Tayside Practitioner's Guidance:

Code of Practice: Information Sharing, Confidentiality and Consent

19 July 2019

1. Purpose and Background

1.1 This Code of Practice has been requested from the Tayside Adult Support and Protection Chairs and Lead officers to ensure staff understand the legislative and policy context when sharing personal information.

1.2 Staff in the public, private and third sectors in Perth and Kinross discharge their individual and collective responsibility for services for adults at risk and their families including adult protection. The Adult Protection Committees provides leadership, direction, support, challenge and scrutiny of these services.

1.3 The Adult Protection Committees recognise that the appropriate processing of information (data), which includes sharing information, is vital in order to ***safeguard, support*** *and* ***promote*** the *welfare* of adults who may be at risk

1.4 It is recognised that the extent to which communication and effective sharing of relevant information takes place has been a key feature in many Significant Case Reviews (SCRs). It is therefore of the utmost importance that all managers and practitioners understand their respective duties; the legislative, policy and practice parameters relating to information sharing and the constraints of confidentiality and consent.

1.5 The Adult Protection Committees recognise that procedures and guidance cannot *in themselves* protect vulnerable adults from harm and exploitation; but a ***competent, confident*** and ***skilful*** workforce, working together with a vigilant public can.

1.6 This Code of Practice has been refreshed for all staff and volunteers working across the public, private and third sectors in Perth and Kinross. It is aimed at all people working in the frontline with adults and their families who have to make decisions about sharing ***personal data*** *(information)* or ***special category data*** *(information)* on a case-by-case basis. **It applies equally to those who work in health and social care. services and adult services; in particular to all staff working with adults at risk.**

1.7 This Code of Practice aims to support managers and practitioners in their decisions when considering whether they need to share information and what steps they need to take to ensure that they are doing so *lawfully, fairly and in a transparent manner*. It supports the application of sound *professional judgment* and *empowers safe practice* to ***safeguard, support*** and ***promote*** the *welfare* of adults at risk and *protect* them from *harm* and *exploitation*.

1.8 The Adult Protection Committees recommends that all managers and practitioners should download and save this Refreshed Code of Practice as a useful electronic resource and reference.

2. Information Sharing

2.1 ***Why is information sharing important?***

2.2 Early and effective intervention relies on good practice in the timely and appropriate sharing of information. Practitioners must understand ***when*** to share information*;*

what information to share; ***how much*** information to share*;* ***who*** to share the information with and ***the way in which*** the information should be shared. Practitioners must also understand the possible adverse consequences ***of not*** sharing information.

2.3 *Proportionate* information sharing can ensure that adults get the right help; at the right time; from the right people; when they need it and for as long as they need it.

2.4 All practitioners must be alert to the signs of harm. Harm can present in many ways; some may be obvious and others difficult to spot. Harm need not have taken place *before* practitioners initiate an appropriate response – it is sufficient to have identified a *likelihood* or *probability* of risk.

2.5 Any practitioner who, in their *professional judgment*, is worried or concerned about the *welfare* of, or *risks* to, a vulnerable adult **must** take action:

- ***doing nothing is not an option***
- *do not assume someone else will do something*
- *do not delay unnecessarily – act quickly*
- *keep focused on the individual*
- *adopt a common sense approach*
- *if in any doubt, speak to a colleague, line manager or supervisor.*

2.6 **Practitioners, who are worried or concerned about the care or protection of an adult at risk, must in the first instance, follow the procedures in their own service / agency. They must share and discuss that worry or concern with their immediate Line Manager.**

2.7 In their absence, practitioners should discuss their worries or concern with an alternative Manager. Additional advice can be obtained by contacting the local duty team. Advice can also be sought from individual service / agency Legal Services Departments.

2.8 Legislation underpinning information sharing includes the General Data Protection Regulation (GDPR); The Data Protection Act 2018; The Human Rights Act 1998 and the European Convention on Human Rights (ECHR). ***This legislation supports lawful information processing, which includes information sharing and should not be seen as a barrier.***

2.9 GDPR describes the *six data protection principles* which must underpin day-to-day practice. There is a further overarching principle of *demonstrable compliance*, which similarly must be adhered to. Practitioners must understand these *principles*. If in doubt, practitioners must consult with their Line Managers.

