BATH & NORTH EAST SOMERSET SAFEGUARDING ADULTS BOARD

MULTI-AGENCY INFORMATION SHARING PROTOCOL

Date approved by LSAB	Revised June 2018
Author	Sue Tabberer Reviewer: Sean Smythe
Detail of review amendments	Revised with GDPR and Data Protection 2018
Next Review Date	March 2021

CONTENTS:

Section 1: Context

Section 2: Practical Guidance

Appendices

Section 1 - Context

1. Introduction

1.1 Sharing the right information, at the right time, with the right people, is fundamental to good practice in safeguarding adults, though this is often complex. 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. This agreement aims to facilitate the lawful and secure sharing of information between partner agencies and professionals working together to safeguard adults.

1.2 An Information Sharing Agreement is a protocol that sets out the detail under which information can be exchanged under certain circumstances. Information Sharing Protocols are not required before front line practitioners can share information about an individual. By itself, the lack of an Information Sharing Protocol must never be a reason for not sharing information that could help a practitioner deliver services or keep a person safe from harm or the risk of harm.

1.3 This Information Sharing Protocol is an agreement between all agencies working together under the remit of the Bath and North East Somerset (B&NES) Local Safeguarding Adult Board (LSAB) to ensure the health, well-being and safeguarding of adults in the B&NES area.

1.4 The aim of this protocol is to establish a common set of key principles and standards to be used by all professionals working with the sub regional Multi-Agency Safeguarding Adults Policy Joint Regional Safeguarding Adults Multi-Agency Policy (December 2017) and the B&NES LSAB Multi-Agency Safeguarding Adults Procedures (January 2018). All partners of the LSAB as listed in the LSAB Terms of Reference are party to this protocol.

1.5 As well as identifying the standards and principles, this protocol is intended to provide practitioners with practical guidance to enable them to share information confidently, appropriately and legally.

1.6 The following statement should guide all information sharing within the B&NES LSAB and among partners involved in responding to safeguarding concerns:

Whenever there is a need to share personal data and/or sensitive personal data to safeguard an adult at risk of abuse or neglect, the specific reasons for sharing the information should be recorded, along with why it is considered relevant. The volume and detail of information shared must always be sufficient but not excessive for the required purpose. Wherever possible, decisions to share information should be made within the context of appropriate support, rather than professionals acting alone

2. Legal framework

A number of safeguards are necessary to ensure a balance between maintaining confidentiality and sharing information appropriately. The key principles governing the sharing of information are detailed in the following legislation and guidance (further supporting information can be found in **Appendix A**)

- The Common Law Duty of Confidentiality
- The Data Protection Act 2018
- The Human Rights Act 1998, Article 8 (the right to respect for private life)
- The Crime and Disorder Act 1998
- The Mental Capacity Act 2005
- The Caldicott Principles
- Responsibilities for sharing information under the Care Act 2014
- Pressing Needs Test

3. The legal framework and principles guiding the sharing of information

3.1 The parties to this protocol are committed to ensuring that information is shared appropriately between those professionals/agencies working with adults at risk of harm across B&NES and who have a legitimate need for that information to assist with investigating alleged abuse and delivering high quality, integrated services that meet assessed need.

3.2 The following key principles guide the sharing of information between partnership organisations:

- Organisations are fully committed to ensuring that if they share confidential information that it is in accordance with their legal, statutory and common law duties, and, that it meets the requirements of any additional supporting guidance.
- All organisations must have in place policies and procedures to meet the national requirements for Data Protection, Data Security and Confidentiality (Information Commissioners Office) and which are consistent with this Information Sharing Protocol. The existence of, and adherence to, such policies provides all organisations with confidence that data shared will be transferred, received, used, held and disposed of appropriately.
- Organisations acknowledge their 'Duty of Confidentiality' to the people they serve. In requesting release and disclosure of personal information from other organisations, employees and contracted volunteers will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that data is not disclosed illegally or inappropriately. This responsibility also extends to third party disclosures; any proposed subsequent re-use of data which is sourced from another organisation should be approved by the source organisation.
- An individual's personal information must be complete and up to date and will only be disclosed where the purpose for which it has been agreed to share

clearly requires that this is necessary. For all other purposes, data should be anonymised.

- Where it is agreed that the sharing of personal information is necessary, only that which is needed, relevant and appropriate will be shared and would only be on a 'need to know' basis.
- When disclosing information about an individual; organisations will clearly state whether the information being shared is fact, opinion, or a combination of the two.
- There will be occasions where it is legal and / or necessary for organisations to request that personal information supplied by them is kept confidential from the person concerned. Decisions of this kind will only be taken on statutory grounds and must be linked to a detrimental effect on the physical or mental wellbeing of that individual or other parties involved with that individual. The outcome of such requests and the reasons for taking such decisions will be recorded.
- All organisations agree to make reasonable efforts to ensure that recipients of personal information are kept informed of any changes to the information that they have received, so that records can be kept up to date.
- Careful consideration will be given to the disclosure of personal information concerning a deceased person, and if necessary, further advice should be sought before such data is released.
- All organisations will ensure that Subject Access Requests made to them are responded to in accordance with the requirements outlined in the Data Protection Act (2018).
- All organisations agree that appropriate training will be given to staff so that they are aware of their responsibilities to ensure personal information is processed lawfully.
- All staff will be made aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action.
- Organisations are responsible for putting into place effective procedures to address complaints relating to the disclosure of personal information.

4. Adoption and implementation of Principles

4.1 Partner organisations agree that the principles detailed in this Protocol and its supporting practical guidance provide a secure framework for the sharing of information between their respective organisations, enabling compliance with their statutory and professional responsibilities.

4.2 The partner organisations agree to:

- Facilitate the sharing of information whenever such sharing is lawful and need can be demonstrated.
- Implement this agreement within their organisation.
- Disseminate to all staff who are directly involved in its implementation.

- Ensure staff adhere to the arrangements set out in this protocol
- Provide evidence, when requested, that the arrangements have been implemented.

5. Breaches of this Agreement

5.1 All partners to this Protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.

5.2 In the event of personal information that has been shared under this protocol having or may have been compromised, whether accidental or intentional, the organisation making the discovery will without delay;

- Inform the information provider (agency) of the details.
- Inform their Information Governance or local Data Protection Officer.
- Take steps to investigate the cause.
- If appropriate, take disciplinary action against the person(s) responsible.
- Take appropriate steps to avoid repetition.
- Take appropriate steps where possible to mitigate any impact.

5.3 On being notified that an individual's personal information has been compromised, the original provider will assess the potential implications for the individual whose information has been compromised and if necessary;

- Notify the individual concerned
- Advise the individual of their rights
- Provide the individual with appropriate support.

6. Complaints regarding information shared under this Agreement

Where complaints are received regarding the use of personal and sensitive personal information shared under this protocol, the partner organisation who is the focus of the complaint will coordinate the response in consultation with relevant partner agencies (if applicable).

7. Information Retention and Disposal

7.1 The Data Protection Act (2018) requires that personal data and sensitive personal data are not retained 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.

