Norfolk Safeguarding Adults Board

Information Sharing in Safeguarding Adults

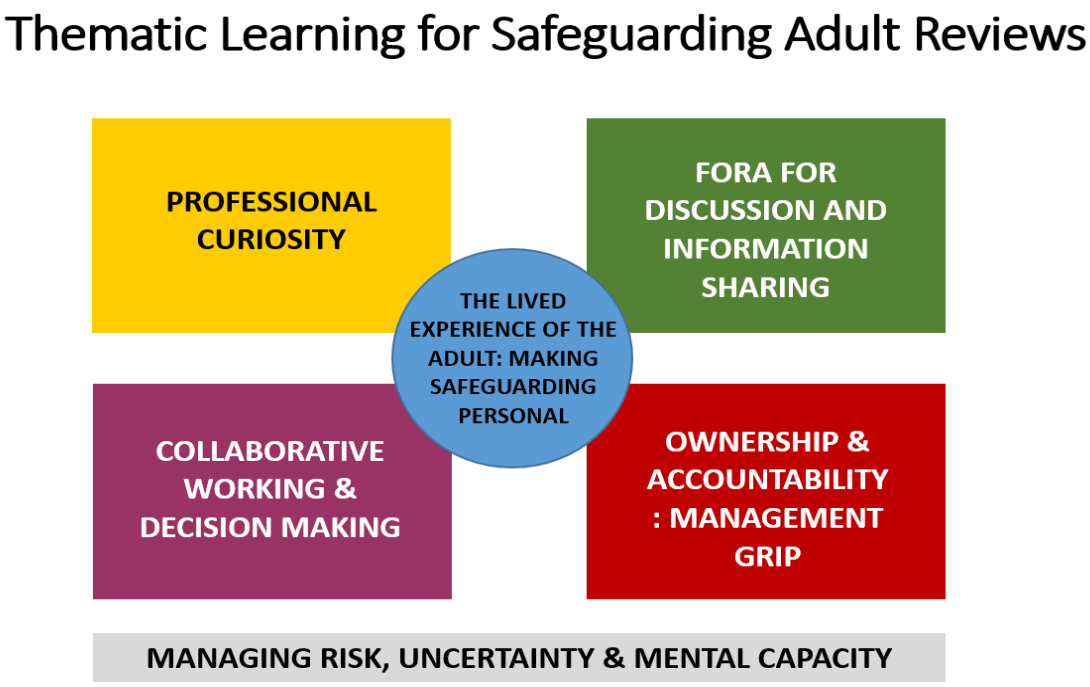
FINAL
April 2023

Issue Number	02
Document Owner	Norfolk Safeguarding Adults Board
Date Approved	April 2023
Date Published on NSAB website	April 2023
Review Date	April 2025 or sooner if required

1. Introduction

Information sharing is a common theme in many Safeguarding Adult Reviews (SARs), Serious Case Reviews (SCRs – children) and Domestic Homicide Reviews (DHRs). Usually information has not been shared between agencies, or there has been delay in getting hold of information, leading to inaccurate responses and preventable harm occurring to children or adults at risk.

In Norfolk we take a thematic approach to our learning from reviews:



Data protection law is intended to keep personal information as safe as possible, especially in an increasingly digital world. But this can be interpreted as a barrier to sharing what we hold with others.

There is an increasing need for professionals to maintain good **legal literacy** (knowledge and understanding) around consent, what can and can't be shared, and in what circumstances. For safeguarding purposes this is essential.

Adults have a general 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.

This guidance looks to support all agencies in Norfolk to understand their roles and responsibilities and to co-operate with one another to share information for safeguarding purposes, in accordance with the statutory frameworks.

2. Why do we need to share information relating to safeguarding adults?

The Care Act 2014 emphasises the need to empower people, to balance choice and control for individuals against preventing harm and reducing risk, and to respond proportionately to safeguarding concerns.

Sharing sensitive or personal information between organisations, as part of day-to-day safeguarding practice and prevention, is not covered in the Care Act because it is already covered in a range of other laws and duties, some of which are below.

The Care Act statutory guidance does reinforce the need to share information about safeguarding concerns at an early stage, and that information sharing agreements or protocols should be in place in all partner organisations.

The guidance also reminds us that those sharing information about individuals alleged to have caused harm are responsible for ensuring that they are compliant with human rights, data protection and confidentiality requirements.

Organisations need to share safeguarding information with the right people at the right time.

This may be within the organisation itself or outside of it. The local authority works with its safeguarding partners (e.g. the police, GPs and health providers, services providers, local councils, CQC) to prevent harm or abuse, or to act where harm or abuse has occurred – information sharing is key to this.