2.10 ***What are the six data protection principles?***

2.11 Practitioners must ensure information is:

- *processed lawfully, fairly and in a transparent manner* (processing includes *gathering; recording; sharing; holding; changing; deleting; using; filing and destroying*)
- collected for *specified, explicit* and *legitimate* purposes and not further processed in a manner 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 personal data.

2.12 *Please remember, the overarching principle that the Data Controller is responsible for demonstrating compliance with these six data protection principles.*

2.13 The key principle to consider when sharing information for the purposes of ***safeguarding, supporting*** and ***promoting*** the *welfare* of adults at risk is the first principle: that is that information must be *processed lawfully, fairly and in a transparent manner*.

2.14 Information will be considered to have been processed in accordance with this principle when:

- in relation to ***personal data***, at least one of the legal bases in Article 6 of the GDPR has been met; and
- in respect of ***special category data***, at least one of the legal bases in Article 6 has been met, **plus** at least one of the legal bases is Article 9 of the GDPR is met.

2.15 Practitioners therefore need to understand what the lawful bases in each of the Articles are and how they can be applied to each particular situation.

2.16 ***What do we mean by personal data and special category data?***

Personal Data[1] *means any information whatsoever which can directly, or indirectly, identify a living person.*

Special Category Data[2] *means any personal data revealing the racial or ethnic origin of a person; their political opinions; their religious or philosophical beliefs; their trade union membership or affiliation; their genetic or biometric data; their physical or mental health; their sexual persuasion or sex life.*

2.17 ***What are the lawful data processing bases and how do they work?***

[1] Personal data as defined in the General Data Protection Regulation Article 4(1)
[2] Special Category Data as defined in General Data Protection Regulation Article 9

2.18 GDPR describes (in full) the lawful bases (Article 6 and Article 9) for processing ***personal data*** and ***special category data***. The first basis described, in both Articles, is that the individual gives consent to their information being processed.

2.19 Whilst this is the first basis described, it may be likely that consent will not necessary in the context of protection investigations, where the seeking of consent could undermine the process and consequently one of the other lawful bases should be considered. The other bases all require that the processing is *necessary* for a specific purpose (this is known as the *"necessity test"*).

2.20 In terms of processing information to ***safeguard, support*** and ***promote*** the *welfare* of adults who may be at risk, the following bases are considered to be the most relevant for practice:

Article 6 ***Bases (personal data)***	
Legal obligation	The sharing or other processing of ***personal data*** is necessary to comply with any legal obligation (duty) which the practitioner / service / agency is subject to.
Task carried out in the public interest or in exercise of official authority	The sharing or other processing of ***personal data*** is necessary for a task carried out in the public interest or to carry out a function where there is a statutory power to do so. The first part would apply where a practitioner / service / agency is not bound by any specific duty or legal obligation, but has relevant information which would help another service / agency to fulfil its statutory functions and it would be in the public interest to do so. For example, a voluntary organisation sharing personal information with the local authority to help them in a protection investigation. The second part would apply where services / agencies have a statutory power to meet needs and to protect and promote the welfare of adults at risk.
Vital interests	The sharing or other processing of ***personal data*** is *necessary* to protect the life and limb of the data subject or other person. If no other condition can be satisfied, this could be applied to cases where there is a ***real risk of significant harm to an individual****.*
Consent	When the individual has freely given, a specific, informed and unambiguous indication of their wishes by a statement or by a clear affirmative action which signifies agreement to the processing of their ***personal data***. **See Section 4 on Consent.**

Article 9 ***Bases (special category data)***	
Substantial Public Interest	The processing of ***special category data*** is ***necessary*** to carry out the obligations of social protection law (DPA 2018 Schedule 1, Part 1, Section 1).

