Data Protection Policy

Document Information	
Document Name/Description/Location	Data Protection Policy 2023 o:\asoffice\data protection\policies and procedures\drafts\data protection policy 2023 v01.01.docx
Version Number *e.g. V1.1*	02.00
Author [Name and Post Title]	Kristen Johnston, Team Leader – Legal
Lead Officer/Manager [Name and Post Title]	Christine Ferguson Director of Corporate Services / Senior Information Risk Owner
Final Approval Date	22 February 2023
Approved by – *Council/Committee/Group/Manager*	Shetland Islands Council
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	01.00	01.01	new draft for consultation - agenda management
22/03/2023	01.01	02.00	Final approved version for publication

Contents

Document Information 1
1. Introduction 3
2. Responsibilities 4
3. Data Protection Definitions 5
4. The Data Protection Principles 8
5. Accountability and Governance of Data Protection 11
6. Individual Rights 13
7. Data Processing Agreements (DPA) and Data Sharing Agreements (DSA) 14
8. Privacy Notice or Statement 14
9. Data Protection Impact Assessment (DPIA) 15
10. Data Security Incidents/Data Breaches 15
11. Contact & Questions 16
Appendix 1 - Frequently Asked Questions & Answers 17

1. Introduction

1.1 Shetland Islands Council (the Council) is committed to ensuring that all personal information about individuals we process is managed appropriately and in compliance with the UK GDPR, the Data Protection Act 2018, and any subsequent data protection legislation (collectively referred to as Data Protection legislation).

1.2 The purpose of the Data Protection Policy (the Policy) is to assist staff in complying with Data Protection legislation.

1.3 The Council regards the lawful and correct treatment of personal information vital to its successful operations, and to maintaining confidence between the Council, its staff and those with whom it carries out business. We want users of our services and staff to feel confident about how personal information is created, obtained, stored and used by the Council.

1.4 Shetland Islands Council Corporate Plan – Our Ambition 2021-2026:

> "Our ambition is for the council to be a fabulous place to work, through exceptional employee experience, talented managers and leaders, and a culture underpinned by our values, kindness, fairness and equality.
>
> We will maintain a clear focus on delivering excellent services to the public."

1.5 Shetland Islands Council Customer First Charter:

> Customer Charter – Putting you first… we will:
> - Respond promptly when you contact us
> - Resolve issues as quickly as possible
> - Be polite, helpful and professional at all times
> - Treat everyone with equity and fairness
> - Communicate clearly, avoiding jargon
> - Maintain confidentiality, ensuring only those who need to see your information do so
> - Take responsibility and rectify any mistakes we make
> - Use your views to help us improve the way we do things

1.6 The Policy should be read alongside other relevant Council policies, guidance and information:

- Data Protection Statement
- ICT Security Policy
- Information Governance Policy
- Data Protection Impact Assessment Guidance, screening questions and template
- Data Breach Guide & notification form
- Information Asset Register and Personal Information Register

- Retention & Destruction Schedule
- Privacy Notices/Statements
- Shetland Data Sharing Framework
- SIC Homeworking Policy
- CCTV Policy [project due 2023 to complete this]
- Information Security Policy (to be developed)

1.7 Other helpful resources can be found on the UK Information Commissioner's Office website - https://ico.org.uk/.

2. Responsibilities

2.1 Chief Executive
Has overall responsibility for ensuring the Council's compliance with this policy and with Data Protection legislation.

2.2 Senior Information Risk Owner
The Council has designated the Director of Corporate Services as the Senior Information Risk Owner (SIRO). This means they have oversight of data protection and other aspects of information governance.

2.3 Data Protection Officer
The Council has appointed the Chief Legal Officer and Executive Manager of Governance & Law as the Data Protection Officer (DPO). The DPO has day-to-day responsibility for monitoring compliance with this policy, advising the organisation on data protection matters and for receiving reports of personal data incidents for escalation as appropriate. The DPO also provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for individuals (staff and customers) and the Information Commissioner's Office (ICO).

2.4 Senior Information Asset Owners (Directors)
The Council has designated Directors as Senior Information Asset Owners. They are responsible for ensuring that all systems, processes, records and datasets within their business area are compliant with this Policy and Data Protection legislation; for assisting the DPO in their duties through providing all appropriate information and support; for ensuring that their staff are aware of their data protection responsibilities; and consulting the DPO on new developments or issues affecting the use of personal data in the organisation; for ensuring DPIA's are conducted as appropriate on data processing activities in their business area, drawing on advice from the DPO.

