Appendix 2 – Information Sharing Protocol

Safeguarding Partnership Board

Information Sharing Protocol between Safeguarding Partnership Board members and their organisations

Document profile	
Document Status	Final
Short Title	Information Sharing Protocol
Document Purpose	To ensure best practice in information sharing between agencies represented on the SPBs
Target Audience	SPB Board members, Statutory departments and third sector agencies working to safeguard children and adults in Jersey
Author	Glenys Johnston, OBE, Independent chair
Publication Date	July 2019
Review Date	March 2022 or if any change is made to this protocol before this date
Approval Route	Safeguarding Partnership Boards
Contact details	safeguardingpartnershipboard@gov.je

This document has been reviewed by the Law Offices Department, and the Jersey Office of the Information Commissioner, Strategic, Policy, Performance and Population prior to completion.

Table of contents

EXECUTIVE SUMMARY

This protocol is intended to assist those involved in the information sharing of safeguarding information relating to adults and children. It serves to offer in depth information to inform and guide professionals in their decision-making process when considering the sharing of personal information. The Social Care Institute for Excellence (SCIE) highlights key messages for all professionals on information sharing, which are as follows:

- 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 served outweighs the public interest served by protecting confidentiality – for example, where a serious crime may be prevented.

- The Data Protection (Jersey) Law 2018 enables the lawful sharing of information

- There should be a local agreement or protocol in place setting out the processes and principles for sharing information between organisations.

- As long as it does not increase risk, practitioners should inform the person if they need to share their information without consent.

- The management interests of an organisation should not override the need to share information to safeguard adults at risk of abuse.

- Children of a sufficient age or understanding should be consulted, their parents and or carers should be asked for their consent unless this compromises the safeguarding and protection of children.

This protocol will also cover what to do in the event that a person does not consent to have their safeguarding information shared (Page 9).

1. INTRODUCTION

The Safeguarding Adults Partnership Board and The Safeguarding Children Partnership Board (hereafter referred to as the SPB's) have a number of specific roles to play in safeguarding and protecting children and adults. These are to:

1) co-ordinate what is done by each organisation participating in the Boards for the purposes of safeguarding and promoting the welfare of children and adults in Jersey;
2) promote understanding of the need and means to protect children and adults from harm; and
3) monitor and ensure the effectiveness of the safeguarding systems that are in place both within and between organisations in Jersey.

The SPB's are the multi-agency bodies responsible for advising the Government of Jersey on safeguarding issues concerning children or adults at risk. They ensures that arrangements are in place to enable services and professionals to work effectively together. This is set out in the Memorandum of Understanding 2019, to which this Protocol is appended.

The definitions in this Protocol are the same as set out in the Data Protection (Jersey) Law 2018 (the DPL) unless otherwise stated in this Protocol.

The DPL regulates the "processing" of "personal data". Personal data means any data relating to a data subject. A data subject is an identified or identifiable, living person who can be identified, directly or indirectly, by reference to an identifier. Processing of personal data includes anything which may be done to personal data, such as obtaining, holding, using, disclosing or destroying it. Therefore, the requirements of the DPL applies to the sharing of information with agencies on, or by the SPB's.

Under the DPL a person or organisation that determines the purposes for which, and the manner in which, any personal data are, or are to be, processed is a "controller". In relation to the SPB, the signatories to the MOU that supply and receive personal data to and from the SPB will be controllers in relation to the version of the data that they process for their own purposes. In respect of the personal data that the SPB's manage, the SPB is registered as a controller under notification number 57385.

2. THE PURPOSE OF THE INFORMATION SHARING PROTOCOL

This Protocol outlines the key principles of data sharing between member organisations and agencies (hereafter "members" – see section 5) of the SPB. Members agree to share information to ensure that the organisations and agencies they represent can individually and collectively safeguard and promote the welfare of children and adults at risk in Jersey.

This Protocol covers:

- Information Sharing between member agencies of the Safeguarding Partnership Boards for the purpose of Serious Case Reviews and audits
- Other information sharing as set out in the Memorandum of Understanding 2019

- Multi-Agency Procedures in the case of Child Deaths in Jersey
- Data sharing policies held by the individual member organisations and agencies which make up the SPB's

3. AIMS OF THIS PROTOCOL

1) To ensure that the members will comply with the requirements of DPL when sharing information for the purposes set out above and in the MOU, as detailed in the Schedules. (See Appendix 3)

2) By signing the MOU, each member agrees to abide by the principal provisions of this Protocol, having regard to the specific sharing activities set out in the relevant Schedules.