	This would include statutory duties on services / agencies to assess and meet needs and to protect and promote the welfare of adults at risk.
Health and Social Care purposes	The processing of ***special category data*** is undertaken by a health professional and is necessary for the provision of health purposes; including preventative medicine and medical diagnosis; or undertaken by a social work professional and is necessary for the provision of social care purposes or social protection.
Vital interests	The sharing of ***special category data*** is *necessary* to protect life and limb of the data subject or other person. If no other condition can be satisfied, this could be applied to cases where there is a ***real risk of significant harm to an individual*** and where consent *cannot* physically or legally be given.
Explicit consent	When the individual has given their ***explicit consent*** to the processing of their ***special category data*** *for one or more specified purposes*. **See Section 4 on Consent.**

2.21 Practitioners must always exercise *professional judgement* and *common sense* when sharing information. They must understand what bases they are relying upon when sharing information and must only share the *necessary* information *proportionately*.

2.22 Practitioners must always have due regard to Article 8 ECHR (right to respect for private and family life) and this will ensure their practice is compliant with both the GDPR and the DPA.

2.23 Article 8 ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence. However, this right is not absolute and the Convention permits interference if it is:

- lawful
- necessary and proportionate and
- for one or more of the following legitimate aims:
    - the interests of national security
    - the interests of public safety or the economic well-being of the country
    - the prevention of disorder or crime
    - the protection of health or morals or
    - the protection of the rights and freedoms of others.

2.24 For the purposes of ***safeguarding, supporting*** and ***promoting*** the *welfare* of adults at risk, practitioners can therefore act to limit that Article 8 ECHR right on the basis of either protecting the health or morals of an individual or protecting the

rights and freedoms of others. To test whether actions comply with the ECHR, practitioners should ask themselves the following questions:

- *Am I interfering with an Article 8 right?*
- *Is the action I propose to take lawful?*
- *Does the action pursue one of the legitimate aims?*
- *Is the action that I propose to take necessary to achieve that aim?*
- *Is the action proportionate? That is – am I doing only as much as I need to in order to achieve the aim?*

3. Confidentiality

3.1 ***How does confidentiality work?***

3.2 Practitioners must work within the limitations and constraints of confidentiality. Not all information is confidential. **Practitioners must never make that promise.**

3.3 Confidentiality ***does not apply*** where the matter is clearly one of protecting adults at risk.

3.4 Practitioners have a ***duty of care*** and are subject to a Common Law and Statutory Obligation of Confidence. Confidentiality is not an absolute right. It has long been established that *just cause, or excuse* and / or *acting in the public interest* are defences to any action for breach of confidence.

3.5 The GDPR and the DPA ***do not prevent the sharing of information.*** On the contrary, *professional judgment, common sense* and an understanding of the data protection principles *and* the lawful bases in Article 6 of the GDPR and Article 9 of the GDPR can empower and support practice.

3.6 Over-riding the *Duty of Confidentiality* owed, sharing information should only occur where practitioners can justify doing so in terms of the data protection principles and where they can identify with a lawful basis specified in *Article 6* and / or Article 9 of the GDPR.

4. Consent

4.1 ***How does consent work?***

4.2 ***Practitioners must clearly understand the limitations and constraints of consent.***

4.3 Previously, practitioners worked on the understanding that to process an individual's personal data, they would ask service users for their consent. **GDPR has introduced a fundamental change to this approach.**

4.4 **Consent is now likely to be the last lawful basis considered when looking to share information and in almost all circumstances there will be another lawful basis for processing. The difference between giving consent to processing (sharing) information (data) and agreeing (giving consent) to the provision of a service (s) must also be understood.**

4.5 **Consent *will never apply* where the matter is clearly one of protecting adults at risk. Seeking consent may not be appropriate as doing so may likely place the adult at further risk.**

4.6 **Consent is only applicable in circumstances where an individual has a real choice over the matter.** In other words, if you intend to carry out a process or action, regardless of whether consent is obtained, then consent should not be considered. There is no real choice for the data subject. An alternate lawful basis should be used.