The main reasons personal confidential information may be shared in the context of safeguarding are to:

- prevent death or serious harm
- coordinate effective and efficient responses
- enable early interventions to prevent the escalation of risk
- prevent abuse and harm that may increase the need for care and support
- maintain and improve good practice in safeguarding adults
- reveal patterns of abuse that were previously undetected, and that could identify others at risk of abuse
- identify low-level concerns that may reveal people at risk of abuse
- help people to access the right kind of support to reduce risk and promote wellbeing

- help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour
- reduce organisational risk and protect reputation

3. What does the law say?

The Data Protection Act 2018 incorporating **General Data Protection Regulation** (GDPR) allows that, if it is deemed to be in the public interest, data may be collected, processed, shared and stored. It may be stored for longer periods in the public interest and in order to safeguard the rights and freedoms of individuals.

The principles of GDPR are that data be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 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 the personal data are processed
- Processed in a manner that ensures appropriate security of the personal data

Article 8 of the European Convention on Human Rights (enshrined in UK law by the Human Rights Act 1988) sets out the right to respect for private and family life, your home and correspondence. It concerns the individual's need to live and develop in a social environment and to maintain relationships with others.

However, as this is a qualified right, a public authority can sometimes interfere with the right to respect for private and family life if it's in the interest of the wider community or to protect other people's rights and freedoms.

Article 8(2): "There shall be no interference by a public authority with the exercise of this right except such as 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 freedoms of others."

The Crime & Disorder Act – any person may disclose information to a relevant authority under Section 115 of the **Crime and Disorder Act 1998**, 'where disclosure is necessary or expedient for the purposes of the Act (reduction and prevention of crime and disorder)'. 'Relevant authorities', broadly, are the police, local authorities, health authorities (clinical commissioning groups) and local probation boards.

The **Mental Capacity Act 2005** – where there is a concern that the decision to consent to sharing information is affected by a cognitive impairment, the principles of the Mental Capacity Act should be applied:

- presume capacity, a condition or disability does not automatically impact on decision making
- make every effort to ensure the person is supported to make the decision, think about the information they need, the way that information is presented or talked through for example
- remember that adults have the right to make decisions that may be seen by others as unwise
- if making a decision on behalf of an adult assessed as lacking capacity, *their* best interests must be considered
- any decision made must be the least restrictive option, with as little impact as possible on the person's rights and freedoms.

4. Confidentiality

Confidentiality is an important principle that enables people to feel safe in sharing their concerns and to ask for help. However, the right to confidentiality is not absolute. It is a common law duty. Sharing relevant information with the right people at the right time is vital to good safeguarding practice.

Staff and volunteers can also contact either the police or the local authority safeguarding lead for advice, without necessarily giving an individual's personal details, if they are unsure whether a safeguarding referral would be appropriate.

The **common law duty of confidentiality** is enshrined in the **Caldicott principles**, which apply to the sharing of information in health and social care (very similar to the GDPR ones):

1. justify the purpose(s)
2. don't use personal confidential data unless absolutely necessary
3. use the minimum necessary personal confidential data
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

5. Complex networks between safeguarding partner agencies

The local authority, Norfolk County Council, has the lead responsibility for safeguarding adults with care and support needs. The police and the NHS also have clear safeguarding duties under the Care Act 2014. The NHS Norfolk & Waveney Integrated Care Board and Norfolk Constabulary have different geographical boundaries and different IT systems. Housing and social care service providers also provide services across boundaries. This makes sharing information complex in practice.

The Care Act 2014 (Section 6) places duties on the local authority and its partners to cooperate where relevant in care and support activities, including safeguarding adults.

The Care Act Statutory Guidance states "Partners should ensure that they have the mechanisms in place that enable early identification and assessment of risk through timely information sharing and targeted multi-agency intervention." (14.67)

Norfolk has a Multi-Agency Safeguarding Hub (MASH) in which key safeguarding agencies are co-located (some virtually) to support real-time information sharing, communication and decision-making. Consent to share remains key, and also any onward sharing is considered and agreed between parties, and in the legal context.

The benefits of this model include having a safe 'bubble' in which agencies can share information with confidence it remains secure at that stage, to enable prompt, proportionate intervention and prevention; better understanding and also constructive challenge between key agencies.

From the perspective of NSAB - if there is continued reluctance from one partner to share information on a safeguarding concern the matter should be referred to the board. It can then consider whether the concern calls for a request, under Section 45 of the Care Act, for the 'supply of information.' Then the reluctant party would only have grounds for refusal if it would be 'incompatible with their own duties or have an adverse effect on the exercise of their functions.'

6. Consent to share

Best practice is to be open and honest with the people we support from the outset. Many people believe that organisations, especially large ones like the police, councils and health care agencies, already share information much more than actually happens in practice. By being as clear as possible from the beginning about the information that we hold, and the circumstances in which we may have to share (e.g. safeguarding issues), individuals are more likely to consent to this, or at least to understand why the sharing takes place.