3) Each Schedule will specify the relevant members for defined purposes.

4) New Schedules may be added by the SPB's from time to time and members will be notified in writing of those additions (this will include electronic notification).

4. COMMITMENT OF SIGNATORIES

The signatories of the MOU subscribe to the following for this Protocol:

- the agreed standards must provide safeguards and an appropriate framework for the controlled exchange of relevant information;
- the Data Protection principles must be upheld;
- this Protocol to be reviewed every 3 years or following any change requested to the MOU or this Protocol;
- any member may request any change to the Protocol or Schedules at any time by submitting to the Protocol holder a suggested revision; any changes to the Protocol or Schedules to be discussed and agreed by the SPB;
- any member can at any time notify the Protocol holder in writing that a Schedule cease to/not apply to them
- the nominated holder of this Protocol is the SPB Board Manager

5. THE SIGNATORIES (MEMBERS)

This Protocol is between the organisations and agencies which form the SPB and are signatories of the SPB MOU 2019 namely:

Government of Jersey departments: Strategic Policy Performance and Population, Health and Community Services (H&CS), Customer and Local Services, Children Young People Education and Skills (CYPE&S), Primary Care, Prison Service, Customs and Immigration, Growth, Housing and Environment Department

Law Officers' Department

States of Jersey Police

Probation and Aftercare Service

Honorary Police

GP's

Jersey Employment Trust (JET)

NSPCC

Family Nursing and Home Care (FNHC)

Community voluntary sector representatives

Associate and lay members

6. DATA PROTECTION PRINCIPLES

In entering into the MOU and this Protocol, the members have carefully considered the requirements of the six Data Protection Principles (the "DP Principles") as set out in Article 8 of the DPL. The members agree that they have complied with and will continue to comply with the DP Principles in respect of the processing of the personal data.

7. SPB DATA PROCESSING

Personal data

The SPB will process Personal Data in accordance with all applicable laws and applicable contractual obligations.

Personal data is information that relates to any living person that can be identified from that data. They do not have to be named, simply identifiable.

Examples of personal data:

- name
- address
- date of birth
- initials
- social security number
- photographs
- payslips
- CCTV footage
- social media posts
- an unnamed photo

Even if something does not look like personal data at first (such as an IP address or an address), if it is combined with other data that can identify a person, then it can be labelled as personal data too.

The SPB's will process data in accordance with DP Principles and the processing conditions set out in Schedule 2 of the DPL. Notwithstanding the generality of this Protocol, the legal basis and relevant processing condition for sharing will be further detailed on a case-by-case basis in the Schedules.

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. The SPB will at all times act in accordance with Article 13 DPL and guidance will be sought from the Data Protection Advisor before any such processing may commence.

Special Category data

Previously known as sensitive personal data, special category data is personal data but of a higher level of sensitivity. Specific rules apply to the way this data is processed.

Special category data is defined as data that reveals information about a person's:

- health
- sex life or sexual orientation
- criminal record or alleged criminal activity
- racial or ethnic origin
- political opinions, religious or philosophical beliefs
- trade union membership
- genetic or biometric data
- criminal or alleged criminal activity

The SPB's will only process special category data where one of the processing conditions in Part 2 of Schedule 2 of the DPL apply.

Law Enforcement Requests and Disclosures

The DPL recognises that in certain circumstances personal data can be shared for a Law Enforcement purpose, as set out in the modified provisions of Schedule 1 of the DPL. In such cases (in the absence of consent) disclosure of personal data is permitted if it is necessary for the performance of a task carried out by a controller for a law enforcement purpose:

> "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public security"

If the SPB processes special category data (which does not relate to a person's criminal record or an alleged criminal activity) for a Law Enforcement purpose then it will do so in accordance with the modified Article 9 in Schedule 1, sub-sections (2) – (4) of the DPL.

8. DATA ITEMS TO BE SHARED (SHARED DATA)

Neither the General Data Protection Regulation (GDPR) nor the Data Protection (Jersey) Law 2018 prevent, or limit, the sharing of information for the purposes of keeping children, young people and adults safe. They put a greater emphasis on organisations being transparent and accountable.