7.2 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 the protection arrangements are not compromised and that

such information is securely disposed of when no longer required. Commissioners of services should consider that appropriate arrangements are in place as part of their contract agreements.

8. Monitoring and Review

8.1 It is the responsibility of each agency signatory to this protocol to ensure that they have the latest version control of this Protocol. They are also responsible for ensuring that their organisation complies with the legislative framework of this Protocol and are working with policies that adequately reflect the secure processing of data.

8.2 Should any member of staff or volunteer working for a partner organisation feel that the letter and spirit of this protocol is not being honoured, or that barriers to legitimate sharing of information are being raised, this should be communicated to their organisations representative on the B&NES LSAB, who will in turn follow this up with their counterparts and Data Protection Lead in the member organisation.

8.3 The Information Sharing Protocol will be reviewed in line with the LSAB 3 year review cycle in March 2020 unless other circumstances require a review sooner, and any required changes will be considered by the LSAB.

Section 2 – Practical Guidance.

9. Background:

9.1 Information sharing is key to improving outcomes for adults with care and support needs and is essential to enable early intervention and preventative work. In many cases, it is only when information is bought together from various sources, that it is identified that a person is vulnerable, in need or at risk of harm.

9.2 The Care Act 2014 sets out a clear legal framework for how local authorities working together with partner organisations should protect adults at risk of abuse or neglect. Local Authorities have new safeguarding duties that include:

- **Lead a multi-agency local adult safeguarding system** that seeks to prevent abuse and neglect and implement preventative / protective measures to stop it from happening again;
- **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;
- **Establish Safeguarding Adult Boards** to include partnership organisations (including the Local Authority, NHS and Police) which will develop, share and implement a joint multi-agency safeguarding strategy and supporting Policies and Procedures;
- **Carry out Safeguarding Adult 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 the person who is subject to a Safeguarding Enquiry or Review, if required.

9.3 The Act also creates a clear duty of co-operation. The Guidance states that:

> *'Local Authorities **must** cooperate with each of their relevant partners, as described in section 6(7) of the Care Act, and those partners **must** cooperate with the local authority, in the exercise of their functions relative to care and support including those to protect adults'* (para 14.51).
>
> The supply of information is integral to that cooperation and *'early sharing of information is the key to providing an effective response where there are emerging concerns'* (para 14.34). All agencies are expected to be governed by a confidentiality and information sharing agreement to ensure that information is only shared on a 'need to know' basis, and in accordance with Data Protection principles.

9.4 Investigating and responding to suspected abuse or neglect requires close cooperation between a range of professionals and organisations. Safeguarding adult work is concerned with sharing personal information, both about someone who is alleged to have experienced abuse and the person(s) who are alleged to have caused the abuse.

9.5 Many agencies and organisations provide support to adults with care and support needs. At times a single agency working with an individual may identify a range of issues that need to be addressed, some of which are outside of its scope or expertise. Conversely, more than one agency could become involved with an individual but be unaware of each other's involvement.

9.6 The need to safeguard and the desire to promote wellbeing is at the heart of joined-up service delivery with a preventative focus. A positive commitment to information sharing between professionals and agencies, taking full advantage of the opportunities set out under statute, is the only way to ensure that all adults are provided with the most appropriate care and support as and when they need it.

9.7 Practitioners working in adult services are aware that problems faced by adults who have parenting responsibilities, are often likely to affect children and other family members, for example; vermin, alcohol and drugs or where there is a dangerous weapon in the house. However, this information is not always shared and opportunities to put preventative measures 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. (LSCB Information Sharing Protocol (June 2018)

9.8 **In many instances failure to pass on information, that might have prevented an adult (or child) suffering harm, can be far more serious and dangerous than an incident of unjustified disclosure.** Fears about sharing information cannot be allowed to stand in the way of the need to promote the welfare and protect the safety of an individual; therefore it is important that information

sharing is carried out appropriately and that professionals and partner agencies are aware of and confident in their information sharing responsibilities and duties.

Key messages – good practice guidance.

When sharing people's information, it is important to recognise that:

- 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.
- Emergency or life threatening situations may 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 may be justified.
- The law does not prevent the sharing of sensitive, personal information **between** organisations where the public interest service outweighs the public interest served by protecting confidentiality – for example; where a serious crime may be prevented.
- The Data Protection Act enables the lawful sharing of information.
- There should be local agreements or protocols in place setting out the processes and principles for sharing information between agencies.

- An individual employee cannot give a personal assurance of confidentiality.
- Frontline staff and volunteers should always report safeguarding concerns in line with their organisational policy – this is usually to their line manager in the first instance except in emergency situations.
- It is good practice to try to gain the person's consent to share information.
- As long as it does not increase the 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 to a safeguarding concern.
- All agencies should 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 or neglect.
- All staff, in all partner agencies should understand the importance of sharing information and the potential risk of not sharing it.
- All staff should understand when to raise and how to raise a safeguarding concern.
- The six safeguarding principles should underpin all safeguarding practice, including information sharing.

10. Confidential Information

10.1 Confidential information is covered by the Common Law Duty of Confidentiality. It applies to any information that has been received or accessed in circumstances where it is reasonable to expect that the information will be kept secret or should only be shared with a limited number of specific people. 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. Sharing relevant information with the right people at the right time is vital to good safeguarding practice.

10.2 When sharing confidential information, the key principle is that any information confided should not be used for any other purpose or disclosed further except as originally understood by the confider or with their subsequent permission. However, the Caldicott Review (2013) states that professionals must not use information governance as a reason not to share data when it is the best interests of those they are caring for. The duty to safeguard adults may mean confidential information should be shared in the public interest without consent

There is no single source of law that regulates the powers that an organisation has to use and to share personal information. Sharing information between agencies is lawful if:

- Consent is given; or
- The public interest in safeguarding a person's welfare overrides the need to keep information confidential;
- 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
- Risk to the health of another person
- Disclosure is required under a statutory obligation for example; a court order.

10.3 **Information types.**

There are two distinct classifications of data covered by the GDPR (Art. 9) and the Data Protection Act (2018), schedule 1; Personal Data and Sensitive Data.

Personal Data includes data relating to a living individual who can be positively identified from the data, or from data and other information which is at the disposal of other individuals or 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.

Sensitive personal data includes data relating to racial or ethnic origins, religious beliefs or similar belief systems, political opinions and affiliations, trade union

membership, physical or medical health (including disabilities), sexual life, the commission or alleged commission of offences, and criminal proceedings.

Information relating to adult safeguarding may include a wide range of both personal data and sensitive personal data, in circumstances relating to many types of abuse and / or neglect,

10.4 **Consent to share information.**

Many of the data protection issues surrounding disclosure can be avoided if the informed consent of the individual has been sought and obtained. As a **minimum,** individuals should be informed that data may be shared and the circumstances in which this could happen unless this poses a risk of harm or danger. Consent may be given in the following ways:

Implied consent – this means that agreement has been signalled by the behaviour of an individual with whom a discussion has been held about the issues of concern and therefore understands the implications of the disclosure of the information. For the avoidance of doubt, implied consent should not be relied upon if informed consent is attainable.

