Data Sharing Framework

between

Shetland Islands Council and NHS Shetland

(hereinafter individually referred to as “a Partner” or collectively as “the Partners”)

Document Information			
Document Name/Description/Location			Data Sharing Framework o:\asoffice\data protection\policies and procedures\finals\data sharing framework v02.01.doc
Version Number *e.g. V1.1*			02.01
Author [Name and Post Title]			Kristen Johnston, Team Leader – Legal Services (Shetland Islands Council) David Morgan, Head of Information Governance (NHS Shetland)
Lead Officer/Manager [Name and Post Title]			Christine Ferguson, Director of Corporate Services / Senior Information Risk Owner (SIC) Colin Marsland, Director of Finance / Senior Information Risk Owner (NHS Shetland)
Final Approval Date			22 February 2023 (SIC) 25 May 2023 (NHS Shetland FPC)
Approved by – Council/Committee/Group/Manager			Shetland Islands Council NHS Shetland
Review Frequency			5 years
Date of next planned review start			January 2028
Summary of changes to document			
Date	Version updated	New version number	Brief description of changes
25/01/2023	0.11	01.00	new draft for consultation - agenda management
30/01/2023	01.00	01.01	Updated with joint author information – NHS Shetland
22/03/2023	01.01	02.00	Finalised following SIC approval – issued to NHS Shetland for approval.
25/05/2023	02.00	02.01	Approved by NHS Shetland Finance and Performance Committee

Contents

Glossary of Terms/Definitions/Abbreviations:
See Information Commissioner's Office (ICO) Glossary

Code of Practice (ICO)
https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

Data sharing decision form template (ICO):
https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-in-an-urgent-situation-or-in-an-emergency/

Information Sharing Toolkit (Scottish Government)
https://www.digihealthcare.scot/app/uploads/2022/03/IS-Toolkit-Introduction-21-05-2019-5.pdf

1. Introduction

1.1 The Data Sharing Framework (the Framework) recognises that data sharing between organisations can play a crucial role in providing better, more efficient and co-ordinated services. It is necessary to understand what data can and cannot be shared to ensure individuals are not placed at a disadvantage due to carelessness or excessive caution.

1.2 The need to share data between organisations has long been recognised in Shetland. The Framework has been developed to provide an agreed process for the legitimate, secure and confidential sharing of personal data between organisations delivering services or linked to the delivery of services based in Shetland.

1.3 The Framework is not a data sharing agreement nor does it provide authorisation for one-off instances of data sharing.

1.4 Where there is a need to share data with organisations who are not a signatory to the Framework, the terms and principles of the Framework should still be applied.

2. Aims & Objectives

2.1 It is often necessary to share data to enable organisations to meet the needs of individuals for their care, protection, support and delivery of services in accordance with government expectations, legislative requirements, and the governance arrangements of individual Partners. The Framework provides guidance for such data sharing and supports practitioners to share data confidently and legally. The appendices provide useful information, tools and diagrams to assist in complying with the terms of the Framework.

2.2 The Framework will also help inform individuals of the reasons why their data may need to be shared and how this data sharing will be managed to ensure they are confident that their personal data is being handled responsibly and securely.

2.3 ICO's Data Sharing Code of Practice https://ico.org.uk/media/for-organisations/data-sharing-a-code-of-practice-1-0.pdf (the Code of Practice) provides important guidance on data sharing and how to comply with the Data Protection Act 2018 and the UK General Data Protection Regulation (or any successor legislation). The Framework aims to put the principles and recommendations within the Code of Practice into a local context.

3. Tools & Resources

3.1 What do I need before deciding whether or not to share personal data?

3.1.1 A flowchart providing an overview of the data sharing process is attached as Appendix B.

3.1.2 Internal Tools & Resources
Partner data protection and information governance policies;
e.g. Data Protection Policy
e.g. Data Protection Impact Assessment Guidance
Partner Data Protection Officers or Data Protection Lead Officer.

3.1.3 External Tools & Resources
Additional resources and assistance can be found at:

- ICO Code of Practice
- Scottish Government's Information Sharing Toolkit

See links on the contents page of this document.