In the course of its work the members agree to share on an ad-hoc basis information pertaining to children and / or adults at risk and to organisational procedures and processes designed to address their needs. Data shared may therefore be personally or commercially sensitive and may include such details as:-

- age;
- gender;
- information about health conditions and / or treatment
- departmental processes;
- financial details;
- correspondence.

Any data that is to be shared for a routine or specific and defined purpose is set out in the Schedules to this Protocol (the "Shared Data"). Only the relevant information for those purposes will be shared as detailed in the Schedules and will be limited to what is necessary and proportionate for the SPB to fulfil its function in safeguarding children and adults.

9. THE IMPORTANCE OF SHARING INFORMATION

Children

Under the MOU, the members of the SPBs work to the information sharing guidelines of the English statutory guidance - **Working Together to Safeguard Children 2015:**

- *22. Effective sharing of information between professionals and local agencies is essential for the effective identification, assessment and service provision.*

- *23. Early sharing of information is the key to providing effective early help where there are emerging concerns. At the other end of the continuum, sharing information can be essential to put in place effective child protection services. Serious Case Reviews have shown how poor information sharing has contributed to the deaths or serious injuries of children*

- *24. Fears about sharing information cannot be allowed to stand in the way of the need to promote the welfare and protect the safety of children. To ensure effective safeguarding arrangements:*
    - *all organisations should have arrangements in place which set out clearly the processes and the principles for sharing information between each other, with other professionals and with the LSCB; and*
    - *no professional should assume that someone else will pass on information which they think may be critical to keeping a child safe. If a professional has concerns about a child's welfare and believes they are suffering or likely to*

suffer harm, then they should share the information with Jersey children's social care.

and also to the **seven golden rules** in ***Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (2018*)**:

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, 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.*

Additional guidance for sharing information about children

Duty of Confidence

In Jersey a duty of confidence will arise where a person receives information that has the necessary quality of confidence about it in circumstances that expressly or impliedly gives rise to an expectation that the information will be kept confidential. Much of the information that will

be shared with or held in the Children's Multi-Agency Safeguarding Hub (MASH) will be subject to a duty of confidence owed to the subjects of that information.

Where a duty of confidence arises, it will usually be unlawful to disclose the information subject to that duty to a third party. However, the existence of a duty of confidence is not an absolute bar on the disclosure. Confidential information can be lawfully disclosed where the person to whom the duty is owed has given their informed consent. Further, even where it is not possible or appropriate to obtain consent to disclose, it may still be possible to share the information lawfully where there is either an overriding public interest in disclosure or sharing is required by a court order or other legal obligation.

Adults

Sharing information concerning **adults** at risk differs mainly due to the issue of consent, however, it is equally important to share relevant information in order to;

- prevent death or serious harm to others;
- coordinate effective and efficient responses;
- enable early interventions to prevent the escalation of risk;
- prevent abuse and harm that may increase the need for care and support;
- maintain and improve good practice in safeguarding adults and children;
- reveal patterns of abuse that were previously undetected and that could identify others at risk of abuse;
- identify low-level concerns that may reveal people at risk of abuse;
- help people to access the right kind of support to reduce risk and promote wellbeing;
- help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour;
- reduce organisational risk and protect reputation;[6]
- Jersey's SPBs provide multi-agency training on information sharing, it has a key role in supporting information sharing between and within organisations and addressing any barriers to this

(This is a non-exhaustive list)

Additional guidance for sharing information about adults

Investigating, assessing and responding to safeguarding concerns relating to adults at risk and children are multi-disciplinary, joint agency activities. They depend on the selective sharing of personal information, which is normally confidential.

For some purposes, it might be sufficient to share anonymised information or share statistical information derived from performing a particular service, to identify the ways that organisations can best work together. Consideration should always be given to the sharing of anonymised or statistical information first where personal information is not required to fulfil the purpose.

[6] Social Care Institute for Excellent (SCIE) https://www.scie.org.uk/adults/safeguarding/

However, in other cases, in order to deliver the best safeguarding decisions which ensure timely, necessary and proportionate interventions, decision makers need the full picture about a particular individual and can only obtain this through appropriate information sharing.

