Shetland Data Sharing Policy

Date: October 2012
Version number: Combined 0.4 NHS v1
Author: Kristen Johnston and Jane Cluness
Review Date: October 2014

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Shetland Data Sharing Policy

1. Introduction

1.1 Data sharing within and 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 within and between organisations has long been recognised in Shetland. The Shetland Data Sharing Policy (the Policy) has been developed to provide an agreed framework for the legitimate, secure and confidential sharing of personal data within and between organisations in Shetland.

1.3 Where there is a need to share data with non-Partner Organisations, the terms of the Policy should be applied.

2. Partner Organisations

2.1 The Policy has been developed and adopted by Shetland Islands Council, NHS Shetland, Northern Constabulary and Voluntary Action Shetland (the partner organisations).

Shetland Islands Council

....
(Print Name) (Title/Designation)

....
(Signature) (Date)

NHS Shetland

....
(Print Name) (Title/Designation)

....
(Signature) (Date)

Northern Constabulary

....
(Print Name) (Title/Designation)

....
(Signature) (Date)

Voluntary Action Shetland

....
(Print Name) (Title/Designation)

....
(Signature) (Date)

3. Aims & Objectives

3.1 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 and legislative requirements. The Policy provides a framework 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 Policy.

3.2 The Policy 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.

3.3 The Information Commissioner's Data Sharing Code of Practice (insert link) (the Code of Practice) provides important guidance on data sharing and how to comply with the Data Protection Act 1998. The Policy puts the principles and recommendations within the Code of Practice into a local context. Therefore, anyone using the Policy must also read the Code of Practice. The Code of Practice is discussed in more detail below at section 5.

4. What is Data Sharing?

4.1 Data sharing is the disclosure of data from one or more organisations to another organisation, or the sharing of data between different parts of an organisation. It is important to remember that data sharing can occur between different parts of an organisation and not just to external third party organisations. The Policy applies equally whether the data sharing is occurring within or out with an organisation.

4.2 Some data sharing does not involve personal data, for example where only statistics that cannot identify anyone are being shared. The Policy does not apply to that type of sharing and only applies when personal data is being shared.

4.3 Personal data is data which relates to a living individual who can be identified from the data. If it is not clear whether the data being shared is personal data, further advice should be sought from the person responsible for data protection within an organisation. Personal data can include minimum amounts of data, e.g. name, date of birth, phone number, etc.

4.4 The Code of Practice covers two main types of data sharing:-

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

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

The flowchart at Appendix 1 provides a guide to support the decision making process on whether to share personal data and which type of data sharing it is.

5. The Information Commissioner's Code of Practice

5.1 Whilst the Policy 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.
- Checklists for data sharing.

Further advice on compliance with the Code of Practice is available from the person responsible for data protection within an organisation.

6. Systematic Data Sharing

6.1 Systematic data sharing will generally involve routine 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.

6.2 A Data Sharing Agreement 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 Policy.

6.3 A template Data Sharing Agreement is attached at Appendix 2 that must be used when organisations do not have their own preferred style of record. The template can also be

used as a checklist to ensure all necessary issues are covered in any other style of Data Sharing Agreement.

6.4 There are a number of Data Sharing Agreements already in place within Shetland (previously known as Information Sharing Agreements or Protocols). Therefore, there may already be a Data Sharing Agreement in place that covers the systematic data sharing that is being proposed. The person responsible for data protection within an organisation should be aware of any Data Sharing Agreements already in place. Alternatively, contact the Shetland Data Sharing Manager for more information about existing Data Sharing Agreements (see Appendix 7 for contact details).

6.5 Before entering into a Data Sharing Agreement, it is good practice to carry out a privacy impact assessment. This will help to assess the benefits that the data sharing might bring to particular individuals or society more widely. It will also help assess any risks or potential negative effects. It will be up to each organisation entering into a Data Sharing Agreement to determine whether a privacy impact assessment is necessary. Further information on privacy impact assessments can be found at the Information Commissioner's Office website at : www.ico.gov.uk

6.6 All Data Sharing Agreements must be signed by the person responsible for data protection within an 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 organisation, which enters into a Data Sharing Agreement under the Policy, is undertaking to implement and adhere to the terms of the Policy.

6.7 The purpose of Data Sharing Agreements is to ensure compliance with the Policy, the Code of Practice and the Data Protection Act 1998 as illustrated by Appendix 3.

6.8 The Shetland Data Sharing Partnership must be advised of any Data Sharing Agreement that is created. This will assist the Shetland Data Sharing Manager to maintain a central register of Data Sharing Agreements within Shetland. Each organisation should also keep a list of the Data Sharing Agreements relating to their own service.

6.9 Where there are any problems in developing a Data Sharing Agreement or where data is to be shared on a large scale, the Shetland Data Sharing Partnership may be able to offer guidance and assistance. The Shetland Data Sharing Manager can be contacted in the first instance for an informal discussion (see Appendix 7 for contact details).