3.1.4 Whilst the Framework puts into practice the principles within the Code of Practice, the Code of Practice must be consulted before any instance of data sharing occurs. In particular, the Code of Practice offers further guidance on:-

- What is systematic or one off data sharing.
- Data sharing and the law.
- Factors to consider when deciding to share personal information.
- Security.

3.1.5 The ICO Code of Practice data sharing checklist provides a step-by-step guide to deciding whether to share personal data. It highlights what should be considered in order to ensure that the sharing complies with the law and meets individuals' expectations.
https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/annex-a-data-sharing-checklist/

4. What is Data Sharing?

4.1 When does the Framework apply?

4.1.1 Data sharing is the disclosure of data from one or more organisations to another organisation. The Framework only applies to the disclosure of personal data between organisations.

4.1.2 The Framework does not apply to the disclosure of personal data within the same organisation. The movement of personal data by one part of an organisation to another part is not data sharing. The obligations under data protection legislation still apply and advice should always be sought from the Data Protection Officer or Data Protection Lead Officer.

4.1.3 Some data sharing does not involve personal data, for example statistics, policy documents or business information that cannot identify an individual. The Framework does not apply to this type of data sharing and only applies when personal data is being shared. However, careful consideration should always be given when sharing an organisation's data, in particular to any obligations under Freedom of Information legislation and whether the information you want to share is commercially sensitive or should not be published.

4.1.4 If an organisation asks another party to process personal data on its behalf, that other party will be a data processor. For example, an organisation has a contract in place for an external company to manage their payroll or provide and support an Information and Communications Technology (ICT) system. There are certain legal requirements that must be in place between the organisation and the data processor to protect the personal data and the rights of the individual(s) affected. This type of data processing is not covered by the Framework.

4.2 What is personal data?

4.2.1 Personal data is data which relates to a living individual who can be identified from the data. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier. Data about a deceased person is not covered by data protection legislation, but caution should still be taken when asked to share data about a deceased person.

4.2.2 If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

4.2.3 If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.

4.2.4 Even if an individual is identified or identifiable from the data you are processing, it is not personal data unless it relates to the individual. To decide whether or not the information relates to the individual, you need to look at the content of the information, the purpose(s) for which it is being used and the likely impact that will have on the individual.

4.2.5 Simply replacing identifying information with a number or reference (known as pseudonymised) is still personal data because the organisation will hold the information which links that number or reference with an individual.

4.2.6 Information which is truly anonymous is not personal data.

4.2.7 More information about what is personal data is available from the ICO website:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

4.3 Identifying Data Flows

4.3.1 Once it has been established that personal data is being shared between organisations, it is important to work out the flow of that personal data. This is about being clear what the journey of the personal data will be, from identifying what needs to be shared through to it being used by the receiving organisation.

- Where does the data come from?
- Which organisation holds the data to be shared?
- Who does it have to be shared with?
- What happens to the data once it is shared?

4.3.2 A simple flow chart will be helpful in mapping the data flow of the proposed data.

5. What type of data sharing is being considered?

5.1 The Framework covers two main types of data sharing:-

- Systematic data sharing – where the same data sets are shared between the same organisations for an established purpose.

- One off data sharing – where there is an exceptional, one off decision to share data for any of a range of purposes.

5.2 Systematic or Routine Data Sharing

5.2.1 Systematic or routine data sharing will generally involve regular sharing of data sets between organisations for an agreed purpose. Where this

occurs, a Data Sharing Agreement must be agreed between the organisations involved in the data sharing.

5.2.2 A Data Sharing Agreement [sometimes referred to as an Information Sharing Agreement or Information Sharing Protocol] is a common set of rules to be adopted by the organisations involved in a data sharing operation. A Data Sharing Agreement sets out the detail of how data will be shared in practice to ensure compliance with the terms of the Framework.

5.2.3 There is a template Data Sharing Agreement available within the Scottish Government Information Sharing Toolkit.

https://www.informationgovernance.scot.nhs.uk/istresources/

This template may be used when a Data Sharing Agreement is required. The template can also be used as a checklist to ensure all necessary issues are covered when using any other style of Data Sharing Agreement. A partner organisation may have a preferred style of Data Sharing Agreement and advice should always be sought from the relevant organisation's Data Protection Officer or Data Protection Lead Officer.