If you have shared information with consent, be sure the person knows what you have shared, with who and why.

7. Where someone refuses consent to share information

There may be times when, even after talking through the relevant concerns, the benefits of sharing information, the additional support available, and exploring anything they may be worried about, the person continues to refuse to give consent.

Where that person has no impairment to their mental capacity, and none of the reasons for sharing without consent apply (see below), the issues and concerns should still be explored with them. Alternative options may be possible, and they should be supported to weigh up the risks and positives of those, as well as their current position.

Consider if they need additional support e.g. an advocate. Work with them to establish a shared understanding of the risk being taken, record this along with their reasons for refusing consent to share to take action. If the risk continues, maintain regular contact and review the decisions made – particularly where mental capacity may fluctuate or there are other factors. Continue to follow the principles of empowerment, prevention and Making Safeguarding Personal.

8. Sharing without consent in safeguarding

If a person refuses intervention to support them with a safeguarding concern, or requests that information about them is not shared with other safeguarding partners, their wishes should be respected. However, there are a number of circumstances where the practitioner can reasonably override such a decision, including where:

- the person lacks the mental capacity to make that decision – this must be properly explored and recorded in line with the Mental Capacity Act.
- other people are, or may be, at risk, including children
- sharing the information could prevent a crime
- the person thought to be the cause of risk has care and support needs and may also be at risk
- a serious crime has been committed
- staff are implicated
- the adult has the mental capacity to make that decision, but they may be under duress or being coerced
- the risk is unreasonably high and needs a multi-agency discussion
- a court order or other legal authority has requested the information

If the person cannot be persuaded to give their consent then, unless it is considered dangerous to do so, it should be explained to them that the information will be

shared without consent. The reasons should be given and recorded. The safeguarding principle of proportionality should underpin decisions about sharing information without consent, and decisions should be on a case-by-case basis.

If it is not clear that information should be shared outside the organisation, a conversation can be had with safeguarding partners in the police or local authority without disclosing the identity of the person in the first instance. They can then advise on whether full disclosure is necessary without the consent of the person concerned.

From the statutory guidance: "If the adult has the mental capacity to make informed decisions about their safety and they do not want any action to be taken, this does not preclude the sharing of information with relevant professional colleagues. This is to enable professionals to assess the risk of harm and to be confident that the adult is not being unduly influenced, coerced or intimidated and is aware of all the options. This will also enable professionals to check the safety and validity of decisions made. It is good practice to inform the adult that this action is being taken unless doing so would increase the risk of harm." (14.92)

It is very important that the **risk of sharing information** is also considered. In some cases, such as domestic violence or hate crime, it is possible that sharing information could increase the risk to the individual. Safeguarding partners need to work together to provide advice, support and protection to the individual in order to minimise the possibility of making things worse, or triggering retribution from the abuser.

9. Where might a safeguarding partner agency refuse to share information?

There are only a limited number of circumstances where it would be acceptable not to share information pertinent to safeguarding with relevant safeguarding partners. These would be where the person involved has the mental capacity to make the decision and does not want their information shared **and**:

- nobody else is at risk
- no serious crime has been or may be committed
- the alleged abuser has no care and support needs
- no staff are implicated
- no coercion or duress is suspected
- the public interest served by disclosure does not outweigh the public interest served by protecting confidentiality
- the risk is not high enough to warrant a multi-agency risk assessment conference referral
- no other legal authority has requested the information.

10. Sharing information on those who may pose a risk to others

The police can keep records on any person known to be a target or perpetrator of abuse and share such information with safeguarding partners for the purposes of protection under Section 115 of the Crime and Disorder Act 1998, 'provided that criteria outlined in the legislation are met'. All police forces now have information technology systems in place to help identify repeat and vulnerable victims of antisocial behaviour.

The Care Act Statutory Guidance tells us that "safeguarding adults boards need to establish and agree a framework and process for how allegations against people working with adults with care and support needs (for example, those in positions of trust) should be notified and responded to." (14.121) The control of information in respect of individual cases must be in line with accepted data protection and confidentiality requirements.

In Norfolk, there is the Safeguarding Adults Data Sharing (SADS) process, led by Norfolk County Council Safeguarding Adults, which is similar to the statutory Local Authority Designated Officer (LADO) role for Children's Services. This considers situations where a safeguarding adult concern has been identified around someone who works with adults at risk, to decide if information about the allegation should be shared with their employer. As there is no standalone statutory basis for this (unlike the LADO), the decision is made in conjunction with other partners to determine the legal basis on which the information should or could be shared.

Bottom line: If you have a clear concern that an adult with care and support needs is being abused or neglected, share the information.

Acknowledgement: this guidance has used adapted material from the Social Care Institute for Excellence (SCIE) Safeguarding adults: sharing information | SCIE

END

03 April 2023