7. One Off Data Sharing

7.1 It is anticipated that the majority of data sharing will systematic data sharing, often governed by a Data Sharing Agreement or similar established rules and procedures as discussed in section 6 above. However, there are times when organisations want to share data in situations that are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency – for example in an emergency situation.

7.2 Disclosures of personal information, even in emergency situations, are still subject to the Data Protection Act 1998. 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. Refer to paragraph 7.3 below.

7.3 A template Data Sharing Decision Form is attached at Appendix 4 that must be used when organisations do not have their own preferred style of record. The template can also be used as a checklist to ensure all necessary issues are covered in any other style of record.

7.4 The purpose of Data Sharing Decision Forms is to ensure that the decision to share data is compliant with the Policy, Code of Practice and the Data Protection Act 1998 as illustrated by Appendix 3.

7.5 The organisations sending and receiving the personal data must both complete the Data Sharing Decision Form. Each organisation must retain a copy of the completed Data Sharing Decision Form for their own records.

7.6 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.

8. Supporting Principles

Whether the data sharing is systematic data sharing or one off data sharing, there are supporting principles applicable to both.

8.1 Data Sharing with Consent

8.1.1 It is important to consider whether consent is required from the individual before their personal data is shared. Consent is not required in certain circumstances, for example, if there are statutory grounds or an overriding justification for data sharing without consent. Data sharing without consent is discussed more fully below at section 8.2.

8.1.2 Where consent is required, the consent must be freely given based on clear and specific information regarding the data sharing. There must be some form of active communication where the individual knowingly indicates consent.

8.1.3 Any Data Sharing Agreement governing the proposed data sharing should detail the process to be followed for obtaining and recording consent. Otherwise, the individual's consent should be detailed on a Data Sharing Decision Form.

8.1.4 The individual's capacity must also be considered to ensure they can competently consent to the data sharing. Appendix 5 illustrates the decision making process for determining the individual's capacity when obtaining consent.

8.2 Data Sharing Without Consent

8.2.1 Data sharing can take place without the individual's consent in limited circumstances. Even where consent is not required, it is good practice to inform the individual that you intend to share their personal data. The following is a list of circumstances where the individual's consent may not be required, however this list is not exhaustive and there will be other situations where consent may not be required.

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax or duty.
- Legislation which allows data sharing without consent in specific circumstances in order that an organisation can fulfil its statutory duties.
- An overriding justification in the individual's vital interests – e.g. life and death situations or child/adult protection concerns.

8.2.2 Any data sharing without consent must always be recorded in compliance with a Data Sharing Agreement or decisions clearly recorded on a Data Sharing Decision Form. Further advice should be sought from the person responsible for data protection within an organisation. However, it is recognised that decisions may have to be taken when such advice is not available. 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. Refer to paragraph 7.3 above.

8.2.3 Appendix 6 illustrates the decision making process for data sharing without consent.

For more information on data sharing without consent, refer to the Information Commissioner's Guide to Data Protection – www.ico.gov.uk

8.2.4 Even if an exemption is identified for data sharing without consent, the data does not always have to be released. This is a decision for an organisation to make in accordance with their own Data Protection policies and procedures, taking advice from the person with responsibility for data protection. If there are genuine concerns about releasing personal data, for instance there are other legal obligations such as the data being confidential, then a court order can be sought requiring the release of the personal data. If a court determines that the personal data should be released, there will be no breach of the Data Protection Act 1998 by obeying the court order.

8.3 Appropriate & Relevant

8.3.1 Any data which is shared must be appropriate and relevant. All organisations involved in sharing data should check:-

- Is it necessary to share personal data, or can anonymised information be used instead;
- That only the minimum amount of data is being shared, to a minimum number of organisations, and that only necessary staff members have access to it;
- That the data is accurate and up to date.
- That only data which is appropriate and relevant to the circumstances is shared and is not excessive.

8.4 Privacy Notices

8.4.1 A Privacy Notice is the explanation given to an individual when personal data about them is collected by an organisation. It is not always necessary to issue a Privacy Notice and further advice should be sought from the person responsible for data protection within an organisation as to whether or not a Privacy Notice is required.

8.4.2 Individuals should generally be aware of the organisations that are sharing their personal data and what it is being used for. The Information Commissioner's Office has produced comprehensive good practice guidance on the drafting and distribution of Privacy Notices (sometimes known as Fair Processing Notices or Information Sharing Leaflets). The Privacy Notices Code of Practice is available at www.ico.gov.uk

8.4.3 For data sharing purposes, a Privacy Notice must at least tell the individual:-

- Who holds the personal data.
- Why the personal data is to be shared.
- Who the personal data is to be shared with.
- How the personal data is to be shared.

8.4.4 Where there is a Data Sharing Agreement, this must detail the process for issuing a Privacy Notice and may include a standard format to be used. Otherwise, it should be recorded on a Data Decision Form what information and explanation was given to the individual.

8.5 Security

8.5.1 Organisations must have in place the appropriate technical and organisational measures when sharing personal data. Both physical and technical security must be considered.

8.5.2 It is important to remember that it is the responsibility of the organisation disclosing the personal data to ensure that the means of transferring the data is secure and that it will continue to be protected with adequate security by any other organisation that will have access to it.

