Sharing Information

There are times when we need to share information in order to make sure that a child gets the appropriate support. Sharing information openly, securely and appropriately is key in working together to support children to reach their potential and promote their wellbeing.

Why do we need to share information?

Organisations need to share information with the right people at the right time to:

- coordinate effective and efficient responses
- enable early interventions to prevent the escalation of risk
- prevent abuse and harm that may increase the need for care and support
- maintain and improve good practice in safeguarding children and helping families
- reveal patterns of abuse that were previously undetected and that could identify others at risk of abuse
- identify low-level concerns that may reveal children at risk of abuse
- help families to access the right kind of support to reduce risk and promote wellbeing
- help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour
- prevent death or serious harm
- reduce organisational risk and protect reputation

False perceptions about needing evidence or consent to share information

Some practitioners can be over-cautious about sharing personal information, particularly if it is against the wishes of the child or family concerned. They may also be mistaken about needing hard evidence or consent to share information. The risk of sharing information is often perceived as higher than it actually is. It is important that practitioners consider the risks of not sharing information when making decisions.

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. Furthermore, the law does not prevent the sharing of sensitive, personal information between organisations where the public interest served outweighs the public interest served by protecting confidentiality – for example, where a serious crime may be prevented.

The Data Protection (Jersey) Law 2018 (the “Data Protection Law”) enables the lawful sharing of information.

Legal basis for sharing

Organisations can only work together effectively to protect children if there is an exchange of relevant information between them. This has been recognised by the courts in Jersey (see **X v Minister for Health and Social Services [2015] JRC252).**

Any disclosure of personal information to others must always have regard to the law.

Law of confidentiality

Personal information about children and families is subject to the legal duty of confidence, and should not generally be disclosed without the consent of the subject.

When a child and family needs multi-agency support, the Lead Worker will be the first point of contact.

If the Lead Worker considers that the involvement of another agency is appropriate they will explain to the child (where appropriate) and their family why sharing information is needed as well as how and why it will be helpful.

However, the law permits the disclosure of confidential information where the public interest outweighs the duty of confidentiality. Such a public interest might relate to the proper administration of justice and to the prevention of wrongdoing. In R v Chief Constable of North Wales Police, ex parte Thorpe [1996] QB 396 Lord Bingham CJ considered that where a public body acquires information relating to a member of the public which is not generally available and is potentially damaging, the body ought not to disclose such information save for the purpose of and to the extent necessary for the performance of its public duty or enabling some other public body to perform its public duty.

There are restrictions on the sharing of information between organisations under the Data Protection Law and the Human Rights (Jersey) Law 2000. However, the sharing of information is not necessarily contrary to these Laws.

Data Protection (Jersey) Law 2018

The Data Protection Law requires via its six principles that personal information is obtained and processed fairly and lawfully; only collected in appropriate circumstances; is accurate, relevant and not held longer than necessary; and is kept securely.

The Data Protection Law allows for disclosure without the consent of the child or family in certain conditions, including where the processing is necessary for the administration of justice, the exercise of any functions conferred on any person by or under any enactment, the exercise of any functions of the Crown, the States or any public authority; or the exercise of any other functions of a public nature with a legal basis in Jersey law to which the controller is subject and exercised in the public interest by any person.

The exercise of functions of the States and functions of a public nature with a legal basis in Jersey law are underpinned by values and principles which apply across all aspects of working with children. They reflect the rights of children as expressed in the United Nations Convention on the Rights of the Child (1989) and they build on the principles set out in Jersey legislation. The principles noted below are reflected in legislation, standards, and procedures and include:

- Promoting the wellbeing of the individual child
- Keeping children safe
- Putting the child at the centre
- Taking a whole child approach
- Building on strengths and promoting resilience
- Promoting opportunities and valuing diversity

- Providing additional help which is appropriate, proportionate and timely
- Working in partnership with families
- Supporting informed choice
- Promoting the same values across all working relationships
- Co-ordinating help when needed
- Building a competent workforce to promote children's wellbeing

When disclosing personal information, many of the data protection issues surrounding disclosure can be avoided if the consent of the individual has been sought and obtained.

There are 3 types of consent:

1. **Implied Consent** – consent indicated by signs and actions or by a lack of objection, and is usually deemed to be sufficient for a single agency working with a family
2. **Informed Consent** – the family is given information and specifically asked to give consent for that information to be shared
3. **Explicit Consent** – the family is given the information to be shared and is also asked to sign to record their agreement for the information to be shared.

The general principle is that information will only be shared with the consent of the subject of the information. Consent must be freely given after the alternatives and consequences are made clear to the person from whom permission is being sought. If the data is classified as sensitive data the consent must be explicit. In any case the specific detail of the processing should be explained to the individual.

This should include:

- Precisely who is processing the data
- The particular types of data to be processed
- The purpose of the processing
- Any special aspects of the processing which may affect the individual e.g. disclosures
- The person/agencies to whom the information will be made available

In the absence of consent, the practitioner must balance the duty of care, the public duty of confidentiality and Human Rights of the individual against the need to prevent and detect crime and disorder, and serve the public interest, in order to make a positive decision whether or not to release the information.

Where consent of the individual is not sought, or is sought but withheld, there can still be an exchange of information where there is an overriding public interest or justification for doing so.

If informed consent has not been sought, or has been sought and withheld, the practitioner must consider if there is any other overriding factor for the justification for the disclosure. In making this decision the following should be considered:

- Is the disclosure necessary for the prevention or detection of crime, prevention of disorder, to protect public safety, or to protect the freedoms of others?
- Is the disclosure necessary for the protection of a child or a vulnerable adult?
- What risk is posed to others by this individual?
- What is the vulnerability of those who may be at risk?
- What will be the impact of the disclosure on the subject and on others?
- Is the disclosure proportionate to the intended aim?
- Is there an equally effective but less intrusive alternative means of achieving that aim?

Disclosure for Purpose of Protecting Children

Child protection enquiries, investigations and conferences can only be successful if practitioners share and exchange all relevant information. Those with such information must treat the information as confidential at all times, but ethical and statutory codes that cover confidentiality and data protection are not intended to prevent the exchange of information between different professional staff which has the purpose of ensuring the protection of children.

Sometimes concerns will arise within an agency as information comes to light about a child or family with whom the service already is in contact. Whilst practitioners should, in general, seek to discuss any concerns with the family and where possible seek their agreement to share the information with other agencies, this should not be done where this will place a child at risk of significant harm. For more information please go to: **http://jerseyscb.proceduresonline.com/chapters/p_info_sharing.html**

The Seven Golden Rules of Information Sharing provide a useful framework for all who work with children and young people when considering the need to share information.

1. Remember that the **Data Protection (Jersey) Law 2018** and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

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

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

4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.

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

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose[1].

[1] **Information sharing – Advice for practitioners providing safeguarding services to children, young people, parents and carers HM Government 2015**