Informed consent can be given verbally or in writing but must be given freely after the alternatives and consequences are made clear to the person from whom consent is being sought. Consent should always be sought and properly recorded if it is safe, appropriate and feasible to do so.

Explicit consent is where an individual is giving a clear and voluntary indication for you to proceed with processing their information for a specific purpose, for example; to investigate an allegation of abuse. In practice, it means that an individual is clearly presented with an option to agree or disagree with the collection, use, or disclosure of personal information.

Practitioners need to make sure that the confider or data subject (the individual to whom the data / information relates) understands what will be recorded, what the information will be used for and with whom is might be shared. If the practitioner does not explain this, they will not be able to give valid informed consent for information sharing to take place. The following should be recorded when consent to share information has been freely given:

- *What information the adult has consented to be shared.*
- *Why the information may need to be shared.*
- *With whom the adult has consented the information to be shared and what basis, for example; if there are any limitations.*
- *That this has been explained to the adult and they understand the implications of giving consent to share their information.*
- *Any comments made by the adult in relation to the disclosure.*
- *Date consent was sought and given.*

Where a person lacks mental capacity to consent to information being shared.

Where the confider or data subject has been assessed as lacking mental capacity to give consent to the sharing of information, then the principles of the Mental Capacity Act (2005) must be applied. Under the Act all decisions must be made in the best interests of the person lacking capacity. The Act (Section 4) is accompanied by a Code of Practice (Chapter 5) that provides details on how to determine what is in someone's best interest.

Withdrawal or reconfirmation of consent.

The confider or data subject may withdraw consent at any time and they should be made aware of this right. If consent is withdrawn, others with whom the information has been shared must be notified.

Consent must not be assumed to be open-ended. Confirmation of continued consent should be sought after a reasonable time according to individual circumstances and an expiry date for consent should be recorded.

In the event of a change in either the extent of information being sought, or the need to share with agencies not included in the original consent agreement, a revised consent should be sought unless the information may legitimately be shared without consent.

10.5 Sharing information without consent.

It is not always safe, appropriate or feasible to obtain consent to share information. Circumstances where it may not be possible to obtain consent include:

- Where obtaining consent might be contrary to the public interest; including risk to the health of the person.
- The data subject / confider may be absent or not contactable.
- The data subject / confider may be permanently or temporarily incapacitated and has no appropriate representative.
- The data subject / confider has withheld or withdrawn their consent.

Under the Common Law Duty of Confidence, the Data Protection Act (2018) and the Human Rights Act (1998), it is possible to disclose information without consent in cases of substantial public interest or in the best interests of the individual. Additionally, information can be disclosed without consent under the Crime and Disorder Act 1998 (as amended by the Police and Justice Act 2006 and the Policing and Crime Act 2009) for community safety purposes.

Decisions regarding the disclosure of information without consent must always be made on a case-by-case basis. Any disclosure must always be proportionate and the minimum necessary to achieve the necessary objective.

If it is not possible to obtain consent before sharing information, the data subject / confider should be informed as soon as possible after the information has been shared, unless to do so would be inappropriate (for example; cause serious harm; effect an on-going investigation.

10.6 **The impact of sharing or withholding information.**

Essentially, a decision to share information without consent rests on an assessment of the relative risks of disclosure and non-disclosure and a professional judgement on the most appropriate action that should be taken in the light of this assessment.

Two key questions are:

1. What if this information is not shared?
2. Who will be affected by this information being shared?

The former considers whether a negative impact is likely if the information is withheld. There will be a clear interest in disclosing information where there is an evident risk to the life or well-being of an individual which is accentuated or not addressed by not doing so; the protection of health, morals and the rights and freedoms of other; public safety; and the prevention of crime and disorder. If the substantive, the public interest value may over-ride that of an individual's human rights.

The latter considers whether there is a disproportionately negative impact in information being made available, for example; familial breakdown or personal risk resulting from unnecessary disclosure. Disclosure should be assessed for its potential impact on others who may be identifiable from the data such as witnesses or staff who are involved in cases, or whose vulnerability makes their interests the over-riding consideration.

Further information can be obtained from the B&NES Multi Agency Safeguarding Adults Consent Policy (June 2016).

10.7 **Disclosing information under this agreement.**

Practitioners disclosing information must always consider the safety and welfare of the adult when making decisions on whether to share information about them. For example; where there is concern that an adult may be suffering or is at risk of suffering serious harm, then the adult's safety and welfare must be the overriding consideration. Where possible, consent should be obtained from the adult to share specific personal information.

The person making the disclosure must also ensure that any information disclosed is:

- Necessary for the specific purpose(s) for which they are sharing it;
- Accurate and up to date;
- Depersonalised (where appropriate);
- Shared only with those people who need to see it; and
- Transferred securely.

11. Information sharing purposes

11.1 There are numerous reasons why an individual may be asked to share information as a result of safeguarding concerns as follows:

1. To seek advice about a specific adult safeguarding situation or to establish grounds for an adult safeguarding response.
2. To prevent or detect a crime, or support the prosecution of offenders.
3. To raise a safeguarding concern.
4. To safeguard an adult at risk of harm or neglect.
5. To make a referral to a partner organisation for immediate action to protect an adult.
6. To establish the potential need for involvement of partner organisations in safeguarding work (Enquiry, prosecution or protection arrangements).
7. To plan, initiate and conduct a Section 42 Safeguarding Enquiry.
8. To make a referral to organisations for the purposes of requesting or amending services to persons or organisations alleged to have caused harm.
9. To make a referral to the Disclosure and Barring Service (DBS) or to provide information to the DBS for the purposes of them coming to a barring decision.
10. To make a referral to, or provide information, to a professional regulator for the purposes of them coming to a decision.
11. To notify the Care Quality Commission (CQC) who may need to take action relating to a source of risk that is a registered care provider.
12. To notify the Charity Commission who may need to take an action relating to an organisation alleged to have caused harm that is a registered charity.
13. To notify employers who may need to take an action about a member of staff, a volunteer or a student (paid or unpaid) who is believed to be a source of risk in their work.
14. To notify service providers of risks imposed by other service users.
15. To inform the development of multi-agency procedures and strategies for protecting adults at risk of abuse.
16. To monitor and review adult concerns and the impact of safeguarding policies and procedures including both the equalities (race, ethnicity, gender, sexuality, age, disadvantages and disability) impact of the policies and the outcomes for individuals. This may include both quantitative and qualitative information, personal data and sensitive personal date, the personal views of individuals and the expressions of relevant professional opinion.
17. To conduct Safeguarding Adult Reviews.
18. To deal with complaints, grievances and professional and administrative malpractice.