This paragraph is intended to help professionals and public officials by summarising the main legal principles applicable to the exchange of personal information. It is not intended as a substitute for legal advice and where there are doubts as to the propriety of sharing information in any specific case then further advice should be sought from the Law Officers' Department.

Public authorities should seek advice from the Law Officers' Department where they are proposing to do something novel or unusual with personal information.

There will be instances where public and voluntary agencies need to share personal information about a person without the person's consent in order to safeguard the person or others from harm. In those instances, those agencies proposing to share personal information must satisfy themselves, in each case, that it is necessary to share information in the public interest. In any such case it will be vital to ensure that the amount of information shared is proportionate to the purpose.

The Social Care Institute for Excellence (SCIE) gives the following guidance for information sharing about adults at risk:

Key messages

- *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 served outweighs the public interest served by protecting confidentiality – for example, where a serious crime may be prevented.*
- *The Data Protection (Jersey) Law 2018 enables the lawful sharing of information*
- *There should be a local agreement or protocol in place setting out the processes and principles for sharing information between organisations.*
- *It is good practice to try to gain the person's consent to share information.*
- *As long as it does not increase risk, practitioners should inform the person if they need to share their information without consent.*
- *The management interests of an organisation should not override the need to share information to safeguard adults at risk of abuse.*

What if an adult does not want you to share their information?

Frontline workers and volunteers should always share safeguarding concerns in line with their organisation's policy, and their line manager, data protection or safeguarding lead in the first instance, except in emergency situations. As long as it does not increase the risk to the individual,

the member of staff should explain to them that it is their duty to share their concern with their manager. The safeguarding principle of proportionality should underpin decisions about sharing information without consent, and decisions should be on a case-by-case basis.

Individuals may not give their consent to the sharing of safeguarding information for a number of reasons. For example, they may be frightened of reprisals, they may fear losing control, they may not trust social services or other partners or they may fear that their relationship with the abuser will be damaged. In the absence of consent, professionals must balance the duty of care, the public duty of confidentiality and the 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. Reassurance and appropriate support along with gentle persuasion may help to change their view on whether it is best to share information.

If a person refuses intervention to support them with a safeguarding concern, or requests that information about them is not shared with other safeguarding partners, their wishes should be respected.

However, there are a number of circumstances where the practitioner can reasonably override such a decision, including:

- the person lacks the mental capacity to make that decision – see Capacity and Self-Determination (Jersey) Law 2016
- other people are, or may be, at risk, including children
- sharing the information could prevent a crime
- the alleged abuser has care and support needs and may also be at risk
- a serious crime has been committed or alleged to have been committed
- staff are implicated
- the person has the mental capacity to make that decision but they may be under duress or being coerced
- the risk is unreasonably high and meets the criteria for a multi-agency risk assessment conference
- a court order or other legal authority has requested the information

If none of the above apply and the decision is not to share safeguarding information with other safeguarding partners, or not to intervene to safeguard the person:

- support the person to weigh up the risks and benefits of different options
- ensure they are aware of the level of risk and possible outcomes
- offer to arrange for them to have an advocate or peer supporter
- offer support for them to build confidence and self-esteem if necessary
- agree on and record the level of risk the person is taking
- record the reasons for not intervening or sharing information
- regularly review the situation
- try to build trust and use gentle persuasion to enable the person to better protect themselves.

If it is necessary to share information outside the organisation:

- explore the reasons for the person's objections – what are they worried about?
- explain the concern and why you think it is important to share the information

- tell the person who you would like to share the information with and why
- explain the benefits, to them or others, of sharing information – could they access better help and support?
- discuss the consequences of not sharing the information – could someone come to harm?
- reassure them that the information will not be shared with anyone who does not need to know
- reassure them that they are not alone and that support is available to them.

If the person cannot be persuaded to give their consent then, unless it is considered dangerous to do so, it should be explained to them that the information will be shared without consent. The reasons should be given and recorded.

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

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

Multi-agency working to safeguard children from harm or adults at risk, is often complex and means that from time to time the judgment of staff from different professional backgrounds may differ, causing potential conflict. In the event of a professional disagreement in relation to the safeguarding needs of children or adults the Safeguarding Partnership Boards' Escalation and Professional Resolution Policy should be followed.