8.5.3 Where there is a Data Sharing Agreement, this should detail the process for secure transfer and handling of the personal data. Otherwise, any relevant security measures should be recorded on a Data Sharing Decision Form.

8.5.4 **E-mail**

E-mailing personal data is only secure when sending and receiving within recognised secure networks.

- nhs.net
- gsx.gov.uk
- gse.gov.uk
- gsi.gov.uk
- police.uk
- pnn.police.uk
- scn.gov.uk
- cjsm.net
- gcsx.gov.uk

8.5.5 **Telephone**

The verification of the identity of the parties to the phone call must always be carried out before any personal data is shared. A phone number must be checked by reference to a phone book and/or contact the main reception or switchboard for the organisation and ask for a specific person rather than relying on a direct dial number.

8.5.6 **Written Communications**

Any written communications containing personal data must be transferred by appropriate and secure means, addressed by name to a designated person within the receiving organisation and marked "Strictly Confidential – Open Only by Addressee". The designated person must be alerted to the despatch of such information and must make arrangements within their own organisation to ensure both that the information is delivered to them unopened and that it is received within the expected timescale.

8.5.7 **Fax**

Fax transfer must be avoided wherever possible. Where it is necessary, then individual organisation's procedures for secure fax transfer must be followed (such as "safe haven" faxes).

8.6 Individual Rights

8.6.1 The Data Protection Act 1998 gives individuals certain rights over their personal data. These include:-

- The right to access personal data held about them.
- The right to know how their data is being used.
- The right to object to the way their data is being used.

8.6.2 When several organisations are sharing personal data it may be difficult for an individual to decide who they should contact in order to exercise these rights. It is good practice to consider having a single point for individuals to contact.

8.6.3 Where there is a Data Sharing Agreement, this should detail the process and point of contact for dealing with these individual rights. Otherwise, any relevant information regarding individual rights should be recorded on a Data Decision Form.

8.6.4 Organisations that have agreed to adhere to the terms of the Policy are responsible for giving an individual general advice and support on how to progress a complaint or concern under the Policy.

8.7 Third Party Information

8.7.1 There may be situations where the sharing of personal data would result in the disclosure of personal information relating to a third party or enable that third party to be identified as the source of the information.

8.7.2 Personal data which identifies a third party should only be disclosed where the third party has consented to the disclosure or where it is reasonable in all the circumstances to comply with the request without the consent of the other individual. The personal data may also be redacted to protect the identity of the third party. This is a decision for an organisation to make in accordance with their own Data Protection policies and procedures, taking advice from the person with responsibility for data protection. Further information on the disclosure of third party information can be found at the Information Commissioner's Office website at: www.ico.gov.uk.

9. Data Protection & the Law

9.1 Data Protection Act 1998

Since 1st March 2000 the key legislation governing the protection and use of personal data has been the Data Protection Act 1998. The Data Protection Act 1998 does not apply to information relating to the deceased or data which does not constitute personal data.

9.2 Human Rights Act 1998

The Human Rights Act 1998 implements the provisions of the European Convention of Human Rights (ECHR). Article 8 of the ECHR guarantees respect for a person's private and family life. Article 8 is not an absolute right, public authorities are permitted to interfere with it if it lawful and proportionate to do so. Disclosure of personal information

only in ways that comply with the Data Protection Act 1998 is likely to comply with the terms of the Human Rights Act 1998.

9.3 Common Law Duty of Confidentiality

All staff working in both the statutory and independent sector should be aware that they are subject to a common law duty of confidentiality and must abide by this.

9.4 Freedom of Information (Scotland) Act 2002

The Freedom of Information (Scotland) Act 2002 (FOISA) requires public authorities to put procedures in place to facilitate disclosure of information under the Act. Generally, personal data is exempt from the requirements of FOISA.

10. Policy in Practice

10.1 Implementation, Dissemination & Training

Managers within an organisation that has agreed to adhere to the terms of the Policy must ensure that:-

- All supporting policies and procedures necessary to comply with the Policy are implemented within their own organisation
- Their staff are aware of the terms of the Policy and the Information Commissioner's Code of Practice.
- Their staff receive the appropriate training to adhere to the terms of the Policy and any subsequent Data Sharing Agreements.

10.2 Retention & Storage of Data

Organisations that have agreed to adhere to the terms of the Policy must ensure that all personal information they hold in relation to this Policy is stored and destroyed in accordance with their own Data Protection and/or Retention and Destruction Policy unless a separate process has been agreed under a Data Sharing Agreement.

10.3 Breaches & Complaints

10.3.1 Any breaches of the Policy must be brought to the immediate attention of the Data Controller within the organisation where the breach occurred. The Data Controller should carry out an internal investigation to identify the cause of the breach.

10.3.2 Any individual wishing to make a complaint regarding how their personal information has been handled should do so through the appropriate organisations Complaints Procedure.

10.3.3 Organisations that have agreed to adhere to the terms of the Policy are responsible for giving an individual general advice and support on how to progress a complaint or concern under the Policy.