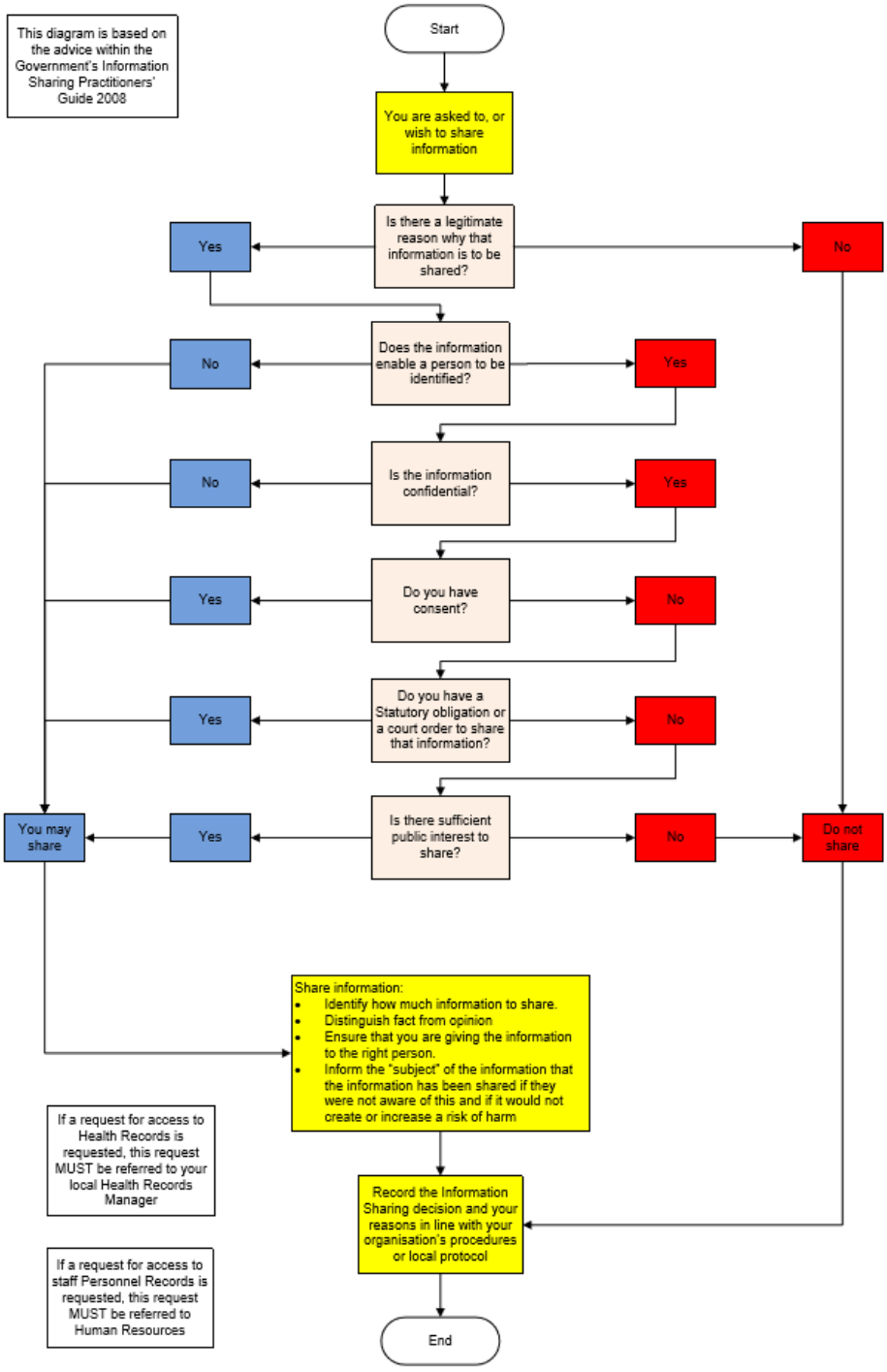
Good practice guidance:

- Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons 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, and seek their agreement, unless it is unsafe or inappropriate to do so.
- 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, that lack of consent can be overridden in the public interest. 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 the 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 a timely fashion, and is shared securely.
- 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.

Information Sharing: Guidance for Practitioners and Managers [1] (HM Government, March 2009).

11.2 Flowchart of key principles for information sharing.

The Information Sharing Flowchart below should be used as a basis for decision making for information sharing by all practitioners along with the Golden Rules to share information:



Seek advice from your manager / supervisor or Caldicott Guardian if you are not sure what to do at this stage and ensure that the outcome of the discussion is documented.

11.3 It is the requirement of the B&NES Safeguarding Adults Information Sharing Protocol that all agencies and staff/practitioners adhere to the **Golden Rules** for information sharing in all instances of information exchange. These are:

- Confirm the identity of the person you are sharing with
- Obtain consent to share if safe, appropriate and feasible to do so
- Confirm the reason the information is required
- Be fully satisfied that it is necessary to share
- Check with a manager / specialist or seek legal advice if you are unsure
- Don't share more information than is necessary
- Inform the recipient if any of the information is potentially inaccurate or unreliable
- Ensure that the information is shared safely and securely
- Be clear with the recipient how the information will be used
- Record what information is shared, when, with whom and why; and if you decide not to share, record your reasons.

Further supporting guidance is available in **Appendix B – Data Sharing Checklist**

12. Powers or obligations to share information for adult safeguarding.

12.1 Caldicott Principles (2013)

The Care Act 2014 states that any agreement for information sharing should be consistent with the principles set out in the Caldicott Review published in 2013. The Caldicott Principles require that Health and Social Care Staff are professionally obliged to comply with these principles when processing person identifiable information.

1. **Justifying the purpose(s) –** every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use personal confidential data unless it is absolutely necessary –** personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for adults to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary personal confidential data –** where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of persona confidential data transferred or accessible as is necessary for a given function can be carried out.
4. **Access to personal confidential data should be on a strict need-to-know basis –** only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items

that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities –** action should be taken to ensure that those handling personal confidential data (both clinical and non-clinical staff) / are made fully aware of their responsibilities and obligations to respect the adult with care and support needs' confidentiality.
6. **Comply with the law –** every use of personal confidential information data must be lawful. Someone in each organisation handling personal confidential data 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 the adult with care and support needs' confidentiality –** health and social care professionals should have the confidence to share information in the best interests of their patients / adult with care and support needs within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

12.2 Duty of Candour

The Health and Social Care Act 2008 (Regulated Activities) (Amendment) Regulations 2015 extended the fit and proper person requirement for directors and the Duty of Candour to all providers from 1 April 2015. Regulation 20 defines what constitutes a notifiable safety incident for health service bodies and all other providers (such as primary medical and dental practices, adult social care and independent healthcare providers) (add hyperlink). The introduction of Regulation 20 is a direct response to recommendation 181 of the Francis Inquiry report into Mid Staffordshire NHS Foundation Trust.

The Duty of Candour requires all health and adult social care providers registered with CQC to be open with people when things go wrong. The regulations impose a specific and detailed duty on all providers where any harm to a patient / service user from their care or treatment is above a certain harm threshold.