Sharing information with carers, family or friends

It is good practice, unless there are clear reasons for not doing so, to work with the carers, family and friends of an individual to help them to get the care and support they need. Sharing information with these people should always be with the consent of the individual. If the person lacks the mental capacity to make decisions about sharing information with key people, then the Capacity and Self-Determination (Jersey) Law 2016 should be followed to ensure each decision to share information is in the person's best interests. Decisions and reasoning should always be recorded.

What if a safeguarding partner is reluctant to share information?

There are only a limited number of circumstances where it would be acceptable not to share information pertinent to safeguarding with relevant safeguarding partners. These would be, as outlined above, where the person involved has the mental capacity to make the decision and makes it clear they do not want their information shared and the circumstances where the practitioner can reasonably override such a decision as set out above apply.

10. LEGAL BASIS FOR SHARING

Whilst unlike some other jurisdictions the Jersey SPBs are not statutory bodies and Jersey does not have an equivalent to the following:

- section 10 of the Children Act (UK) (2004) - statutory duty to co-operate with each other in the safeguarding and promoting the welfare of children;
- the functions of the Local Safeguarding Children Board (LSCB) under section 14 of the Children Act (UK) (2004) - each LSCB member agency to co-operate with the LSCB
- The Care Act 2014 – Safeguarding Adults Board
- The Safeguarding Partnership Boards need to seek co-operation and collaboration from their member agencies in implementing their strategic plan.

However, Jersey does have legislation on Capacity and self-determination (Capacity and Self-Determination (Jersey) Law 2016) and protecting Children (Children (Jersey) Law 2002).

Children (Jersey) Law 2002

An express power to share information arises from Article 42 of the 2002 Law, which creates an obligation for the minister to make enquiries where he or she is informed that a child is the subject of an emergency protection order or is in Police protection, or where the relevant minister has reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm. In such circumstances the minister is required to make or cause to be made, such enquiries as the minister considers necessary to enable the minister to decide whether he or she should take any action to safeguard or promote the child's welfare. Where the minister is conducting enquiries under this Article, it is the duty of any administration of the States to assist the minister with his or her enquiries (in particular by providing relevant information and advice) if called upon by the minister to do so, unless it would be unreasonable to do so in all the circumstances of the case.

Article 42 is a potential source of powers for both the Children's Service (which exercises these functions on behalf of the Minister for Children) and all other administrations of the Government of Jersey responding to enquiries from the Children's Service, to share personal data.

Implied powers for the minister (and their officials) to share information may arise from several functions under the 2002 Law, particularly those functions in Part 3, which contain provisions concerning ministerial support for children and families. For example, Article 17 of the 2002 Law contains obligations for the minister to provide accommodation to any child in need who appears to the minister to require accommodation. Article 24 of the 2002 Law makes provision for the minister to apply for a care order or supervision order where he or she is satisfied of certain matters. It is considered that information sharing is necessary in order for the minister to fulfil these duties and functions.

Express and Implied powers for the police to share information arise from Article 41 of the 2002 Law which empowers a police officer, who has reasonable cause to believe that a child would otherwise be likely to suffer significant harm, to take the child into Police protection.

Without limiting the generality of the above, it may be necessary to process personal data in accordance with some of the following (non-exhaustive) list of laws:-

- Mental Health (Jersey) Law 2016
- Children's (Jersey) Law 2002
- Discrimination (Jersey) Law 2013

- Human Rights (Jersey) Law 2000
- The customary law duty of confidentiality
- Capacity and Self Determination (Jersey) Law 2016
- Freedom of Information (Jersey) Law 2011
- Sexual Offences (Jersey) Law 2018
- Criminal Offences (Jersey) Law 2009
- Police Procedure & Criminal Evidence (Jersey) Law 2003
- Nursing Agencies (Jersey) Law 1978
- Nursing and Residential Homes (Jersey) Law 1994

11. PROCESSING CONDITIONS

The members will process data in accordance with the processing conditions set out in Schedule 2 of the DPL. The relevant processing condition will be detailed on a case-by-case basis in the Schedules to this Protocol.

Notwithstanding the generality of the above, whilst sections 3.12 to 3.15 of the MOU deals with information sharing generally, the MOU also sets out the functions of the SPB. The SPB is a public authority for the purposes of the DPL and in addition to any statutory legal basis for sharing (express or implied), the SPB can also rely on paragraph 4(c) of Schedule 2 to the DPL in respect of personal data and paragraph 13(c) of Schedule 2 to the DPL in respect of special category data in order to process data in pursuance of its public functions.