2.5 Information Asset Owners (Executive Managers)
The Council has designated Executive Managers as Information Asset Owners. They are responsible for ensuring information management policies and procedures are followed, recognising actual or potential security incidents, consulting their Senior Information Risk Owner on incident management, and ensuring that information asset registers are accurate and up to date and that appropriate monitoring and reporting is in place.

2.6 All Employees

Each member of staff is responsible for understanding and complying with relevant policies and procedures for handling personal information appropriate to their role, and for immediately reporting any event or breach affecting personal information held by the Council.

2.7 Information Governance Board

Responsible for ensuring that the Council develops the governance, accountability and strategic direction of all corporate information asset management now and in the future. The Board's purpose is to support and drive the information governance agenda, and provide the Council with assurance that there is legal compliance and that there are effective information governance best practice mechanisms in place.

2.8 Risk Board

The Council's Corporate Management Team meets as a Risk Board with responsibility for driving the management of risk across the organisation by ensuring the Risk Management Strategy and Policy are fully implemented and complied with.

3. Data Protection Definitions

Data Controller	Any person (or an organisation) who decides how, and for what purposes, personal information is held and processed (used). Shetland Islands Council is a Data Controller.
Data Processing Agreement	This is a legal requirement whenever the Council uses a data processor to manage or use personal data. The agreement ensures the data processing is clearly communicated and understood by both parties. It aims to ensure that methods of sharing, storing, use, in transit, backups, destruction, etc. are agreed before sharing with the data processor happens. More information at section 7 of this document.
Data Processor	This role is carried out by any person (or organisation) other than an employee of the Council, who processes (uses) personal information on the Council's behalf and in accordance with the Council's instructions. A Data Processor has no right to decide what happens to the personal information.
Data Protection Impact Assessment (DPIA)	An assessment tool to help you identify and minimise the data protection risks of a project. Depending on the type of personal information involved and how it will be used, a DPIA may be a legal requirement. The end product of a DPIA is an action plan outlining what has to be

	done to ensure a project is compliant with data protection legislation. More information at section 9 of this document.
Data Sharing Agreement	A commitment and agreement between organisations that specifies the arrangements required to ensure secure and appropriate sharing of personal information. There are no data processors involved and each organisation is in full control of the data being shared. More information at section 7 of this document.
Data Subject	Any living individual who is the subject of personal information.
Information Asset Register	Spreadsheet detailing all information held by individual teams/directorates, location, use/purpose, etc.
Information Commissioner's Office (ICO)	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Joint Data Controllers	There are people or organisations who jointly process and share information for the same purpose.
Personal Data or Information	Any information relating to a living individual who can be identified from that information. Includes names, addresses, telephone numbers, etc. Also includes expressions of opinion about the individual and of any intention or decisions taken in respect of an individual.
Personal Information Register	Spreadsheet detailing all personal information held by individuals teams/directorates, location, use/purpose, etc. A sub-set of the Information Asset Register above.
Privacy Notice or Statement	This tells people what the Council does with their personal data. A Privacy Notice or Statement explains why the Council needs their data, what we will do with it and who we are going to share it with. The Council has a template Privacy Statement and the register of completed Statements can be found here. More information can be found at section 8 of this document.
Processing	This is the term used within data protection legislation to describe any use or operation related to the holding, organisation, retrieval, disclosure and deletion of data. Put simply, the term processing covers anything the Council does with personal information.
Retention & Destruction Schedule	This document describes an organisations records and provides instructions for when records will

	be destroyed. The Council's Retention & Destruction Schedule can be found here.
Special Category Data (Sensitive Personal Data)	This is information that specifically relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life or sexual orientation, criminal convictions & alleged offences and biometric or genetic data. There are stricter conditions applicable when this type of personal data is processed (used).

4. The Data Protection Principles

4.1 The Council will at all times comply with the data protection principles in respect of all personal information processed by us. This includes personal information relating to staff, volunteers, service users, customers, potential customers and business contacts.

All personal data will be:-

1) Processed fairly, lawfully and transparently (see our Privacy Notices)

2) Collected for specific purposes and not used for incompatible purposes (see our Personal Information Registers)

3) Adequate, relevant and limited to what is necessary

4) Accurate and, where necessary, kept up to date

5) Retained no longer than necessary (see our Retention & Destruction Schedule)

6) Kept securely (see our ICT Security Policy)

4.2 There is more detailed information on each principle in the next section of the Policy and the ICO has guidance on the data protection principles which can be found here.