10.4 Rectification, Blocking, Erasure & Destruction

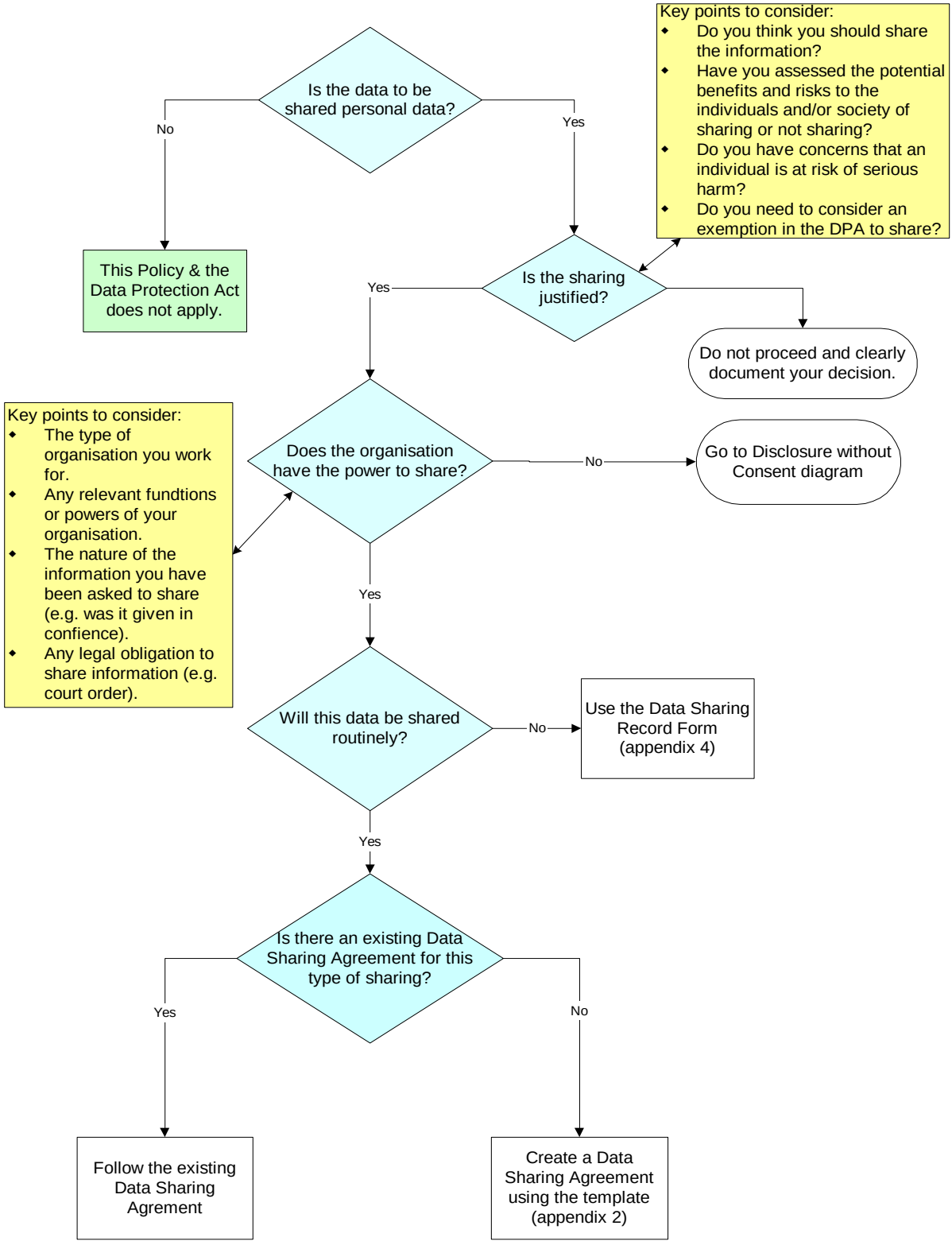
10.4.1 Organisations that have agreed to adhere to the terms of the Policy are responsible for ensuring that their Data Protection Policy covers the procedure for responding to a Notice or Court Order requiring rectification, blocking, erasure or destruction of personal data.

11. Review

11.1 The Policy will be reviewed every three years or more regularly if necessary due to changes in legislation, guidance or good practice. The review will be organised by Shetland Islands Council's Governance & Law section and should involve representatives from:-

- Shetland Islands Council
- NHS Shetland
- Northern Constabulary
- Voluntary Action Shetland
- Shetland Data Sharing Partnership

Shetland Data Sharing Policy – Appendix 1
Data Sharing Decision Process



DATA SHARING AGREEMENT

Between

List Organisations

1. Introduction

1.1 This is a Data Sharing Agreement (the Agreement) supported by the Shetland Data Sharing Policy (the Policy). The Policy forms part of the Agreement. By agreeing to the terms of the Agreement, all parties have undertaken to implement and adhere to the terms of the Policy.

