DUMFRIES & GALLOWAY
PUBLIC PROTECTION COMMITTEE

Information Sharing - A 10 Step Guide
Safeguarding Children/ Child Protection

Management Information	
Responsible Manager	Public Protection Committee
Author	Name: Clare Cowan
	Designation: Lead Officer Child Protection
Date Agreed	19/03/2024
Agreed by	Policy & Procedure Sub-Committee
Implementation Date	26/03/2024
Last Review Date	19/03/2024
Next Review Date	19/03/2026

Version Control			
Version	Date	Author	Comment
1.1	19/03/2024	Clare Cowan	
1.2	11/06/2025	Cheryl Copeland	Revised link

Table of Contents

1. Information Sharing in Scotland

1.1. **The National Guidance for Child Protection in Scotland, 2021 (Updated 2023) states that Sharing relevant information is an essential part of protecting children from harm. Practitioners and managers in statutory services and the voluntary sector should all understand when and how they may share information**.

1.2. Practitioners must be supported and guided in working within and applying the law through organisational procedures and supervisory processes. Within agencies, data controllers and information governance/ data protection leads should ensure that the systems and procedures for which they share accountability provide an effective framework for lawful, fair, and transparent information sharing. Where there is a child protection concern, relevant information should be shared with police or social work without delay, provided it is necessary, proportionate, and lawful to do so.

GIRFEC Information Sharing Guidance

1.3. The guidance published in 2022 aims to clarify the circumstances in which information can be shared with another agency, the considerations that need to be taken into account to ensure sharing information with another agency is appropriate, and the importance of involving children, young people, and families in the decision to share information with another agency.

1.4. Please refer to the *GIRFEC Practice Guidance 4 – Information Sharing 2022*

2. A 10 Step Guide to Information Sharing to Safeguard Children

2.1. This 10-step guide from the Information Commissioners Officer (ICO) on data protection considerations when sharing personal information for child safeguarding/ child protection purposes. It aims to help you feel confident about sharing information when you need to safeguard and protect a child or young person at risk of harm.

2.2. **It does not tell you how to safeguard / protect children and young people** (this can be found in your child protection guidance)**, but it does give you practical advice on data protection as part of the safeguarding process.** The ICO's role is as the regulator of information rights, not of safeguarding practices.

2.3. Data protection law allows you to share information when required to identify children at risk of harm and to safeguard/ protect them from harm. Data protection law does not prevent you from doing this. It simply helps you to share information in a fair, proportionate and lawful way.

2.4. **It can be more harmful not to share information that is needed to protect a child or young person.**

2.5. Appropriate information sharing is central to effectively safeguarding/ protecting children from harm and promoting their wellbeing. There have been many reviews of cases where children have died or been seriously harmed through abuse or neglect. The case reviews frequently identify gaps

in information sharing as a factor contributing to failures to protect the children involved.

2.6. Data protection law has an enabling role, supporting you to share information.

3. Who is the Guidance for?

3.1. This short 10 Step Guide is aimed at people who are involved in safeguarding and protecting children: at all levels, and in all sectors in the UK.

3.2. Safeguarding children and child protection is everyone's responsibility – not just practitioners working in child protection. Sharing information to safeguard and protect children includes:

- preventing harm.
- promoting the welfare of a child; and
- identifying risk in order to prevent harm (especially helpful where the risk may not be obvious to a single person or organisation).

3.3. A number of organisations have their own definitions and advice on safeguarding and child protection.

3.4. In this short ICO guide (adapted to reflect language and systems in Scotland), the 'safeguarding of children' and references to children include children and young people up to the age of 18yrs. This relates specifically to children in receipt of children's services/ subject to a statutory supervision order; s83 Children's Hearing (Scotland) Act 2011.

3.5. NB: It is important that discussion takes place with adult services when a young person is in the process of transitioning to the support of adult services.

3.6. The information in this guide is important for people in a wide range of roles and organisations, such as:

- Senior leaders in organisations (they might not work directly with children on a day-to-day basis, although some have a legally defined role such as the Chief Social Work Officer in Scotland).
- Managers who hold key responsibilities for ensuring their staff share information appropriately and sit between senior leadership and people in front line practice.
- People who are designated safeguarding/ child protection leads and practitioners, as well as people who are less directly involved.
- Those who work or volunteer in smaller local organisations such as youth groups, arts groups, or sports teams, including the social sector.
- Those who work in the private sector, such as childminders, private schools, private day nurseries, and after school clubs; and
- Competent authorities, such as the police or certain other public bodies and specific officials, sharing personal information for law enforcement

purposes, who are subject to Part 3 of the Data Protection Act 2018 (DPA 2018).