4.3 Principle 1 – Processed Fairly, Lawfully & Transparently

Fairness

- Consideration has been given to how using the personal data may affect the individuals concerns and that any adverse impact is justified.
- People's personal data is only handled in ways they would reasonably expect, or any unexpected processing is justified.
- People are not deceived or misled when their personal data is collected.

Lawfulness

- An appropriate lawful basis (or bases) has been identified for our processing of personal data and special category data.
- Nothing unlawful is done with personal data.
- Advice on what is the appropriate lawful basis for processing personal data can be obtained from the Data Protection Officer.

Transparency

- The Council should be open and honest about how personal data is used and comply with the right to be informed.
- This principle is met by having clear Privacy Notices or Statements for staff and customers explaining how their personal data is used.
- The Council's Privacy Notices are found here – [insert link].
- The Council's Template Privacy Notice is attached as Appendix 1.
- The Data Protection Officer provides advice on the content of Privacy Notices and approves them before publication.

4.4 Principle 2 – collected for specified, explicit and legitimate purposes

- There are clearly identified purpose or purposes for processing personal data.
- Those purposes should be documented in the Personal Information Registers and will also be detailed in any DPIA, Data Processing Agreement or Data Sharing Agreement.
- Details of the purpose will be included in Privacy Notices (see above).
- Processing of personal data is regularly reviewed and where necessary documentation and privacy notices are updated.
- If a new purpose is proposed, it should be compatible with the original purpose.

4.5 Principle 3 – Adequate, Relevant & limited to what is necessary

- **Adequate**
- Sufficient to properly fulfil the identified purpose for using the personal data.

- **Relevant**
- Has a rational link to the identified purpose above.

- **Limited to what is necessary**
- Do not hold more than is required for the identified purpose above.

Also known as the data minimisation principle because only the minimum amount of personal data should be held and used to fulfil the identified purpose. This is the first of three principles about data standards, along with accuracy and storage limitation.

4.6 Principle 4 – Accurate and where necessary, kept up to date

- Ensure the accuracy of any personal data created or recorded.
- There are appropriate processes in place to check the accuracy of any personal data collected and the source of that data is recorded.
- There are appropriate processes in place to identify when data needs to be updated to properly fulfil the purpose for having the personal data, and the data is then updated as necessary.
- If a record is required of any mistakes or errors, it is clearly identified as such.
- Records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- There is compliance with the individual's right to rectification and careful consideration given to any challenges about the accuracy of personal data.
- A record will be kept of any challenges to the accuracy of personal data.

This is the second of three principles about data standards, along with data minimisation above and storage limitation below.

4.7 Principle 5 – Retained no longer than necessary

- It is known what personal data is held and why it is needed.
- There is careful consideration and justification for how long personal data is kept.
- The Council's Retention & Destruction Schedule contains standard retention periods in line with documentation obligations
- Personal information is regularly reviewed and erased or anonymised when no longer required.
- There are appropriate processes in place to comply with individuals requests for erasure under the right to be forgotten.
- Personal data that needs to be kept for public interest archiving, scientific or historical research, or statistical purposes is clearly identified.

This principle is sometimes known as the storage limitation principle and is the third of three principles about data standards. Even if personal data is collected and used fairly and lawfully, it cannot be kept for longer than is actually required.

The data protection legislation does not set specific time limits for different types of personal data. How long the data is required or needed will depend on the purpose for which it is being used.

4.8 Principle 6 – Kept Securely

- There must be an analysis of the risks presented by the processing or use of personal data which is used to identify the appropriate level of security to be put in place.
- When deciding what measures to implement, the most recent developments and costs of implementation will be taken into account.
- The Council has an ICT Security Policy
- Where necessary, additional policies and controls are put in place.
- Information security policies will be regularly reviewed and updated/improved as necessary.
- There should be an assessment of what needs to be done by considering what the security outcomes are.
- Completion of a Data Protection Impact Assessment will help assess the security risks.
- Personal data must be appropriately safeguarded against accidental destruction, theft or any other loss.
- The Council has a Homeworking Policy. Homeworkers are responsible for keeping all information associated with the Council secure at all times, ensuring reasonable precautions are being taken to maintain confidentiality in accordance with the Data Protection Act.