12. ACCESS AND INDIVIDUALS' RIGHTS

Freedom of Information

Whilst the SPB's are not a Scheduled Public Authority (SPA) under Schedule 1 to the Freedom of Information (Jersey) Law 2011 (FOI Law) because partnership arrangements like those of the SPB's do not have the legal status of a body or organisation separate to the individual members, by virtue of the fact that some members are SPA's, means the information held may be subject to the FOI Law. In addition, in agreeing to co-operate to achieve a common goal they create an organisational structure of their own in which information sharing is a key part.

For this reason all Freedom of Information Requests will be considered and dealt with on an individual basis and should be directed to FOI@gov.je in the first instance.

Subject Rights Request

Each member is a controller in relation to the version of the data that they process for their own purposes. In respect of the personal data that the SPB's manages, the SPB's are the controller. Each member is therefore responsible for handling any subject rights requests that are made to them directly and are responsible for dealing with general data protection queries and complaints received from members of the public.

However, in respect of Government of Jersey departments all Subject Rights Requests should be directed to sar@gov.je in the first instance.

13. SECURITY AND CONFIDENTIALITY OF THE SHARED DATA

The SPB's will treat the shared data as confidential. It will be kept secure through the Government of Jersey security system. The employees who will have access to such data will comply with the Government of Jersey securities policies.

14. DATA QUALITY

Data quality is a perception or an assessment of data's fitness to serve its purpose in a given context. Aspects of data quality include (but are not limited to): accuracy; completeness; status; consistency; reliability; accessibility. The members agree data quality is crucial to operational and transactional processes. Where applicable, before sharing data pursuant to this Protocol, the controller will check that the data is accurate and up-to-date to the best of their knowledge. Where special category data is being processed which could harm the data subject if it was inaccurate, particular care must be taken to ensure the quality of the data.

15. DATA BREACHES

In the event that data shared with the SPB's is subject to a "*personal data breach*" (as defined in Article 1 (1) of the DPL), the SPB's will be responsible for escalating this through the Government of Jersey security incidents reporting system, in accordance with the Government of Jersey data breach process. Notification of the incident can be made via email, by telephone or in person. The SPB's will be responsible for informing the other relevant members of the data breach as soon as possible. Members remain responsible, as controllers, for the version of the data that they process for their own purposes and will manage any person data breach in accordance with their own processors.

16. DATA RETENTION

Personal data must not be retained for longer than is necessary for its lawful purpose. Each agency is responsible for maintaining and publishing their own retention schedules. The SPB's will retain information in accordance with the guidance of Jersey Archive. The SPB's will gather, retain and dispose of any personal data in accordance with the Government of Jersey information sharing Policies.

17. AUDITS AND INSPECTIONS OF THE SHARED DATA

A) The members shall make available to each other all information necessary to demonstrate compliance with the obligations laid down in this Protocol and allow for and contribute to audits, including inspections, conducted by the other member or another auditor mandated by the relevant member as set out below.

B) Upon a relevant member's reasonable request, the other members agree to provide that member with any documentation or records which will enable it to verify and monitor that member's compliance with its data protection and security obligations under the

terms of this Protocol, within 14 days of receipt of such request, and to notify the relevant member of the relevant person who will act as the point of contact for provision of the information required. For this purpose, a member may present up-to-date attestations, reports or extracts thereof from independent bodies (e.g. External auditors, internal audit, the data protection officer, the I.T. security department or quality auditors) or suitable certification by way of an I.T. security or data protection audit.

C) Where, in the reasonable opinion of either member, such documentation is not sufficient in order to meet the obligations of the law, either member will be entitled, upon reasonable prior written notice to the other member and upon reasonable grounds, to conduct an on-site audit of the other member's premises used (save for domestic premises), solely to confirm compliance with its data protection and security obligations under this Protocol.

D) Any audit carried out a member will be conducted in a manner that does not disrupt, delay or interfere with the other member's performance of its business. The member shall ensure that the individuals carrying out an audit are under the same confidentiality obligations as set out in this agreement.