3.7. Senior leaders should make sure everyone in their organisation has the required level of understanding of what to do to safeguard and protect children. The Dumfries and Galloway Public Protection Committee support this work. You can contact the Public Protection Team with any enquiries regarding this guidance by emailing: publicprotection@dumgal.gov.uk

4. The 10 Steps

Step 1 – Be Clear About How Data Protection Can Help You Share Information to Safeguard/ Protect a Child

4.1. The clear message from the ICO is that data protection is a framework to help you share information. It does not prevent you from sharing information to safeguard and protect a child. It can be more harmful not to share information that is needed to protect a child or young person.

4.2. We know that there can be challenges when you want to share information:

- Practical challenges, such as technological ones, or relating to systems and processes that are not effective or that are not compatible with other organisations you need to share information with.
- Challenges due to organisational culture or long-established practices, which can be difficult to change; and
- Misconceptions that you cannot share information 'due to data protection.' Yes, you can!

Following these steps will help you to overcome these.

4.3. Get advice from the data protection officer in your organisation when you have any concerns. They can support you when you need to share information.

4.4. There are other laws and duties outside data protection that you also have to comply with in your safeguarding/ child protection work. Some of those require you to share information in certain circumstances. Some sectors have particular requirements; for example, guidance for professionals laid down by UK regulators such as the General Medical Council, which cover things such as doctor-patient confidentiality. For those detailed requirements within your own organisation, make sure you adhere to agreed policies and obtain internal advice as needed.

4.5. **When you share information in good faith to help identify and safeguard/ protect a child you believe is at risk of harm, you will not get into trouble with the ICO. It will never breach UK data protection law to share all the information you need to with an appropriate person or authority in order to safeguard and protect a child or young person.**

4.6. You may find hearing about this in a one minute message directly from John Edwards, Information Commissioner for the UK helpful by clicking and scrolling via this link here:

Step 2 – Identify Your Objective for Sharing Information and Share the Information you Need to in Order to Safeguard and Protect a Child

4.7. Be clear about your purpose for sharing the information. Safeguarding/ protecting a child is a compelling reason for sharing information.

4.8. You can share all the information you need to, with an appropriate person or authority, in order to safeguard and protect a child.

How this works in practice

4.9. You are working with a child and have identified concerns about their welfare. You are going to share this information with an organisation who can help, and you want to know how much to share.

- You may be able to share a minimal amount of information to achieve your purpose, such as accessing direct support for a service to benefit the child. In this scenario, it is appropriate only to share this minimal information.
- However, there will be times where multiple organisations participate in an intervention, or where there are concerns about serious harm. In these cases, it may be necessary to share information more widely, or to share more information on a child's circumstances.

4.10. It is not always clear how the details of a child's history or circumstances are relevant to the concerns you have identified. But you will be sharing proportionately if you can link it back to a compelling reason to share. In these circumstances, that compelling reason is safeguarding the child.

4.11. Documenting the safeguarding/ protection links in that work will not only help you make your decision, but it helps you comply with the law.

Step 3 – Develop Clear and Secure Policies and Systems for Information Sharing

4.12. Your service will have strong governance, policies and systems in place and will keep everything under regular review.

4.13. Follow a '*data protection by design and default'* approach to handling and sharing information **helps build a culture of compliance** and good practice throughout your organisation to help you to share information securely.

4.14. Providing learning tools or training staff in understanding safeguarding/ child protection around data protection, and to the level needed is essential.

Example

4.15. A nursery assistant notices a concerning pattern of behaviour by an adult towards a toddler in the adult's care. The nursery assistant understands that she needs to promptly tell her manager her concerns. To protect the child, the nursery shares the information with the local child protection service.

4.16. For your part it is essential to:

- Ensure you, your staff and any volunteers all understand what they need to do to share information to safeguard and protect children. This is always best practice.
- Consider if you will require additional support from your management team when sharing information when safeguarding/ child protection is not your day-to-day responsibility.
- Actively seek out opportunities to enhance your understanding of sharing information by becoming familiar with your organisation's policies, and procedures. Accessing learning opportunities is essential.