4.7 It is recognised that developing and maintaining a good working relationship with adult at risk is crucial in front-line work and this is greatly assisted by clear communication with them. It is therefore still good practice to inform them of what you are going to be doing and explain the reasons why. This would normally include advising them, where appropriate, of who you will be sharing data with (e.g. it may not be appropriate if advising them would result in further harm to an adult at risk, or result in the loss of crucial evidence). This is not the same as seeking consent to share information, but simply being transparent in explaining what you are going to do. This may go some way in maintaining some form of working relationship between the practitioner and the adult at risk.

4.8 However, where no other lawful bases apply, consent should be sought. Seeking consent can be difficult and with it comes additional rights for the data subject (individual). Where consent is considered appropriate, practitioners must ensure the individual being asked to provide their consent fully understands that request and its extent.

4.9 ***Consent must be considered on a case-by-case basis***. Consent, when sought, must be ***freely given, specific, informed*** and ***unambiguous***:

- *Freely given* – the individual must have a real choice over the matter – if an action or process will be undertaken regardless of the individual's consent, then it cannot be said to be freely given
- *Specific* – it must relate to a particular action or purpose which is clearly distinguishable from other matters
- *Informed* – the individual must understand what is being asked of them
- *Unambiguous* – the individual must clearly indicate their wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of information relating to him or her.

4.10 Consent can take the form of a written statement, (including by electronic means) or an oral statement. However, consent in writing should be obtained wherever

possible so that it can be easily evidenced if subsequently challenged or questioned.

4.11 Consent and discussions relating to consent must always be recorded in service / agency case file notes and / or on agency databases. There is no legal requirement for a specific Consent Form. There is no recognition of Implied Consent in the current data protection regime. All discussions about consent must also be recorded, whether granted or not.

4.12 Remember, it has to be as easy to withdraw consent as it is to give consent. It also must be understood that information that was provided under consent has to be deleted when consent is withdrawn.

4.13 Consent to share personal data is a condition under Article 6 of the GDPR and with regard to the sharing of special category data requires an additional basis under Article 9 of the GDPR. Consent under Article 9 of the GDPR requires consent to be **explicit.** This means obtaining a written statement that clearly gives consent to particular processing for the specified purpose.

4.14 Practitioners should consult their Line Manager if there are any issues or doubts whatsoever about Consent. In their absence, practitioners should contact the local duty team. Advice can also be sought from service / agency Legal Services Departments. NHS Tayside staff can also seek advice through NHS Tayside's Information Governance / Caldicott Guardian, or via NHS Tayside's Child Protection Advice Line (per NHS Tayside Staffnet).

5. ICO: Scotland - Key Messages

5.1 *"It is very important that the practitioner uses all available information before they decide whether or not to share. Experience, professional instinct and other available information will all help with the decision making process as will anonymised discussions with colleagues about the case. If there is any doubt about the wellbeing of the adult at risk and the decision is to share, the Data Protection Act should not be viewed as a barrier to proportionate sharing". (ICO: Scotland 2013).*

5.2 *"The ICO's data sharing code recognises that obtaining consent for sharing information can be difficult. It should only be sought in circumstances where an individual has real choice over the matter, reflecting the need under Principle 1 of the DPA for processing to be fair to the individual concerned. For a professional to request consent from an individual whilst knowing that sharing will take place nonetheless, raises false expectations and endangers the client relationship". (ICO: Scotland 2016).*

6. Key Underpinning Legislation

The Social Work (Scotland) Act 1968

The Age of Legal Capacity (Scotland) Act 1991

The Human Rights Act 1998

The Freedom of Information (Scotland) Act 2002

The Data Protection Act 2018

General Data Protection Regulation

Adult Support and Protection (Scotland) Act 2007

7. Key Underpinning Policy Developments

United Nations Convention on the Rights of the Child (UNCRC)

European Convention on Human Rights (ECHR)

Common Law and Statutory Obligations of Confidence

Information Commissioner's Office: Data Protection: Data Sharing Code of Practice

8. Electronic Links to Tayside Multi-agency Guidance including Information Sharing

Protecting Adults in Dundee from Harm

What to do if you are concerned about an adult in Angus

Perth & Kinross - Adult support and protection