5. Accountability and Governance of Data Protection

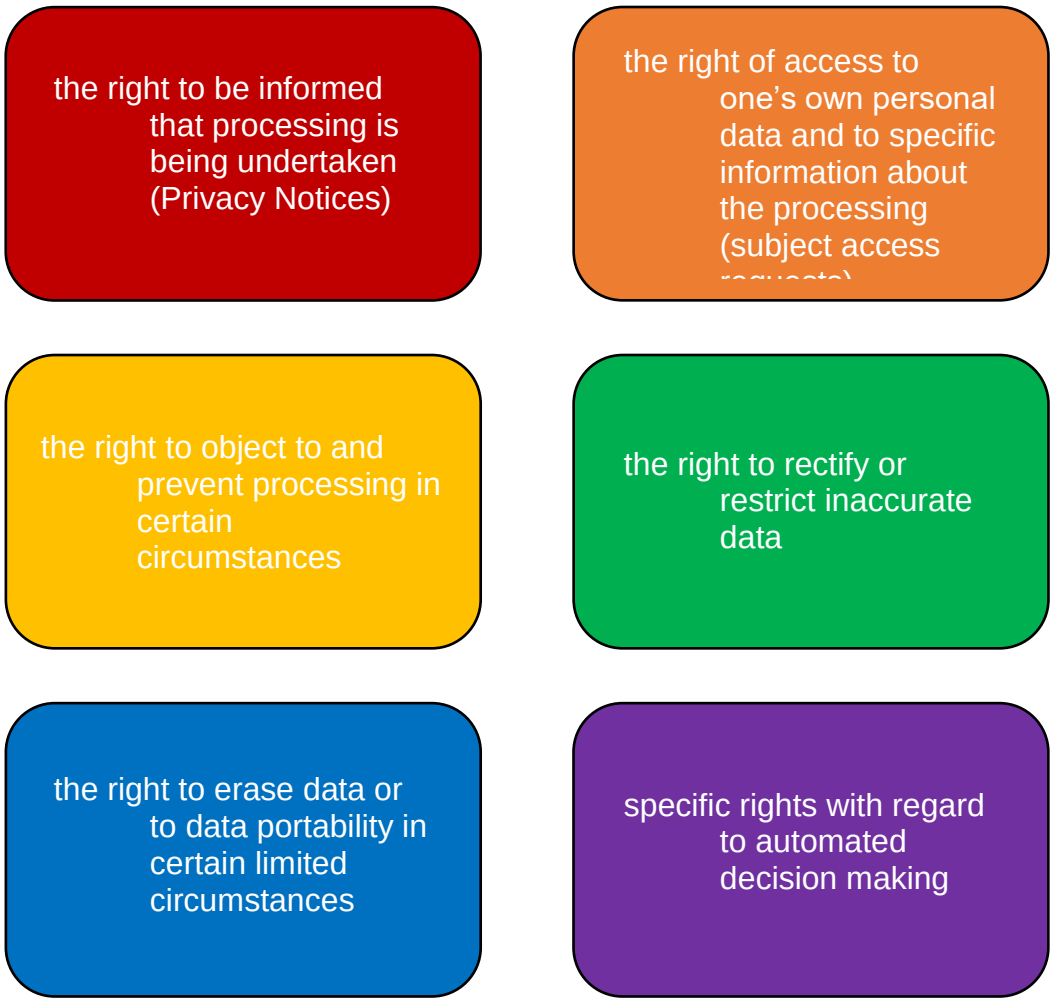
5.1 Accountability is a further principle of data protection legislation which requires the Council to demonstrate its compliance. The Council must maintain oversight and transparency in the management of personal data. To meet our accountability duties, the following records will be kept:-

1) Up to date **privacy notices or privacy statements** for colleagues, customers and service users (see published Register of Privacy Statements);
2) A **Personal Information Register** describing the personal data held, purpose, controls and accountability for each data system or set of records (each Team/Service area holds their own Personal Information Register);
3) A **Data Breach Log** which describes incidents that have impacted on personal data held by the Council (see section 10 below);
4) A **Data Protection Advice Log** which describes data protection advice provided by or on behalf of the DPO;
5) **Data Protection Impact Assessments** will be completed when legally required and as a matter of good practice on the acquisition and development of new information systems and on proposals for significant new business processes and change (see section 9 below); and
6) **Contracts** with organisations who are processing personal data on behalf of the Council will have the relevant data protection contract clauses and

be subject to appropriate levels of review and oversight (data processor agreements).