The Duty of Candour is a legal requirement and CQC is able to take enforcement action when / if breaches occur. The duty requires registered providers to:

- 'act in an open and transparent way in relation to service user care and treatment';
- tell the person concerned when something has gone wrong as soon as possible and provide support to them; and
- give an apology and keep the person informed about any further enquiries.

This means that the default position should be open, honest and candid, unless there are justifiable reasons for not being so. However, these circumstances should be the exception rather than the norm.

This protocol embraces the Duty of Candour in relation to safeguarding adults. All Section 42 enquiries and safeguarding processes must check that this Duty has been fulfilled. Further information can be found at (add hyperlink).

12.3 Professional Codes of Conduct

Many professionals, including those in health and social care, are registered with a professional body (for example, the Nursing and Midwifery Council) and are governed by a code of practice or conduct. These codes require those professionals to report any safeguarding concerns in line with guidance or legislation. Additionally, concerns regarding a professional's conduct that has caused harm to an individual (and others) should be referred to the relevant body. This applies even if they have left their job and regardless of whether they have been convicted or a related crime. Referrals should be carried out promptly and appropriately.

12.4 Referring to the Disclosure and Barring Service

The Safeguarding Vulnerable Groups Act (2006) places specific duties on those providing 'regulated' health and social care activities. They must refer to the Disclosure and Barring Service (DBS) anyone who has been dismissed or removed from their role because they are thought to have harmed, or pose a risk of harm to, a child or adult with care and support needs. This applies even if they have left their job and regardless of whether they have been convicted of a related crime. Referrals of individual employees to the DBS should be carried out promptly and appropriately. This may be an outcome of the safeguarding process following a Section 42 Enquiry.

12.5 Commissioners

Commissioning Services should consider whether contracts should place an obligation on service providers to share safeguarding information when requested. Any specifications would need to be in line with policy, regulation and the law

12.6 Safeguarding Children

Sharing data is crucial to protecting the child (even when the child or young person does not agree). Failure to share appropriate data places children at greater risk.

Where the safety or welfare of a child is in doubt, staff / practitioners must share data with the statutory agencies which can provide protection (Children's Social Care and the Police). This is irrespective of whether the child and / or their parents or carers have given permission for information to be shared. This is a legal duty under the Children's Act 2004. Failure to share relevant data places a child in danger, and leaves staff / practitioners vulnerable to both professional misconduct and disciplinary procedures. Further information can be found in the LSCB Information Sharing Protocol (June 2018)

Sharing information on prisoners

The statutory guidance to the Care Act 2014 requires Local Authorities to share information about people with care and support needs in, or in transition from or to, prison or custodial settings. This includes 'the sharing information about risk to the prisoner and others where this is relevant'.

12.7 Multi Agency Safeguarding Hub (MASH)

The B&NES Multi Agency Safeguarding Hub was established in September 2016. It has its own formalised procedures and arrangements for information sharing. The purpose of the MASH is to ensure that relevant information about potential safeguarding concerns in respect of children and adults is shared appropriately by partner agencies where necessary. This enables the level of risk to be assessed appropriately and allows for suitable responses to be agreed.

12.8 Domestic Abuse, Stalking, Harassment and Honour Based Violence (DASHH)

Making links between adult safeguarding and domestic abuse is vital to make sure that people have access to the best help that can be offered, are treated with dignity and respect and are supported to achieve the best outcomes for them.

Domestic abuse is defined as ‘any incident or pattern of incidents of controlling, coercive or threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless of gender or sexuality’.

Please refer to the relevant information sharing protocol for information sharing arrangements for domestic violence and MARAC (Multi Agency Risk Assessment Conference).

Multi Agency Public Protection Arrangements (MAPPA)

Multi Agency Public Protection Arrangements are in place to ensure the successful management of violent and sexual offenders.

Section 325 (4), of the Criminal Justice Act 2003 (‘CJA 2003) expressly permits the sharing of information between these agencies for MAPPA purposes.

Violent and sexual offenders are supervised by police, probation, youth offending teams and mental health services. These organisations can refer offenders for consideration by a multi-agency meeting. The task of these meetings is to share information, assess the risk(s) the offender represents, and plan safeguards to protect the public. Every case has built-in timescales for the risk management plan, individual accountability and a mechanism for checking progress. MAPPA are set up in B&NES to consider the risks posed by sexual and violent offenders. Sharing of information through MAPPA must be approved by the Chief Constable (Avon and Somerset Constabulary).

Please refer to the purpose specific information sharing protocol for sharing arrangements for the MAPPA.

12.9 Deprivation of Liberty Safeguards (DOLS)

The Mental Capacity Act Deprivation of Liberty Safeguards (MCA DOLS) came into effect on 1 April 2009. These safeguards address the gap in domestic legislation to ensure compliance with the European Convention on Human Rights (1953) and provide the lawful deprivation of liberty of those people who lack capacity to consent to arrangements to be made for their care and treatment in either hospitals or care homes, but who need to be deprived of their liberty in their own best interests, to protect them from harm.

Local Authorities (designated as 'supervisory bodies' under the legislation) will have statutory responsibility for operating and overseeing the MCA DOLS whilst hospitals and care homes ('managing authorities') will have responsibility for applying to the relevant Local Authority for a Deprivation of Liberty authorisation.

12.10 Domestic Homicide Reviews (DHR)

Domestic Homicide Review means a review of the circumstances in which the death of a person aged 16 or over has, or appears to have, resulted from violence, abuse or neglect by –

a) a person to whom s/he was related or with whom s/he was or had been in an intimate personal relationship; or
b) a member of the same household as him/herself, held with a view to identifying the lessons to be learnt from the death.

Where the definition set out in this paragraph has been met, then a Domestic Homicide Review (DHR) must be undertaken. Please refer to the purpose specific information sharing protocol arrangements.

12.11 Person in Position of Trust

'People in a Position of Trust' are currently defined as those who work with children, young people and adults with a care and support need and applies whether in a paid or voluntary basis'. Local authority responsibilities for safeguarding adult activity are based on the Care Act (2014) guidance which includes reference to 'Positions of Trust' and to the management of allegations of adult abuse against staff employed to work with adults with care and support needs.

Sharing information with carers, parents, family, partners etc

When the adult has the capacity to make the decision, it should be up to them to decide what information is disclosed to their carers/ parents/ family/ partners, and records should reflect this unless this would put the person at significant risk.

When the adult does not have the capacity, information should, as a matter of course be shared with carers/parents of the adult unless there are clear reasons not to. In addition, consideration must be given to the relationship between the carers/parents and the person alleged responsible

Clear decisions should be recorded about when and what to share, and who the most appropriate person to talk is. More generally, assessment should be made as

to whether the sharing of certain information with a particular person or organisation is in the adult's best interests

12.12 Sharing information with third parties about the 'alleged person responsible' – using the Test of Pressing Need.

Organisations and workers must 'honestly and reasonably believe' that the sharing of information is necessary to protect an adult or the wider public and must use the test of 'pressing social need'. To pass this test the relevant organisation must consider the following issues

- How strong is the belief in the truth of the particular allegation? The greater the conviction that the allegation is true, the more compelling the need for disclosure.
- What is the interest of the third party in receiving the information? The greater the legitimacy of the interest in the third party in having the information, the more important the need to disclose.
- What is the degree of risk posed by the individual if disclosure is not made?