5.2.4 Anyone drafting a Data Sharing Agreement should refer to the ICO Code of Practice referred to above and the Scottish Government Information Sharing Toolkit. See links on the contents page of this document.

5.2.5 There are a number of Data Sharing Agreements already in place within Shetland. Therefore, there may be a Data Sharing Agreement in place that covers the systematic or routine data sharing that is being proposed. The Data Protection Officer or Data Protection Lead Officer should be aware of any Data Sharing Agreements already in place. (See Partner Organisation details at section 9 below).

5.2.6 All Data Sharing Agreements must be signed by the Information Asset Owner or person responsible for that data within a partner organisation and at the appropriate managerial level to ensure compliance with the terms of the agreement and that the correct organisational governance requirements are met. Any partner organisation, which enters into a Data Sharing Agreement under the Framework, is undertaking to implement and adhere to the terms of the Framework. Advice on the terms of the Data Sharing Agreement must be sought from the partner organisation's Data Protection Officer or Data Protection Lead Officer

5.2.7 The purpose of Data Sharing Agreements are to ensure compliance with the Framework, the ICO Code of Practice, the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR) as illustrated by Appendix A.

5.3 One Off Data Sharing

5.3.1 It is anticipated that the majority of data sharing will be systematic or routine data sharing, often governed by a Data Sharing Agreement or similar established rules and procedures as discussed above. However, there are times when organisations want to share data in situations that are not covered by any established agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency – for example in an emergency situation.

https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-in-an-urgent-situation-or-in-an-emergency/

5.3.2 Disclosures of personal information, even in emergency situations, are still subject to the Data Protection Act 2018 and UK GDPR. Therefore, it is important that the decision to share personal data is properly recorded. It may not always be possible to document the sharing in an emergency or time dependent situation. A record of data sharing actions and the reasons why the data was shared must be completed as soon as possible.

5.3.3 There are template Data Sharing Decision Forms available from the ICO. One is for use by the organisation making the request for data to be shared and the other is for the organisation taking the decision to share personal data.

https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/annex-b-data-sharing-request-form-template/data-sharing-template/

https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/annex-b-data-sharing-request-form-template/

5.3.4 These templates may be used when there are one-off occasions of data sharing. These templates can also be used as a checklist to ensure all necessary issues are covered when using any other style of Data Sharing Decision Form. A partner organisation may have a preferred style of recording one-off instances of data sharing and advice should always be sought from the relevant organisation's Data Protection Officer or Data Protection Lead Officer.

5.3.5 More information is available on the ICO Code of Practice referred to above and the Scottish Government Information Sharing Toolkit. See links on the contents page of this document.

5.3.6 The purpose of a Data Sharing Decision Form is to ensure that the decision to share data is compliant with the Framework, Code of Practice, the Data Protection Act 2018 and UK GDPR.

5.3.7 The organisations sending and receiving the personal data must both complete the relevant Data Sharing Decision Form - a request to share or a decision to share. Each organisation must retain a copy of the completed Data Sharing Decision Forms for their own records.

5.3.8 Having numerous Data Sharing Decision Forms for sharing the same information between the same organisations on multiple occasions is a clear indication that a Data Sharing Agreement must be considered. The data sharing is no longer one off instances, but is becoming routine and systematic.

6. Do I need a Data Protection Impact Assessment (DPIA)?

6.1 Before sharing any personal data, consideration must be given as to whether or not a DPIA is required. Where there is systematic or routine data sharing and a Data Sharing Agreement is required, a DPIA must be completed.

6.2 A DPIA is an invaluable tool to help you assess any privacy risks in your proposed data sharing, and work out how to mitigate these risks. It will help you to ensure you are sharing data fairly and transparently. It will help you to consider these matters, and to document them. Depending on the nature of the data sharing, you may be legally obliged to carry out a DPIA. However, even if you are not legally obliged to complete one, it is very beneficial for you to follow the DPIA process.

6.3 A DPIA will help you to fully understand whether you can share the data at all and whether you can share the data, but with steps and measures in place to mitigate against any risks to privacy.

6.4 The DPIA process will not only help to ensure personal data is protected, but will also help you to put additional safeguards in place to mitigate risk where needed. In turn, this will help to provide reassurance to the people whose data you are sharing.