2. Purpose

2.1 The purpose of the Agreement is to facilitate the exchange of data .....

Outline the following:-

- The justification for data sharing –
  - What is the sharing meant to achieve?
  - What are the benefits and risks of sharing or not sharing?
  - Is the sharing proporionate?
  - Could the objective be achieved without sharing personal data?
- The power for data sharing –
  - Any relevant functions or powers of the organisation.
  - Any legal obligation to share information.

3. Data to be Shared

3.1 Outline the following:-

- What data will be shared by each of the parties to the Agreement.
- Where necessary, identify posts which are responsible for sharing or receiving the data.

4. Recording the Data Sharing

4.1 If necessary, consider having a Data Sharing Decision Form detailing the data sharing. This may not always be necessary depending on the type of data, what is being shared and how often it occurs. There may be other ways the data sharing is recorded – e.g. on a care plan for an individual.

5. Consent

5.1 Outline the following:-

- **Whether consent is necessary before the data is shared.**
- **The process for obtaining consent.**
- **If there a specific consent form to be used.**
- **If there a specific privacy notice to be given to the individual when seeking consent.**
- **Any capacity issues that should be considered.**

- **Where consent is not required – the justification for data sharing without consent must be clearly stated.**

6. Security

6.1 **Outline the security measures to be taken when data sharing so the parties to the Agreement are clear how the data will be physically passed between the organisations.**

7. Retention & Storage of Data

7.1 **The parties to the Agreement are responsible for ensuring all personal data they hold under the Agreement is stored and destroyed in accordance with their own Data Protection and/or Retention and Destruction Policy.**

Alternatively, a specific retention and destruction period may be agreed between the parties and should be detailed here.

8. Responsibilities

8.1 **The parties to the Agreement are responsible for ensuring their staff are bound by the Agreement and adhere to its terms. The parties are individually responsible for ensuring that all supporting policies and procedures necessary to comply with the Agreement are implemented within their own organisation.**

Alternatively, there may be a need to specify that a particular training programme or procedure is required to enable compliance with the Agreement.

9. Individual Rights of Access to Data

9.1 **The parties to the Agreement are responsible for ensuring they have the necessary policies and procedures in place to deal with a request from an individual to access their personal data and an explanation of how it has been handled under the Agreement.**

Alternatively, there may be a need to specify a particular process for individuals to follow if they are exercising any of their access rights. E.g. a single point of contact where there are multiple organisations involved.

10. Complaints & Breaches

10.1 **Any breaches of the Agreement identified by the parties must be brought to the immediate attention of the Data Controller within the agency where the breach occurred. The Data Controller should carry out an internal investigation to identify the cause of the breach.**

10.2 **Any individual wishing to make a complaint regarding how their personal data has been handled under the Agreement should do so through the appropriate organisation's internal Complaints Procedure.**

10.3 The parties to the Agreement are responsible for giving an individual general advice and support on how to progress a complaint or concern under the Policy.

Alternatively, there may be a need to specifiy that a particular process for dealing with complaints and breaches that is required. E.g. a single point of contact where there are multiple organisations involved.

11. Rectification, Blocking, Erasure & Destruction

11.1 The parties to the Agreement are responsible for ensuring that their Data Protection Policy covers the procedure for responding to a Notice or Court Order requiring rectification, blocking, erasure or destruction of personal data.