18. REVIEW ARRANGEMENTS

This Protocol will be reviewed every three years or following any change requested to the MOU or this Protocol. The instigation of the review process will be the responsibility of the SPB. This agreement will also be reviewed in the event of significant changes to any of the following:

I) the data sharing process;

Ii) the use of the shared data by a member;

Iii) data security arrangements; or

Iv) jersey data protection legislation.

19. THIRD COUNTRY DATA TRANSFERS

The SPB's will not transfer the shared data to third countries or jurisdictions without an explicit MOU.

20. RESOURCES

HM Government Information Sharing: Guidance for practitioners and managers

ICO Data Sharing Code of Practice

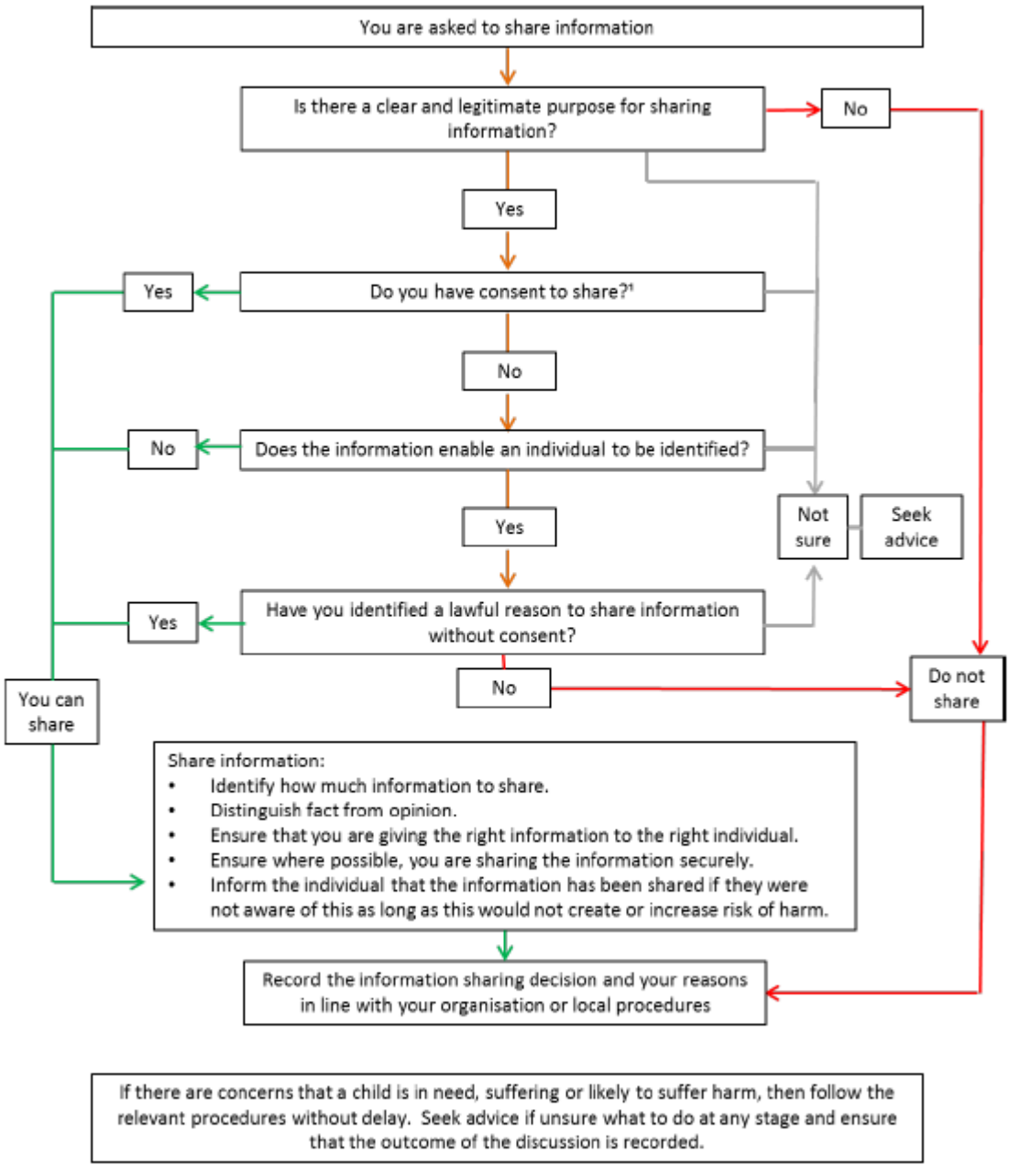
Working together to Safeguard Children 2015 in England

Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (2015)

Social Care Institute for Excellence (SCIE)

Data Protection (Jersey) Law 2018

Flowchart of when and how to share information



1. Consent must be unambiguous, freely given and may be withdrawn at any time

Appendix 3

The Information Sharing Protocol outlines that specific sharing for a defined purpose will be set out in a Schedule. The protocol instructs that the Safeguarding Partnership Boards will notify members of a Schedule and that once notified (in writing or electronically) the member that has been notified will be subject to it unless they have opted-out. With regards to audits, the Schedule should be used for each audit as it can be very specific to the data being shared; who is sharing the data with the Safeguarding Partnership Board and on what legal basis this information is being shared.

Schedule 1 – Processing of personal data for the purpose of [name audit, project etc]

1. COMMENCEMENT DATE

This Schedule 1 shall take effect from the date the member was notified in writing of this Schedule 1.

2. PARTIES TO SCHEDULE 1

All signatories to the MOU that have been notified of this Schedule and have not advised the Protocol holder they have opted-out.

3. AIM OF THIS SCHEDULE

To ensure that the members comply with the requirements of DPL during the course of the Safeguarding Partnership Boards' audits. [insert name of audit, project type etc]

4. DATA TO BE PROCESSED

The purpose for processing personal data for the Safeguarding Partnership Boards' multi-agency audits [insert name of audit] and Serious Case Reviews [insert name of Serious Case Review] and other audits and reviews, may involve the processing of both personal and special category data:

a. The administrative records kept by members, which entails the processing of the following types of data:

    i) name;
    ii) address;
    iii) telephone number;
    iv) place of birth
    v) nationality
    vi) financial information;

b. The sensitive records of families, which entails the processing of the following types of data:

    i) sexual orientation;
    ii) alleged criminal offence;

iii) medical information;

The personal data will be limited to only data which is strictly necessary for the SPB to enable them to achieve its objectives.

5. LEGAL BASIS FOR DATA PROCESSING

a) In accordance with clause 10 of the Protocol, the legal basis for the SPB to process the personal data is the MOU.

6. PROCESSING CONDITIONS

a) Personal data is processed in accordance with the following processing conditions:

i) Schedule 2, Part 1, Paragraph (4) of the DPL, which permits the processing of personal data by public authorities, when performing public functions; and

ii) Schedule 2, Part 2, Paragraph (13) of the DP18, which permits the processing of special category data by public authorities, when performing public functions.

7. DURATION OF PROCESSING

Processing of the personal data will continue for up to 6 months after completion of the audit report. After which time the information will either be returned to the members, or if copies were provided, the copies will be securely disposed.

8. PURPOSE AND NATURE OF DATA PROCESSING

a) As part of the SPB functions set out in the MOU, the SPB have a number of specific roles to play in safeguarding and protecting children and adults. One of these is to monitor and ensure the effectiveness of the safeguarding systems that are in place both within and between organisations in Jersey.

b) As part of its role in monitoring the effectiveness of what is done collectively and individually by organisations to protect children and adults, the Safeguarding Partnership Boards will:

i) Ensure that investigations into allegations concerning persons who work with children are carried out effectively;

ii) Periodically audit inter-agency practice, focusing on compliance with the multi-agency procedures, the quality of service and the views of service users;

iii) Monitor the arrangements (including recruitment and training policies) made by the Government of Jersey and voluntary and private agencies to ensure that the children and adults to whom they provide services, are protected and safeguarded;

iv) Operate a multi-agency complaints procedure so that persons who have been subject of, or affected by, a protection or abuse enquiry can make a formal complaint, or

express dissatisfaction where they have concerns about how agencies have been working together to safeguard a child or adult;

v) Actively seek feedback from adults and children who are in receipt of child or adult protection services or have experience of how the procedures and guidelines work in practice, so that their opinions can be taken into account when evaluating and further developing guidelines and procedures;

vi) Participate in the planning of services for children and adults in Jersey; and

vii) Undertake Serious Case Reviews, advise the individuals and organisations involved on lessons to be learned and monitor the implementation of recommendations (see section 4.1 MOU).