6. Individual Rights

6.1 The Council will ensure that individuals rights over their personal data are respected. These rights include:



6.2 All requests made by individuals (colleagues, staff, contacts, customers & service users) relating to their personal data rights must immediately be forwarded to the Data Protection Officer who will ensure that appropriate actions are taken, and a response issued without undue delay and at least within one month.

The Data Protection Officer's contact details are:-

8 North Ness Business Park,
Lerwick,
Shetland
ZE1 0LZ

E-mail: dataprotection@shetland.gov.uk

Telephone: (01595) 744 550.

7. Data Processing Agreements (DPA) and Data Sharing Agreements (DSA)

7.1 Both DPAs and DSAs provide frameworks for the secure and confidential collection, control, storage and sharing of information between participating partner agencies or organisations. It contains an agreed set of principles about sharing personal or confidential information, and, enables each organisation to understand the legal powers and circumstances in which it should share information and what their responsibilities are.

7.2 A DPA is a legal requirement whenever the Council uses a data processor to manage or use personal data. The agreement ensures the data processing is clearly communicated and understood by both parties. It aims to ensure that methods of sharing, storing, use, in transit, backups, destruction, etc. are agreed before sharing with the data processor happens.

7.3 A DSA is a commitment and agreement between organisations that specifies the arrangements required to ensure secure and appropriate sharing of personal information. There are no data processors involved and each organisation is in full control of the data being shared.

7.4 Advice from the Council's Data Protection Officer must be obtained before signing a DPA or DSA. The DPO should maintain a central record of all DPAs and DSAs, but the service/officer should also retain a copy.

8. Privacy Notice or Statement

8.1 A Privacy Notice or Statement tells people what the Council does with their personal data. A Privacy Notice or Statement explains why the Council needs their data, what we will do with it and who we are going to share it with.

8.2 Transparency is a key data protection principle (see Principle 1 above). Being transparent facilitates the exercise of individuals' rights and gives people greater control (individual right to be informed – see above). The Council's Privacy Statements will include:-

- All relevant contact information and the DPO's contact details.
- The purposes of the processing and the lawful bases for processing.
- The types of personal data obtained and the source of that data.
- Details of all personal data that you share with other organisations and, if applicable, details of transfers to any third countries or international organisations.
- Retention periods for the personal data.
- Details about individuals rights including, if applicable, the right to withdraw consent and the right to make a complaint.
- Details of whether individuals are under a statutory or contractual obligation to provide the personal data.
- Information regarding the source of the processed personal data if it is not obtained from the individual concerned.

8.3 The Council has a template Privacy Statement and a register of Privacy Statements or Notices is published on the Council website.

8.4 Each Directorate/Service needs to determine how best to tell the public about how their personal data is used to deliver a particular service. All new Privacy Statements or amendments to existing Privacy Statements have to be approved by the DPO prior to publication.

9. Data Protection Impact Assessment (DPIA)

9.1 A DPIA is an assessment tool to help you identify and minimise the data protection risks of a project. DPIAs are required for any processes that are likely to result in a high risk to data subjects' interests and will assist the Council in adopting a 'privacy by design' culture. Depending on the type of personal information involved and how it will be used, a DPIA may be a legal requirement. The end product of a DPIA is an action plan outlining what has to be done to ensure a project is compliant with data protection legislation.

9.2 Completing a DPIA is a key part of the Council's accountability obligations (see Section 5 above) and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations. The DPIA does not have to eradicate all risk, but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

9.3 DIPAs should be a flexible and scalable tool that does not have to be complex and time consuming in every case. There must be a level of rigour in proportion to the privacy risks arising.

9.4 DPIA guidance, screening questions and the template DPIA is published on the Intranet. The DPIA screening questions help you identify when a DPIA is a legal requirement and must be completed before commencing a DPIA.

10. Data Security Incidents/Data Breaches

10.1 Any data security incidents (or data breaches) which may impact on the confidentiality, integrity or availability of personal data held by the Council must be reported immediately to the Data Protection Officer via the e-mail address above, including a completed Data Breach Notification Form.

10.2 A data security incident could include:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

10.3 There may still be a data breach where both the sender and the recipient work for the Council, but in different departments or service areas. Both are bound by the same employee code of conduct and Council policies. The recipient should immediately delete the information and inform the sender. It is very unlikely that there would be any risk of harm or detriment to the data subject, even if special category personal data is involved. However, the Council must still document the breach internally and provide guidance on minimising risk in the future.