4.17. Having knowledge of policies and systems in place will help you to share information confidently, whether you are sharing information on a routine basis or as a one-off.

4.18. Routine information sharing is "*sharing done on a regular basis"* in a preplanned way. For example, a group of organisations might arrange to share information for specific child protection purposes, on a frequent or regular basis, or both. This type of sharing will be an established process.

4.19. For one-off information sharing, make a decision on what is needed to safeguard and protect a child based on the circumstances at the time, bearing in mind what is fair and proportionate. Planning ahead within your organisation will make the process clear to everyone.

4.20. In some instances, you may decide, or be asked, to share information in one-off situations that are not covered by any routine arrangement or agreement. You may still share that information, assessing the risks at the time.

4.21. Sometimes you may have to decide quickly about sharing information in conditions of real urgency, or even in an emergency. In these situations, do not be put off from sharing information; assess the risk and do what is necessary and proportionate.

Step 4 - Be Clear About Transparency and Individual Rights

4.22. Be clear about what happens to personal information at every stage; about how you will inform people about this, and how you will manage any requests by people to access their information rights.

4.23. Tell people about how and why their information is used, giving them privacy information. In any sharing arrangement, ensure you/ your organisation has policies and procedures that allow people to exercise their individual rights under data protection law:

- the right to access information held about them (the right of subject access).
- the rights to have their information rectified, erased, or restricted.
- the right to object.
- the right to portability of their information; and

- the right not to be subject to a decision based solely on automated processing.

4.24. **However, if you are sharing information for safeguarding/ protection purposes, you might not be obliged to allow people to exercise all these rights. For example, if giving access to a person to information you hold about them would be likely to cause serious harm to a child.**

4.25. There are exemptions and restrictions that you may use in some circumstances to limit these rights. The DPA 2018 lists the exemptions relating to health, social work, education and child abuse, and the circumstances where they can be applied. This includes cases of information being processed by a court, requests made by someone with parental responsibility or in cases where compliance would be likely to cause someone serious harm.

Step 5 – Assess the Risks and Share as Needed

4.26. When you are making a decision about sharing information about a child, it is particularly important to assess the risks.

4.27. If you work for an organisation that shares information on a regular or routine basis, a Data Protection Impact Assessment (DPIA) will help. A DPIA is a practical tool to help you plan for the information sharing and assess and mitigate the risks to children's rights and freedoms. It helps you to ensure your sharing is done safely, lawfully and with accountability. Speak to legal services in your agency if you need help, advice, or support.

4.28. There will be circumstances not covered by a DPIA, such as sharing information on a one-off basis (for example, if you are an individual employee or volunteer raising the alarm over something you have seen), or in an urgent situation or in an emergency. You can go ahead and share that information based on what is necessary and proportionate in the circumstances at the time to safeguard and protect the child.

Step 6 – Enter into a Data Sharing Agreement

4.29. Although it is not mandatory to enter into a data sharing agreement, it can help all parties concerned in some cases.

4.30. As an organisation your agency can assist you draw up a data sharing agreement (DSA) between you and any others that you are intending to share information with. As with a DPIA this is more likely to be feasible in scenarios of regular and routine information sharing between organisations.

4.31. Benefits include helping you and the party or parties you are planning to share the information with to:

- be clear about what information you are sharing.
- be clear how it will happen; and
- demonstrate that you are responsible for complying with data protection law (the accountability principle).

4.32. It may also be known as an information sharing agreement (ISA), or a data or information sharing protocol or contract.

4.33. Some organisations, including Scottish Government may instead enter into a memorandum of understanding (MOU) with each other that includes information sharing provisions and fulfils the role of a data sharing agreement. Please check with your agency's legal services department if you have any queries regarding above.

Example

4.34. Some local organisations wanted to identify young people who already had been or were currently at high risk of disengaging from education, employment, or training. They decided to routinely share personal information with each other. These partner organisations included two councils, local schools and colleges, housing providers, relevant community organisations, the local job centres, and careers service. By sharing the information, they were able to co-ordinate their approach to providing the most appropriate support to the young person to encourage them back into education, work, or training.

