential to keep pertinent information as long as there continues to be a need for protection arrangements, to ensure that protection arrangements are not compromised and equally that such information is securely disposed of when no longer required.

Where information is to be shared via granting inter-organisational access to systems operated by partner organisations, the 'owning' organisation of the system will draft and agree an Access Agreement with the partner organisation to govern the activities of partner staff using the system.

6. Review

This Information Sharing Agreement will be reviewed six months after its launch and six thereafter. The person responsible for initiating this process is: **Lorraine Garbutt** (Business Manager). If a significant change takes place which means that the agreement becomes an unreliable reference point, then the agreement will be updated as needed and a new version circulated to replace the old. If the lead person departs their role, an alternative lead must be nominated as soon as possible.

7. Discipline

Although this agreement seeks to promote the sharing of information between partner organisations, use of the information shared should never exceed the purposes or intentions of the original reason for sharing. Where allegations are made that information has been used inappropriately, or that the confidentiality of subjects has been breached, partner organisations will co-operate in a full and frank enquiry of these allegations.

In the event that any wilful misconduct is substantiated which resulted in a breach of subject confidentiality, this will be regarded as an act of serious or gross misconduct and acted upon accordingly.

8. Sources of Further Information

Outlined below are the pieces of legislation/Policy which link to this decision making process:

- Common law duty of confidentiality
- General Data Protection Regulation & Data Protection Act 2018 & Human Rights Act 1998 & Freedom of Information Act 2000
- Crime and Disorder Act 1998- Section 17 of the Crime and Disorder Act 1998 (as amended by the Police and Justice Act 2006 and the Policing and Crime Act 2009)
- The 2008 Entry Regulations duty to allow entry to local Healthwatch
- MCA Deprivation of Liberty Safeguards (DoLS) 2007
- Inter- Agency Safeguarding Adults Policy
- Making Safeguarding Personal: TSAB Guidance
- Safeguarding and Promoting the Welfare of Adults and Children at Risk Guidance

Appendices

A. Template 'information sharing request' form

Name of the organisation requesting information:	
Name and position of the person requesting the information:	
What are the specific details of the information being requested:	
What is the intended use or the purpose of requesting the information?	
Is this personal data?	
Is this a special category of personal data?	
Reference to the TSAB Information Sharing Agreement:	
Date information is required:	
Any specific arrangements ref: retention/deletion of information:	
Signed:	
Dated:	

B. Template 'information sharing decision and update' form

Name of organisation holding information:		
Name and position of person making the information sharing decision:		
Date information was requested:		
What is the intended use or the purpose of the requested information?		
Methodology:	Yes	No
Do all of the individuals the information refers to give informed consent to share this information?		
Do all of the individuals the information refers to have mental capacity to make the relevant decision(s)?		
If you do not have informed consent and you intend to share personal and or special personal categories of data. What is the legal basis under Article 6/9 of the General Data Protection Regulation? If		
Decision on information sharing request		
Date of disclosure (if any):		
Any specific arrangements ref: retention/deletion of information:		
Signed:		
Dated:		