Decisions about who needs to know and what needs to be known should be taken on a case-by-case basis. The consequences of disclosure should be balanced against the risks to the adult at risk. In such cases the issues of proportionality and necessity are key.

This decision should be made at the safeguarding planning meeting / discussion stage, where it will be determined who, as part of the Section 42 Enquiry will contact and speak to the person alleged responsible and how this will be managed.

The person alleged responsible should be given the right to reply to any allegations and should have an opportunity to correct any information held about them that is not accurate

12.13 Disclosures to other organisations outside the Safeguarding Process (Safeguarding Adult Procedures or a Safeguarding Adult Review).

There may be some cases where the risk posed by an individual in the community cannot be managed without the disclosure of some information to a third party outside the organisations immediately involved in the review. Such an example would be where an employer, voluntary group organiser or church leader has a position of responsibility/control over the individual, and other persons who may be at serious risk.

Caution should be exercised before making any such disclosure. The following factors should be taken into account:

- Does the individual present a risk of serious harm to the adult, or to those for whom the recipient of the information has responsibility. The correct person to receive information will be the person who needs to know in order to minimise or prevent the risks.
- Is there no other practical, less intrusive means of protecting the adult, and failure to disclose would put them in danger? Only that information which is

necessary to prevent harm should be disclosed, which will rarely be all the information available.

- The disclosure is to the right person and that they understand the confidential and sensitive nature of the information they have received. The information will not be disclosed by the recipient third party without the express permission of the original disclosing organisation. Consider consulting the individual about the proposed disclosure. This should be done in all cases, unless to do so would not be safe and appropriate. If it is possible and appropriate to obtain the individual's consent, then a number of potential objections to the disclosure are overcome.
- Ensure that whoever has been given the information knows what to do with it. Again, where this is a specific person, this may be less problematic but in the case of an employer, for example, advice and support may need to be given.
- The risk to the individual should be considered although it should not outweigh the potential risk to others were disclosure not to be made. The individual retains his/her rights under The Human Rights Act 1998 and consideration must be given to whether those rights are endangered as a consequence of the disclosure.

12.14 Disclosing information about the person raising the safeguarding concern.

Employees / volunteers - Where there is a safeguarding concern, employees have a duty to raise a concern. This will be done via their manager or safeguarding lead, however it can be raised directly with B&NES Community Services on 01225 396000 or the Emergency Duty Team (EDT) for out of hours/Weekend calls on 01454 615165. When an employee raises a concern, it must be explained to them that their identity may not remain confidential and may be shared with the alleged person responsible. The only exception to this is where there is a significant risk of harm to the employee or their identity is known to the alleged person responsible. Employees / volunteers should be referred to their organisational whistleblowing policy. ** Raising concerns without fear of prejudice.

Members of the public raising a concern – in a situation where a member of the public has raised a concern, there is an expectation of confidentiality, in that their identity will be protected within the safeguarding process. In most situations the person alleged responsible, family members and anyone outside of the safeguarding procedures will not know the identity of the person raising the concern, unless the case goes to court, and the testimony of the person raising the concern is required. This should be made clear to them at the time of the concern being raised, and recorded that this has been explained to them.

Adults or family members raising a concern – as with members of the public raising a concern, in most cases family members and/or other adults raising concerns via the safeguarding process may wish for their identity to remain confidential. This may be due to potential risks they may be exposed to as a result of them raising a concern, or situations where their care or the care of someone else may be compromised. Therefore it is essential that when a concern is raised, you

establish whether or not the person raising the concern is in agreement with their details being made known to the person alleged responsible and the reasons for this. If there is an unrealistic expectation of confidentiality or it is likely that their confidentiality cannot be maintained, then this must be explained and recorded on the file. If there are genuine reasons to maintain the confidentiality of the person raising the concern, this must be shared with everyone within the safeguarding process, so that anonymity is maintained. Again, as with the above, if the case goes to court, and the testimony of the person raising the safeguarding concern is required, their identity may need to be revealed. This should be made clear to them at the time of the concern been raised, and recorded that this has been explained to them. The person raising the concern is entitled to feedback on the outcome of the safeguarding enquiry/review, but due consideration should be given as to whether any identities can be disclosed to the alerter.

12.15 Disclosing information to the 'person alleged responsible'.

The person alleged responsible is entitled to know certain details about the allegations made against them in the safeguarding process. They have a right to know any allegations made against them as well as any relevant information that needs to be shared with them as a part of the safeguarding process. If they wish to see all information held on them as a part of the investigation, an application should be made under the Data Protection Act 2018, Subject Access. In most cases third party information will be redacted before it is disclosed to them, even though the identities may be known to them.

When disclosing information to the person alleged responsible in the safeguarding process, careful consideration needs to be given as to whether or not the identities of the person raising the concern and the identity of the adult being abused can be disclosed.

In most cases the identity of the adult will be disclosed unless this will put them at further risk or harm or they have explicitly withdrawn consent to share this with the person alleged responsible.

The identity of the alerter will remain confidential if the person raising the concern has expressed that they wish to remain anonymous or they are at risk or harm or discrimination if their identity is known. Careful consideration need to be given here if there is an expectation of confidentiality.

13. Methods for sharing information.

13.1 Each partner organisation will ensure that there are appropriate arrangements in place to ensure that any personal or personal sensitive information (protected or restricted information), is transferred securely.

Within the safeguarding process, information may be transferred in the following ways:

- Verbally, face to face, in meetings, on the telephone or via FAX.

- In written communications (for example; forms, minutes, letters, statements or reports) transferred in hard copy though internal or external mail services.
- Documents transferred on encrypted electronic digital media devices.
- In written information transferred by secure email, or secure file transfer systems.
- Information accessed in situ, via provision of access to organisational data bases or records.

13.2 When any of these methods are used it is essential to consider the safest way to record and mark the information, and to ensure safe transit and delivery. Information should be appropriately secured in transit and transferred by methods aligned to best practice as specified in the report 'Protecting Information in Government' – January 2010'.

1. Verbal conversations and interviews should be recorded in a written statement that is agreed by the information giver. Care must be taken to record and denote information clearly as fact, statement or opinion and attribute any statement or opinion to the owner. All information should be recorded in such a way that it can be used as evidence in court, should that be required at a later date.
2. Disclosures of information over the telephone should only be conducted where the identity of the recipient is known and has been verified.
3. Meetings should be recorded in minutes that are agreed by the delegates present and authorised by the Chair (Team Manager, Safeguarding Adults and Quality Assurance, B&NES Council).
4. Written communications containing confidential information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly marked 'Private and Confidential – to be opened by recipient only'. Any PROTECT / RESTICTED information shared by post must be done via registered post or secured courier.
5. When files are transferred on electronic digital media devices, the files should be encrypted to an appropriate standard, with decryption keys / passwords supplied separately.
6. When confidential information is sent by email, it should be sent and received using secure government domain email addresses, to ensure encryption of information in transit. The full list of secure Government email systems are below. They have the following address endings:

- .cjsm.net (Criminal and Justice).
- .gcsx.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 ((NHS mail).
- .pnn.police.uk (Police)

- .scn.gov.uk (Criminal and Justice).