6.5 Each partner organisation may have their own DPIA process and templates and further information can be found on the Information Commissioner's Office website at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

6.6 There will be situations where specialist advice is required, for example:-

- Law enforcement processing;
- Due diligence (mergers & acquisitions);
- Sharing databases & lists;
- Data Sharing & Children; and
- Data sharing in an urgent situation or in an emergency.

Further information can be found within the ICO Data Sharing Code of Practice at https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

6.7 It is likely you will need the advice and support from your Data Protection Officer or Data Protection Lead Officer to complete your DPIA.

7. Data Protection Principles

7.1 What do I need to know to help me decide whether or not to share?

7.1.1 Whether the data sharing is systematic / routine data sharing or one off data sharing, there are supporting principles applicable to both. Understanding these principles will help you to decide whether or not to share personal data and complete any necessary documentation – e.g. a DPIA, a Data Sharing Agreement or a Data Sharing Decision Form.

7.2 Data Protection Principles

- Processed fairly, lawfully and transparently (e.g. Privacy Notices/Statements).
- Collected for specific purposes and not used for incompatible purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Retained no longer than necessary (e.g. Retention & Destruction Schedules).
- Kept securely (e.g. ICT Security Policies).

More detail on each of the data protection principles is attached as Appendix C or from the ICO. See links on the contents page of this document.

7.3 Accountability and Governance of Data Protection

7.3.1 Accountability is a further principle of data protection legislation which requires organisations to demonstrate its compliance. Organisations must maintain oversight and transparency in the management of personal data.

7.3.2 It is important to maintain relevant documentation to demonstrate that organisations are meeting their accountability obligations. Examples of documentation that should be kept in relation to data sharing (this list is illustrative only & not exhaustive):

- Data sharing agreement
- Data sharing decision form
- Data protection impact assessment
- Privacy notice or privacy statement
- Personal information register
- Data breach log

7.4 Individual Rights

7.4.1 In a data sharing agreement, it must be clear how data subjects exercise their individual rights easily.

7.4.2 Details of how to exercise these rights must be in the Privacy Notices/Statements available to individuals.

7.4.3 Where several organisations are sharing data, it may be difficult for an individual to decide which organisation they should contact. This should be made clear in the privacy information provided.

7.4.4 In a data sharing agreement, it is good practice to provide a single point of contact for individuals, which allows them to exercise their rights over the data that has been shared without making multiple requests to several organisations. However, they are permitted to choose to exercise their rights against any organisation they wish.

8. Review

8.1 The Framework will be reviewed every five years or more regularly if necessary due to changes in legislation, guidance or good practice. The review will be organised by Shetland Islands Council and should involve representatives from:-

