Appendix 4

INFORMATION SHARING GUIDANCE – VULNERABLE ADULTS

Contents

---

1. Introduction

In Jersey, the legal framework relating to the protection of personal information is set out in:

- The Data Protection Authority (Jersey) Law 2018
- The Data Protection (Jersey) Law 2018
- The Human Rights (Jersey) Law 2000 ("HRL 2000"), which incorporates the European Convention on Human Rights ("ECHR") into Jersey law, including the Article 8 right to a private and family life

Information sharing agreements are being developed for each of the multi-agency groups concerned with Safeguarding children and adults at risk. These will be made available as they are completed on the **Safeguarding Partnership Board Website**.

2. The Data Protection (Jersey) Law 2018. (DPJL)

The DPJL is based around **six principles** of 'good information handling' (the Principles). These principles give people (the data subjects) specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

1. FAIR, LAWFUL and TRANSPARENT PROCESSING: Personal data are to be processed lawfully, fairly and in a transparent manner in relation to the data.

2. PURPOSE LIMITATION: Personal data must be collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes.

3. EXCESSIVE DATA COLLECTION: Personal data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. ACCURACY OF DATA: Personal data must be accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. STORAGE LIMITATION: Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

6. DATA SECURITY, INTEGRITY AND CONFIDENTIALITY: Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Key Points for Workers when Sharing Information

It is important that people remain confident that their personal information is kept safe and secure and that professionals maintain the privacy of the individual, whilst sharing information to deliver better services. It is therefore important that professionals share information appropriately as part of their day-to-day practice and do so confidently. Disclosure of any personal data must be bound to both common and statute law and professional ethics and codes of conduct. The data protection principles require that such information is obtained and processed fairly and lawfully; is only disclosed in appropriate circumstances and for the purpose(s) it was obtained; is accurate, relevant, and not held longer than necessary; and is kept securely. Each agency must be clear about their legal gateway to the proactive sharing of information.

Consent

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 persons/agencies to whom the information will be made available.

In the absence of consent, the professional 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.

If informed consent has not been sought, or has been sought and withheld, the professional 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 young person 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?

If consent is not sought, or is sought and not / partially obtained, the reasons for not seeking consent or otherwise breaching confidentiality must be recorded. The reasons must be explained to the subject as soon as this can be done without negating the purpose of the original information enquiry.

All agencies should seek advice from the partner that provided the original information. Any partner should ensure that all the principles of the Data Protection Law are adhered to and that the sharing of personal data is not processed in any manner incompatible with the purpose/s it was obtained for.

Good record keeping is an important part of the accountability of professionals to those who use their service. Clear and accurate records ensure that there is a documented account of an agency's or professional's involvement with an adult/child/family. To serve these purposes, records should use clear, straightforward language.

Retention
Any information shared must only be retained for as long as necessary for the purpose it was shared. Agencies will maintain appropriate retention schedules. This information must be kept and disposed of securely.

4. Government Guidance (UK)

"Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers" states*: (1)*

"This guidance has been updated to reflect the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (In Jersey the DPJL). This advice is for all frontline practitioners working with children, young people, parents and carers who have to make decisions about sharing personal information on a case-by-case basis. It might also be helpful for practitioners working with adults who are responsible for children who may be in need."

This guidance outlines 7 golden rules to sharing information and these are relevant to adults as well as children:

The seven golden rules to sharing information:

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 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, legal department or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis 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 clear of the basis upon which you are doing so. Where you do not 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.

5. Summary

All agencies have a responsibility to ensure that staff are aware of the current legislation and what it means in practice. It is important for staff to be encouraged to discuss any queries or

doubts about information sharing with colleagues, line managers or the information commissioner and/or legal team. Multi-disciplinary forums may also wish to discuss implications of sharing information in order to protect vulnerable people and make joint decisions, effectively recorded, outlining reasons for actions and the basis of the decisions.

Suggested reading/references

www.skillsforcare.org.uk

www.savelives.org.uk

Guidance notes – The Data Protection Principles, Data Protection (Jersey) Law 2018 (Office of the Information Commissioner)

(1) HM Government (UK) published July 2018