7. In-transit security is reliant on BOTH the sender AND the recipient using one of the email domains listed above. In the absence of this, the SENDER will need to encrypt the content of the email using additional software. 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.

8. Fax is only secure if the person who requires the information is waiting by the receiving fax machine to receive the document immediately. Confirmation should be immediately sought that information has been received by the intended recipient. A record of the transmission must be retained.
9. In the event that a recipient receives information from an unsecured route, it is incumbent on the recipient to advise the sender and agree a secure route for future transfers of information. The sender and recipient should also inform their manager of a breach in data protection and follow their own organisational procedures (also see Section 4 of this Protocol).

14. Record keeping and confidentiality

14.1 Organisations will have their own recording systems for keeping comprehensive records whenever a concern is made/arises/occurs, and of any work undertaken under the B&NES Multi-Agency Safeguarding Adult Procedures, including all concerns received and all referrals made.

14.2 Organisations should refer to their own internal policies and procedures for additional guidance on recording and storage of records. Throughout the safeguarding process, detailed factual records must be kept. This includes the date and circumstances in which conversations and interviews are held, who was involved and a record of all decisions taken relating to the process.

14.3 Records may be disclosed in court as part of the evidence in a criminal action/case or may be required if the regulatory or statutory authority decides to take legal action against a provider.

14.4 Records kept by providers of services should be available to service commissioners and to regulatory authorities. Agencies should identify arrangements, consistent with the principle of fairness, for making records available to those affected by, and subject to, investigation with due regard to confidentiality.

15. Reluctance to share information (applying Section 45 Care Act)

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

15.2 A 'Supply 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 function'.

15.3 Such supply of information requests may concern, but are not necessarily limited to Safeguarding Adult Reviews and the undertaking of Section 42 safeguarding enquiries.

15.4 Requests for the Board to exercise Section 45 must be made in writing to the Chair of the SAB by the organisation's Board Member or Deputy, detailing how the relevant criteria are met.

15.5 Wherever practicable, the Chair of the SAB 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 of harm.

Appendix A - Key Statutory Provisions, legislation and supporting guidance

Data Protection Act 2018

The key legislation governing the protection and use of identifiable patient/service user information (Personal Data) is the Data Protection Act 2018. The Act does not apply to data relating to the deceased.

The Act stipulates that anyone processing personal data comply with eight principles of good practice. These principles are legally enforceable.

Principle 1: Personal data processing shall be lawful and fair.

Principle 2: Personal data shall be processed for a specified, explicit and legitimate purpose. and should be limited to only those uses.

Principle 3: Personal data shall be adequate, relevant and not excessive.

Principle 4: Personal data shall be accurate and, kept up to date

Principle 5: Personal data processed for any purpose or purposes shall not be kept longer than is absolutely necessary.

Principle 6: Personal data shall be processed in a secure manner.

Common Law duty of Confidentiality

All staff working in both the public and private sector are subject to a common law duty of confidentiality and must abide by this. The common law duty protects from disclosure, information (whether personal/sensitive or not) that *'is given in circumstances giving rise to an obligation of confidence on the part of the person to whom the information has been given'.* 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, for example; 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 the purposes that the subject has been informed about and has consented to. This duty is not absolute but should only be overridden if:

- The information is not confidential in nature; or
- The person to whom the duty is owed has given explicit consent; or
- There is an overriding public interest in disclosure; or
- Sharing is required by a court order or other legal obligation.

When considering disclosure, a judgement must be made as to where the public interest lies (the more sensitive and damaging the information, the stronger the public interest in disclosure needs to be). Disclosure of confidential information must always be considered on a case-by-case basis and the reasons for the decision,

clearly recorded. When obtaining information from someone, it is important not to give an unrealistic expectation of confidentiality.

Whilst it is not entirely clear under law whether or not a common law Duty of Confidentiality 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.

Human Rights Act 1998 and the European Convention on Human Rights

The European Convention on Human Rights has been interpreted to confer positive obligations on public authorities to take reasonable actions within their powers (which would include information sharing) to safeguard the Convention rights of adults. These rights include right to life (Article 2), the right not be subjected to torture or inhuman or degrading treatment (Article 3) and the right to liberty and security (Article 5).

Article 8 of the European Convention on Human Rights was incorporated into UK law by the Human Rights Act 1998 and recognises a right to respect for private and family life:

- Article 8.1 provides that *'everyone has the right to respect for his private and family life, his home and his correspondence'*.
- Article 8.2 provides there will be no such interference by a public authority with 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, for the prevention of crime and disorder, protection of health and morals, or for the protection of rights and freedoms of others.

Sharing confidential information may be a breach of an individual's Article 8 rights. The question is whether sharing information would be justified under Article 8.2 and proportionate. Consideration should be given to pressing social need, whether sharing information is a proportionate response to this need and whether considerations can override the individual's right to privacy. If a person is at risk of significant harm, or sharing information is necessary to prevent crime or disorder, breach of the person's may be justified under Article 8. A decision to share information and the reasoning behind it should be recorded.

Crime and Disorder Act 1998

The Crime and Disorder Act 1998 introduced measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing care and disorder in the local area.

Section 115: establishes a gateway (the power) to disclose information, which is central to the Act's partnership approach. It must be remembered that this is a power

and not a duty meaning you must still meet the requirements of the Human Rights Act, Common Law Duty and the Data Protection Act.

The Police have an important and general power at common law to disclose information for the prevention, detection and reduction of crime. However, some other public bodies which collect information may not previously have had power to disclose it to the Police and others. This section therefore puts beyond doubt the power of any organisation to disclose information to the Police authorities, local authorities, probation committees, health authorities, or to persons acting on their behalf, so long as such disclosure if necessary or expedient for the purposes of this Act.

These bodies also have the power to use this information. It is to be noted that there is no requirement to exchange information, merely permission to do so. The purpose of the Act broadly covers the prevention and reduction of crime and the identification or apprehension of offenders.

Domestic Violence, Crime and Victims Act 2004

Domestic Homicide Reviews (DHRs) were established on a statutory basis under Section 9 of the Domestic Violence, Crime and Victims Act (2004). The provision came into force on 13 April 2011; responsibility for undertaking DHRs lies with the Community Safety Partnership (CSP) within the victims area of residence (where the victim's area of residence is not known, the CSP lead responsibility will relate to the area where the victim was last known to have frequented as a first option and then considered on a case by case basis).