4.35. The partners used a data sharing agreement to set out their purpose, lawful bases, and the information they would share. The agreement included a section on how to manage people's rights and agreed shared security standards; the partners also updated their privacy notices. To quality-assure their agreement, they shared it with a local group of data protection practitioners for feedback. They also set a timescale for the partners to regularly review the agreement to ensure it stayed up-to-date and fit for purpose.

Step 7 – Follow the Data Protection Principles

4.36. The seven data protection principles lie at the heart of data protection; follow them when handling or sharing personal information. They are all important.

- Lawfulness, fairness, and transparency
- Purpose limitation (share only for your clear, specified, legitimate purposes)
- Data minimisation (share information that is adequate, relevant, and limited to what is necessary for your purposes)
- Accuracy (and keep the information up to date)
- Storage limitation (keep the information no longer than necessary for your purposes)
- Integrity and confidentiality (ensure appropriate security)
- Accountability (demonstrate your compliance with the principles)

Step 8 – Share Information Using the Right Lawful Basis

4.37. Sharing information is always lawful when you choose the right lawful basis for you and for the circumstances. The Information Commissioner's Office (ICO) has a tool to help you on their website.

4.38. A lawful basis is a valid reason in data protection law for processing personal information. Using the right lawful basis means you can share all the information you need to, with an appropriate authority or individual, in order to safeguard a child.

4.39. Identify at least one lawful basis for sharing information before you start the sharing. Ensure you can demonstrate that you considered which lawful basis to use, in order to satisfy the accountability principle. **Keep a record of your decision and your reasons, even if you decide that you do not have a lawful basis and therefore cannot share the information.**

4.40. Consent is one lawful basis, but it is not required for sharing information in a safeguarding context. In fact, in most safeguarding/ child protection scenarios you will be able to find a more appropriate lawful basis.

Example

4.41. A teacher notices a child in his class is demonstrating some concerning behaviour, including showing fear about being collected from school by a relative with whom they live. The teacher follows the school's procedures and speaks to the safeguarding lead. The school contacts the local safeguarding/ child protection service to share the information about the child.

4.42. The school does not need to obtain the consent of the relative to share this information.

4.43. The most common lawful bases suitable for safeguarding/ child protection purposes are public task, legitimate interests, and legal obligation.

Step 9 – Share Information in an Emergency

4.44. In an emergency, do not hesitate to share information to safeguard and protect a child. You might not have time to follow all the usual processes.

4.45. Make a record of what you shared, who with, and why, as soon as possible.

4.46. Some situations might be urgent, but not an emergency. Take a proportionate approach in the circumstances.

4.47. Plan ahead for emergency or urgent situations so that everyone knows what to do and the processes to follow when time is of the essence.

Step 10 – Read the ICO Data Sharing Code

4.48. We recommend you use this 10-step guide in conjunction with:

- Data sharing code of practice
- Data sharing page

5. What About Children's Rights & Information Sharing?

5.1. Article 8 European Convention on Human Rights (ECHR) and Article 16 of the UNCRC Article 8 of the ECHR – Right to respect for private and family life states:

1. Everyone has the right to respect for his private and family life, his home, and his correspondence.
2. There shall be no interference by a public authority with the 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, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 gives everyone the right to respect for their private and family life, their home, and their correspondence. Sharing personal information is likely to interfere with that right. For that interference to be lawful, the information must be shared in a way that is proportionate to the achievement of a legitimate aim. The GIRFEC Information Sharing Guidance (2022) provides details of the two-part test that needs to be met to ensure that children, young people, and family member's human rights are respected, and that any interference is justified as lawful and proportionate. Provided the information sharing is compliant with data protection legislation and you assess the information sharing in the particular circumstances to be in the best interests of the child or young person and to promote, support or safeguard their wellbeing, the conditions of the first part of the test will be met. In addition, the impact on the person's right to privacy must not be disproportionate to the aim of sharing. If there is an alternative option, which is less intrusive but still achieves the aim, then the interference with an individual's private and family life will be disproportionate. You must share the minimum confidential or sensitive information necessary with the minimum services or individuals necessary in the interests of the child or young person.

Article 16 of the UNCRC provides a similar right to privacy, but provided that you comply with the Article 8 test you will not breach Article 16.

Published 2023