- Shetland Islands Council
- NHS Shetland
- Other relevant signatories

9. Signatories

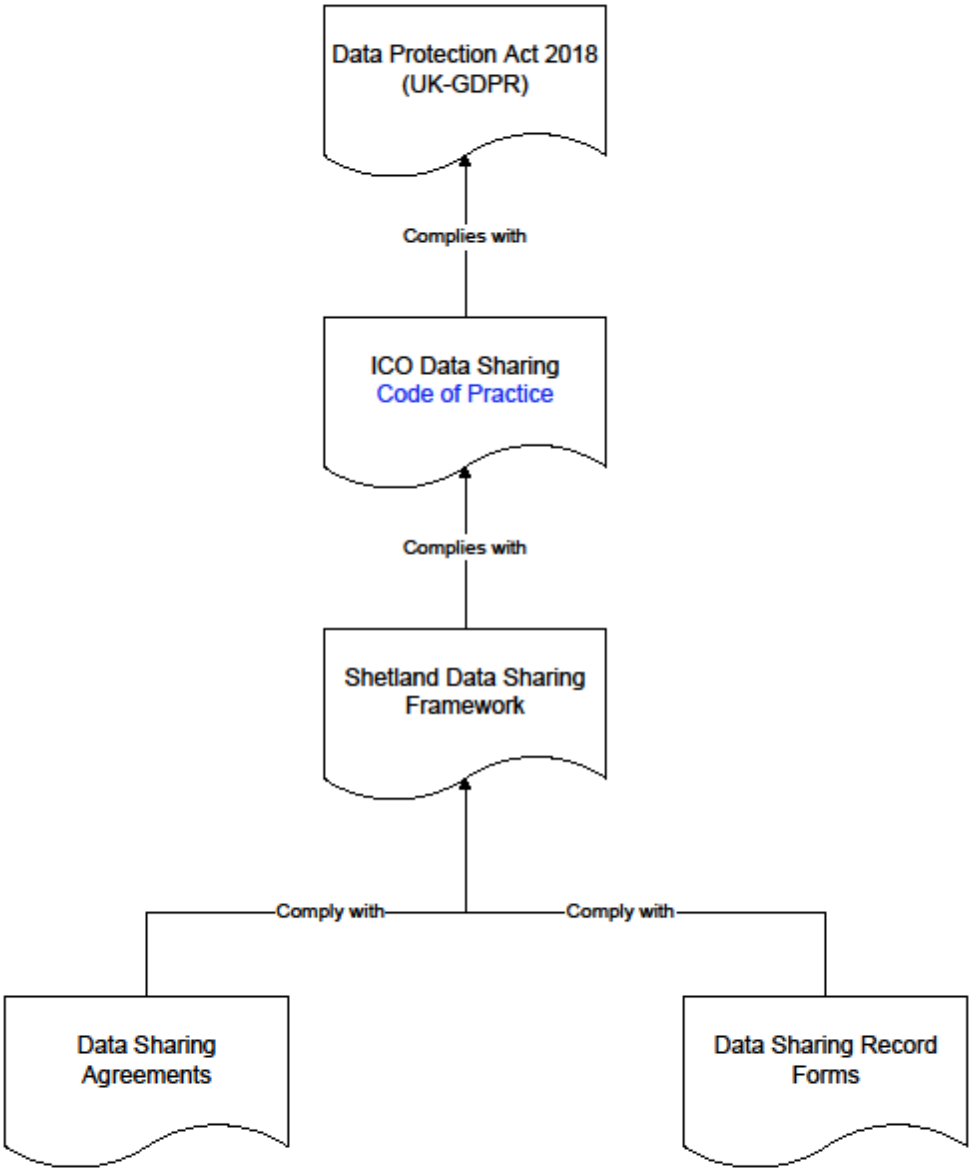
By signing the Framework the Partners confirm that they accept its terms.

SHETLAND ISLANDS COUNCIL		
Authorised Signatory	PRINT NAME	Christine Ferguson
	TITLE/DESIGNATION	Director of Corporate Services / Senior Information Risk Owner (Shetland Islands Council)
	SIGNATURE	
	DATE	21/08/2023
Data Protection Officer	NAME	Jan-Robert Riise
	TITLE/DESIGNATION	Data Protection Officer
	ADDRESS	8 North Ness, Lerwick, Shetland, ZE1 0LZ
	TELEPHONE No.	01595 744551
	E-MAIL	Data.protection@shetland.gov.uk

NHS SHETLAND		
Authorised Signatory	PRINT NAME	Colin Marsland
	TITLE/DESIGNATION	Director of Finance / Senior Information Risk Owner (NHS Shetland)
	SIGNATURE	Colin Marsland
	DATE	24/08/2023
Data Protection Officer or Data Protection Lead Officer	NAME	David Morgan
	TITLE/DESIGNATION	Head of Information Governance, FOI Lead & DPO
	ADDRESS	11 Alexandra Building, Esplanade, Lerwick ZE1 0LL
	TELEPHONE No.	01595 743363
	E-MAIL	shet.dpo@nhs.scot