12. Review

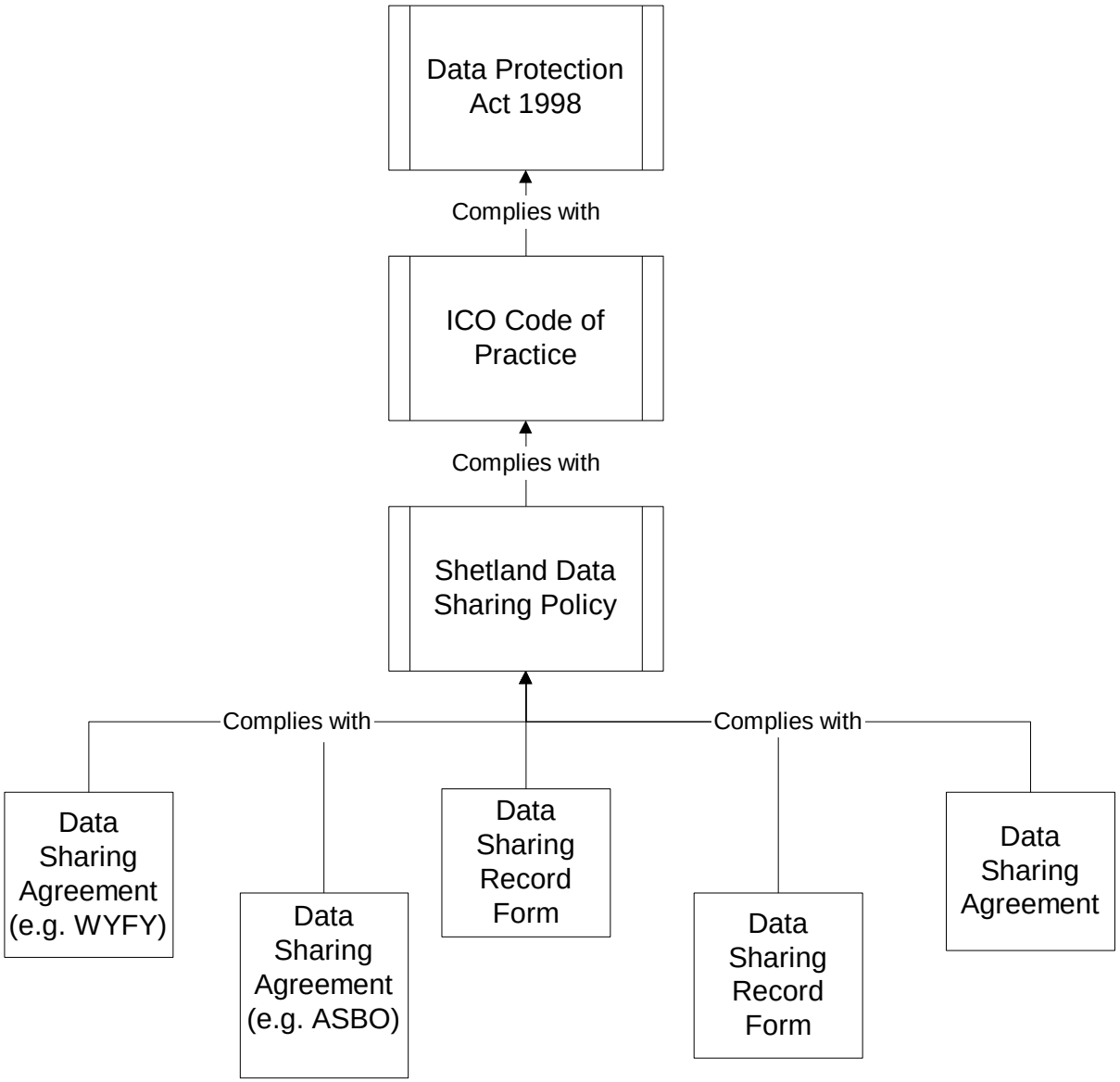
12.1 The Agreement will be reviewed [insert appropriate period] or more regularly if necessary due to changes in legislation, guidance or good practice. The review will be organised by [insert appropriate organisation] and should involve:-

- **Detail what organisations should be represented.**

12.2 The following information will be prepared and considered at the annual review:-

- **Detail any annual reports, statistical information, analysis of the data sharing, etc. that is required to help inform the outcome of the review.**
- **Detail if the outcome of the review has to be reported to any particular group or organisation.**