Criminal Justice Act 2003

Section 325 of the Criminal Justice Act 2003 details the arrangements for assessing risk posed by different offenders;

- The 'responsible authority' in relation to any area, means the chief officer of police, the local probation board and the Minister of the Crown exercising functions in relation to prisons, acting jointly.
- The 'responsible authority' must establish arrangements for the purpose of assessing and managing the risks posed in that area by:
  a) Relevant sexual and violent offenders; and
  b) Other persons who, by reason of offences committed by them are considered by the 'responsible authority' to be persons who may cause serious harm to the public.
- In establishing those arrangements, the 'responsible authority' must act in cooperation with the persons identified below.
- Cooperation may include the exchange of information.

The following agencies have a duty to cooperate with these arrangements:

- Every Youth Offending Team established in an area
- The Ministers of the Crown, exercising functions in relation to social security, child support, war pensions, employment and training.

- Every Local Education Authority.
- Every Local Housing Authority or Social Services Authority
- Every registered social landlord which provides or manages residential accommodation
- Every Health Authority or Strategic Health Authority
- Every Primary Care Trust or Local Health Board (Clinical Commissioning Groups)
- Every NHS Trust
- Every person who is designated by the Secretary of State as a provider of electronic monitoring services.

Immigration and Asylum Act 1999

Section 20 provides for a range of information sharing for the purposes of the Secretary of State:

- To undertake the administration of immigration controls to detect or prevent criminal offences under the Immigration Act;
- To undertake the provision of support for asylum seekers and their dependents.

National Health Service Act 2006

Part 3, Section 82 of the National Health Service Act 2006 places a duty on NHS bodies and local authorities to cooperate with one another in order '*to secure and advance the health and welfare of the people in England and Wales*'.

National Health Service and Community Care Act 1990

National Health Service and Community Care Act 1990 provides that when a local authority is assessing need and it appears that there may be a need for health or housing provision, the local authority shall notify the appropriate CCG, Health Authority or Housing Department and invite them to assist.

Children Act 2004

Section 10 of the Act places a duty on each Children's Services authority to make arrangements to promote cooperation between itself and relevant partner agencies to improve the well-being of children in their areas in relation to:

- Physical and mental health, and well-being
- Protection from harm and neglect
- Education, training and recreation
- Making a positive contribution to society
- Social and economic well-being

These five outcomes have since been embodied in the Every Child Matters Green Paper as universal ambitions for every child and young person. The relevant partners must cooperate with the local authority to make arrangements to improve children's well-being. The relevant partners are:

- District Councils
- Police
- Probation Service
- Youth Offending Teams
- Strategic Health Authorities and CCGs
- Connexions
- The Learning and Skills Council

The statutory guidance for Section 10 states that good information sharing is key to successful collaborative working and that arrangements under Section 10 of the Act should ensure that information is shared for strategic planning purposes and to support effective service delivery. It also states that these arrangements should cover issues such as improving the understanding of the legal framework and developing better information sharing practice between and within organisations.

The **Children's and Family Act (2014)** also emphasises the accessibility of information to adult teams taking over the care of those children transitioning into adulthood.

The Caldicott Report (1997) and the Caldicott Review (2013)

The sharing of information in health and social care is guided by The Caldicott Principles. Each organisation should have a senior person to act as a Caldicott Guardian. The Caldicott Principles are reflected in the Data Protection Act and are useful to other sectors:

- Justify the purpose(s) for using confidential information
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum personal confidential data necessary for purpose
- Access to personal confidential data should be on a strict need-to-know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

The most recent discussion of all aspects of an individual's identifiable information and how this is to be protected can be found in the Caldicott Committee Report on the review of patient-identifiable information. That report recognises that confidential information may need to be disclosed in the best interests of the individual and discusses in what circumstances this may be appropriate and what safeguards need to be observed.

The safeguards can be summarised as follows:

- information will only be shared on a 'need to know' basis when it is in the best interests of the adult;
- confidentiality must not be confused with secrecy;

- informed consent should be obtained but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement; and,
- it is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other vulnerable people may be at risk

Decisions about who needs to know and what needs to be known should be taken on a case by case basis, within agency policies and the constraints of the legal framework.

Principles of confidentiality designed to safeguard and promote the interests of an adult should not be confused with those designed to protect the management interests of an organisation. These have a legitimate role but must never be allowed to conflict with the interests of an adult. If it appears to an employee or person in a similar role that such confidentiality rules may be operating against the interests of adults at risk of abuse or neglect then a duty arises to make full disclosure in the public interest.

Freedom of Information Act 2000

The Freedom of Information Act provides clearly 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 the Data Protection Act 2018.

Health and Social Care Act 2012

The Health and Social Care Act 2012 underpins wide ranging reforms of the NHS since founded in 1948. Changes include the establishment of a National Health Service Commissioning Board and Clinical Commissioning Groups, as well as the Health and Wellbeing Board. The changes became operational on 1 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 cooperation 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 information. 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.

The Care Act 2014

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

The sections with most relevance to information sharing are:

Sections 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.

Section 37: Duty to notify the receiving Local Authority when an adult receiving care and support moves.

Section 45: Duty to comply with a request for information by the Safeguarding Adults Board to enable or assist the SAB to exercise its functions. This could include information about individuals.

Section 67: Involvement of independent advocate in assessments plans etc.

Statutory guidance is available on all parts of this Act (add hyperlink)

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 are available from http://ico.org.uk/

Anonymisation Code of Practice

Data Sharing Code of Practice

Subject Access Code of Practice

Guide to Data Protection

Appendix B

Data Sharing Checklists

These two Data Sharing Checklists provided by the Information Commissioners Office (Data Sharing Code of Practice) provide a handy step by step guide through the process of deciding whether to share personal data. One is for systematic data sharing, the other is for one off requests.

These checklists are designed to be used alongside the full code and highlight the relevant considerations to ensure that the sharing complies with the law and meets individuals' expectation.

1. Data Sharing Checklist – systematic data sharing

Scenario – you want to enter into an agreement to share personal data on an ongoing basis.

Is the sharing justified?

Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information that you have been asked to share (for example; was it given in confidence?).
- Any legal obligations to share information (for example; a statutory requirement or court order).

If you decide to share.

It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate this information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.

- Agreed common retention periods for the data.
- Processes to ensure deletion takes place.

2. Data Sharing Checklist – one off requests.

Scenario – you are asked to share personal data relating to an individual in 'one off' circumstances.

Is the sharing justified?

Key points to consider:

- Do you think you should share this information?
- Have you assessed the potential benefits and risks to individuals and/or society or sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the Data Protection Act to share?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information that you have been asked to share (for example; was it given in confidence?).
- Any legal obligations to share information (for example; a statutory requirement or a court order).

If you decide to share.

Key points to consider:

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information should be shared securely.
  - Ensure you are giving information to the right person
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision.

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share the information you should record:

- What information was shared and for what purpose.

- Who you shared it with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

REMEMBER: Only share on a need to know basis and enough information to achieve the necessary outcome. This is known at the principle of PROPORTIONALITY. The amount of confidential information disclosed and the number of people to whom it is disclosed, should be no more than is strictly necessary to protect the health and wellbeing of the adult at risk.