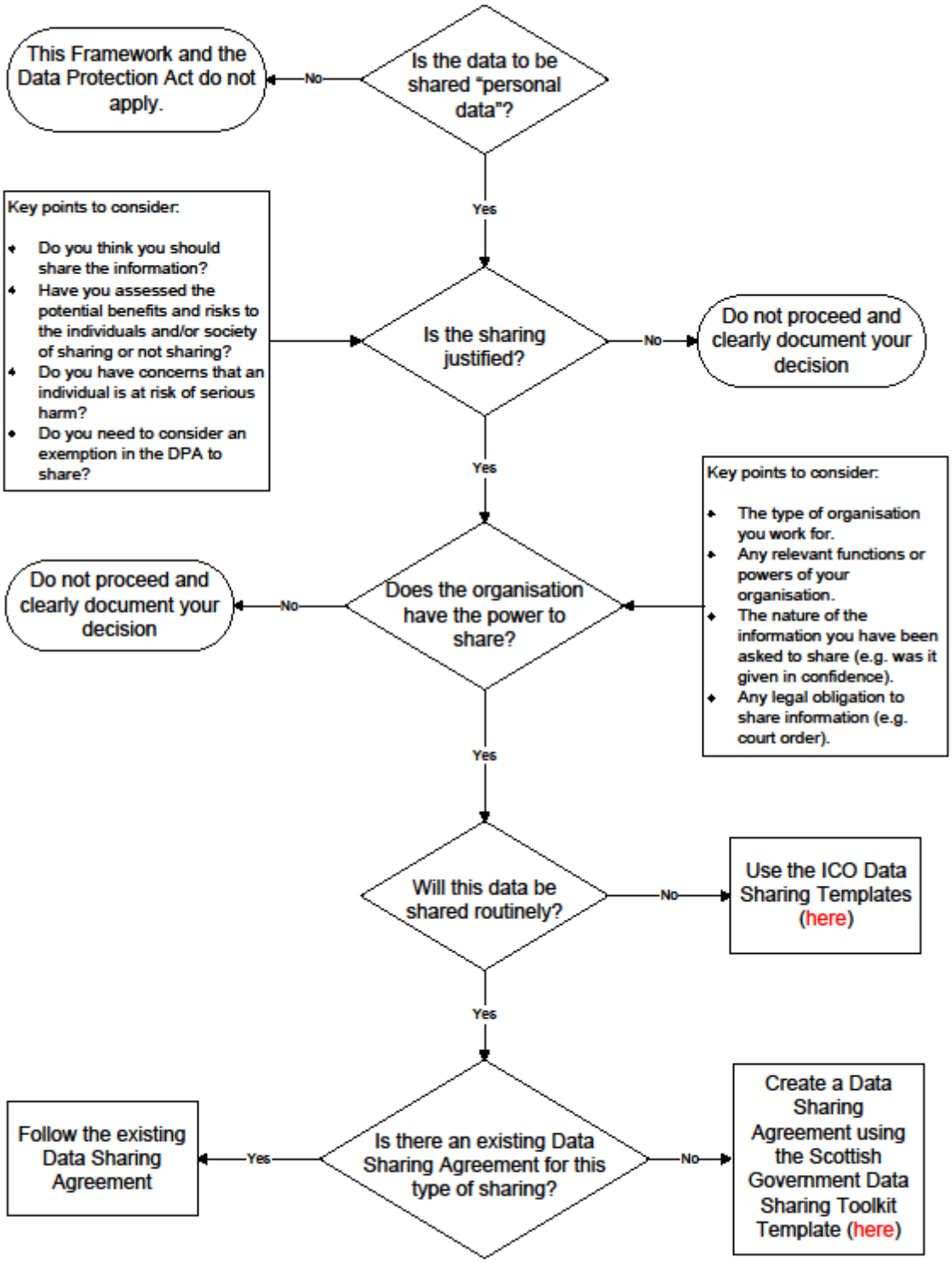
END

Overview of Data Sharing Governance Appendix A



Data Sharing Decision Process

Appendix B



The Data Protection Principles

Appendix C

The Partners will at all times comply with the data protection principles when processing personal information. This includes personal information relating to any individual with whom a Partner has a relationship, e.g. staff, volunteers, service users, customers, potential customers and business contacts.

All personal data will be:

Principle 1

Processed fairly, lawfully and transparently
(e.g. Privacy Notices/Statements)

Principle 2

Collected for specific purposes and not used for incompatible purposes
(refer to Personal Information Registers)

Principle 3

Adequate, relevant and limited to what is necessary

Principle 4

Accurate and, where necessary, kept up to date

Principle 5

Retained no longer than necessary
(refer to Retention & Destruction Schedules)

Principle 6

Kept securely
(refer to ICT Security Policies)

Principle 7

Be able to demonstrate compliance with Principles 1-6

There is more information on each principle in the following pages and the ICO has detailed guidance about the data protection principles at:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

END OF DOCUMENT

Back to Contents Page