Shetland Data Sharing Policy – Appendix 3
Data Sharing Structure

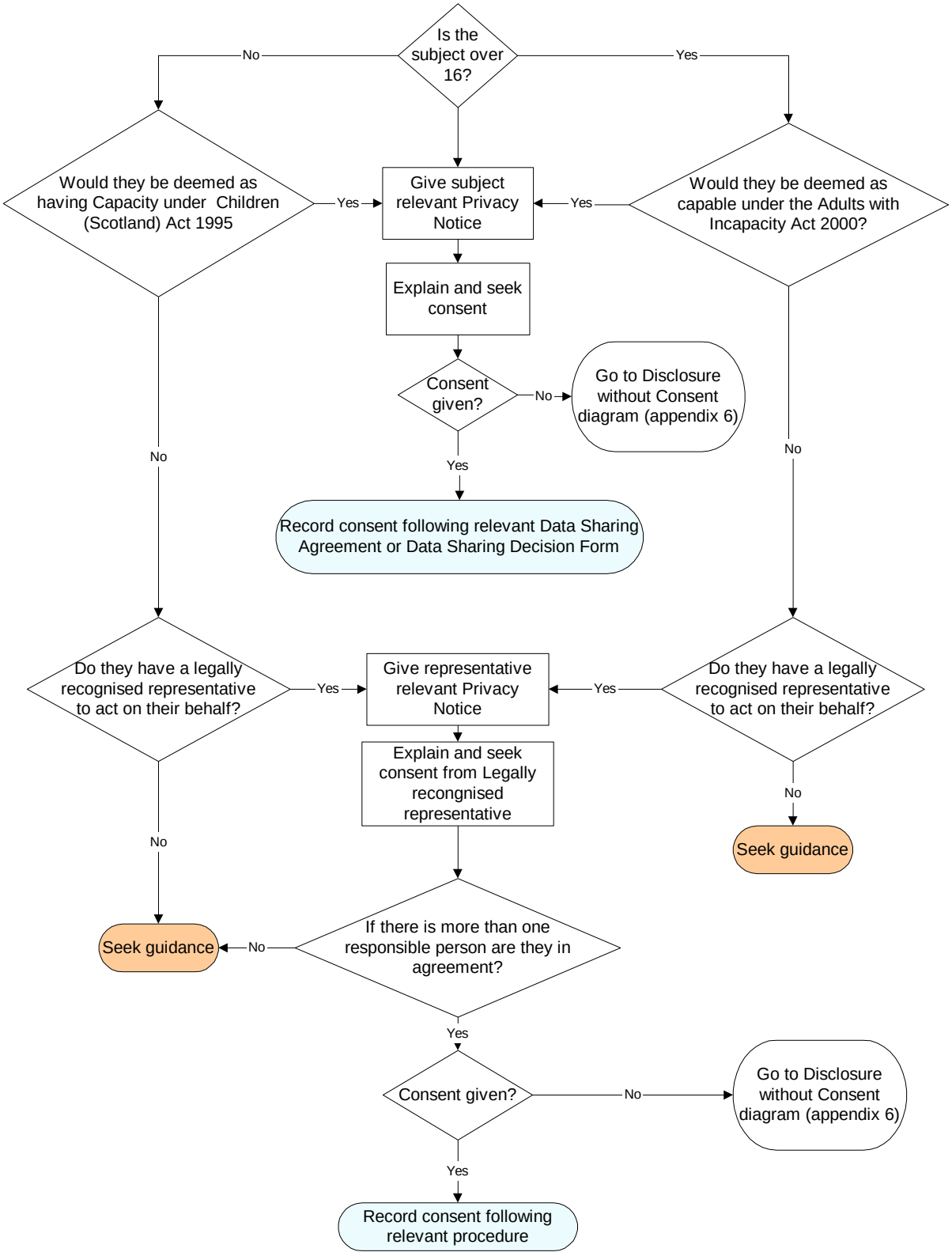


Appendix 4 – Template Data Sharing Decision Form

DATA SHARING DECISION FORM

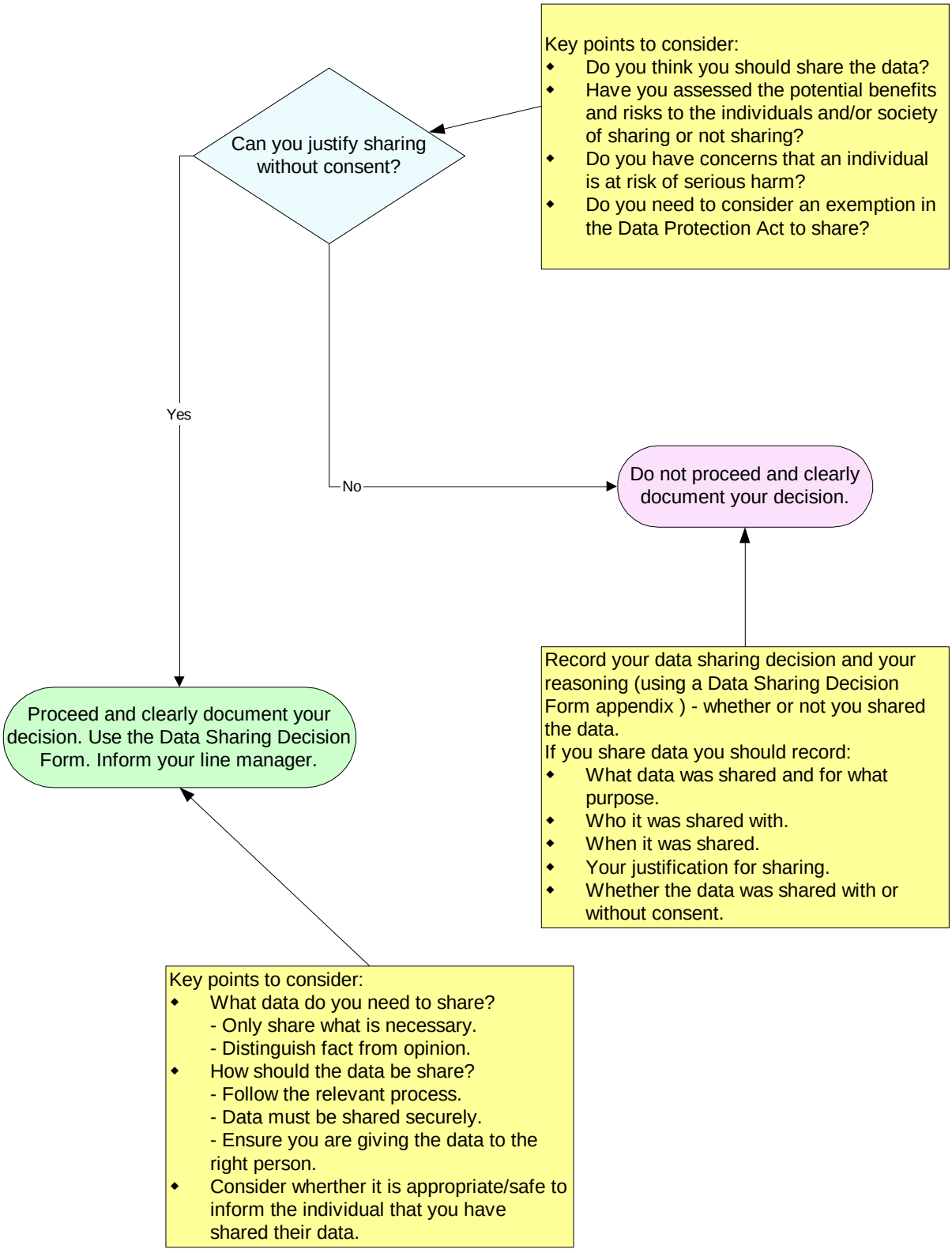
Name of organisation:	
Name & position of person requesting data:	
Date request received:	
Data requested:	
Purpose:	
Decision:	
Data supplied:	
Has the individual given their consent?	
Reason(s) for sharing or not sharing:	
Secure method of data transfer:	
Any specific arrangements re: retention/deletion of data:	
Decision taken by (name & position):	
Date of disclosure:	
Any other relevant information:	
Signed:	
Date:	
Signed:	
Date:	

Shetland Data Sharing Policy – Appendix 5
Data Sharing With Consent



Shetland Data Sharing Policy – Appendix 6
Data Sharing Without Consent

Add a key point that consent should be asked even if sharing can be justified without consent.



Appendix 7 – Contact Details

Contact Details

Shetland Islands Council

Team Leader – Administration
Governance & Law
Office Headquarters
8 North Ness Business Park
Lerwick ZE1 0LZ
(01595) 744550
administrative.services@shetland.gov.uk

Team Leader – Legal
Governance & Law
Office Headquarters
8 North Ness Business Park
Lerwick ZE1 0LZ
(01595) 744550
legal.services@shetland.gov.uk

NHS Shetland

Caldicott Guardian (Medical Director)
Brevik House
South Road
Lerwick ZE1 0TG
(01595) 743060

Data Protection Lead (Finance Director)
Brevik House
South Road
Lerwick ZE1 0TG
(01595) 743060

Information Governance Lead (Information Manager)
Breiwick House
South Road
Lerwick ZE1 0RB
(01595) 743059

Northern Constabulary

Contact details awaited

Voluntary Action Shetland

Development Officer
Market House
14 Market Street
Lerwick ZE1 0JP
(01595) 743902
vas@shetland.org

Shetland Data Sharing Manager

Children's Services
Hayfield House
Hayfield Lane
Lerwick
ZE1 0QD
Tel (01595) 744000
jane.cluness@shetland.gov.uk

Equality Impact Assessment

Part 1

Title of document being assessed	*Shetland Data Sharing Policy*
Is this a new or an existing policy, procedure, strategy or practice being assessed?	New policy.
Please give a brief description of the policy, procedure, strategy or practice being assessed	The Policy provides a framework for data sharing. which supports practitioners to share data confidently and legally. It also informs individuals of the reasons why their data may need to be shared and how that will happen.
What is the intended outcome of this policy, procedure, strategy or practice?	To support practitioners to share data confidently and legally.
Please list any existing documents which have been used to inform this Equality and Diversity Impact Assessment	The Information Commissioner's Data Sharing Code of Practice. SIC Equality and Diversity Policy.
Has any consultation, involvement or research with people from protected characteristics informed this assessment? If yes please give details.	No.
Is there a need to collect further evidence or to involve or consult people from protected characteristic on the impact of the proposed policy? (Example: if the impact on a group is not known what will you do to gather the information needed and when will you do this?)	No.

Part 2

Which protected characteristics will be positively or negatively affected by this policy, procedure or strategy?

Please place an X in the box which best describes the overall impact. It is possible for an assessment to identify that a positive policy can have some negative impacts and vice versa. When this is the case please identify both positive and negative impacts in Part 3 of this form.

If the impact on a protected characteristic is not known please state how you will gather evidence of any potential negative impacts in the relevant section of Part 1.

	Positively	**Negatively**	**No Impact**	**Not Known**
Ethnic Minority Communities (consider different ethnic groups, nationalities, language barriers)			X	
Gender			X	
Gender Reassignment (consider transgender and transsexual people. This can include issues such as privacy of data and harassment)			X	
Religion or Belief (consider people with different religions, beliefs or no belief)			X	
People with a disability (consider attitudinal, physical and social barriers)			X	
Age (consider across age ranges. This can include safeguarding, consent and child welfare)			X	
Lesbian, Gay and Bisexual			X	
Pregnancy and Maternity (consider working arrangements, part-time working, infant caring responsibilities)			X	
Other (please state)				

Part 3

Have any positive impacts been identified? (We must ensure at this stage that we are not achieving equality for one group at the expense of another)	No.
Have any negative impacts been identified? (Based on direct knowledge, published research, community involvement, customer feedback etc.)	No.
What action is proposed to overcome any negative impacts? (e.g. involving community groups in the development or delivery of the policy or practice, providing information in community	Not applicable.

languages etc)	
Is there a justification for continuing with this policy even if it cannot be amended or changed to end or reduce inequality without compromising its intended outcome? (If the policy shows actual or potential unlawful discrimination you must stop and seek legal advice)	Not applicable.
How will the policy be monitored? (How will you know it is doing what it is intended to do? e.g. data collection, customer survey etc)	There is a 3 year review written into the Policy. A review can be undertaken at any time if required. Each partner organisation collects information on data breaches via their complaints procedures.