10.4 You must still notify the Data Protection Officer even if you consider no breach occurred, or if the information was recovered or retrieved. This is classed as a "near miss" and it is important for the Council to register these so that lessons can be learned, and patterns of breaches or areas for further training identified.

10.5 All reported incidents will be recorded in the Council's Data Breach Log to ensure appropriate mitigation measures are in place and to identify lessons or necessary improvements.

10.6 The Data Protection Officer will consider whether the data security incident meets the data protection legislation definition of a "personal data breach" which presents a risk to individuals and include a recommendation on whether to report the matter to the Information Commissioner's Office.

10.7 A recommendation to report the matter to the Information Commissioner's office will be notified to the Senior Information Risk Owner (SIRO). The SIRO will then determine if the incident constitutes a reportable data breach and the DPO will report the incident to the ICO and liaise as appropriate.

10.8 If a data breach presents a high risk to the data subject(s) affected, the DPO will ensure they are also notified of the breach.

11. Contact & Questions

A list of frequently asked questions and answers is attached as Appendix 3.

Any questions about the Policy should be directed to the Data Protection Officer:-

Data Protection Officer
8 North Ness Business Park,
Lerwick,
Shetland
ZE1 0LZ

E-mail: dataprotection@shetland.gov.uk

Telephone: (01595) 744 550.

Appendix 1 - Frequently Asked Questions & Answers

Q1 – When do I have to do a Data Protection Impact Assessment?

A – There are screening questions that help you to determine whether a DPIA is legally required or would just be good practice to have. The screening questions and accompanying guidance can be accessed from the intranet or the Data Protection Officer. If you need help completing the screening questions, you should contact the Data Protection Officer.

Q2 – I want to conduct an anonymous survey, do I need to consider data protection?

A – Yes. If your survey includes free text boxes there will be a risk that participants will include personal data that identifies them. Therefore if you want to keep your survey anonymous you should consider if your free text boxes can be removed or provide clear instructions that personal data should not be included & will be removed.

Q3 – There is a general privacy statement for the Council, does my Team need its own specific one?

A – Yes. The general privacy statement is there to provide general information on how the Council uses personal data, but does not give our customers enough information about individual services they may access. There's a template privacy statement that you should use (available on the intranet) and you can get help from the Data Protection Officer. It is worthwhile looking at what other Teams Privacy Statements look like [here].

Q4 – Is there a standard form of wording that summarises how the Council treats personal data for inclusion on forms, letters, etc.?

A – Yes. The standard form of wording approved by the Data Protection Officer is –

The information provided by you is processed in accordance with the Data Protection Act 2018 to allow us to effectively *[insert brief description of the service or purpose].* The Data Protection Act 2018 gives you the right to know how we will use your data. Further information about how we use your personal data is available from *[insert name of service]* or the Council's website at http://www.shetland.gov.uk/information-rights/DataProtection.asp.

Q5 – I want to take photos or a video clip of customers/staff/users, do I need consent?

A – Maybe. If you are taking a broad angled shot of a large group of people from behind and/or you cannot identify any individuals, then you do not

require consent. Although it would be good practice to inform participants that photographs will be taken but that they will not identify individuals.

If you want to take photographs of individuals then you must seek their consent before doing so. Using photographs is unlikely to be a mandatory or necessary part of any service provision, so you will need people's consent to do so. You must tell them what you intend to do with the photograph, particularly if it is going to be published on the internet or used on social media. Individuals must be able to say no and still access the service or event. Where the individuals are children, consent must be sought from their parent, carer or guardian.

You may also wish to consider whether the individual's names need to be included – particularly where the photograph is of children. If the use of names is not necessary, then you should not include any names or further identifiable information.

Q6 – What personal information can I include on social media about customers/staff/users/pupils?

A – None. The Council should never publish personal information about their customers/staff/users/pupils unless they are legally required to do so or have obtained explicit consent from the individual. You should seek advice from the Data Protection Officer before publishing any personal data on social media.

Q7 – I want to use a new app or platform to enhance service delivery, communication between staff or with customers/users/parents. Do I need to complete a Data Protection Impact Assessment?

A – Maybe. See the answer to number 1 above.

Q8 – Can I use photographs that include more than one user in an individual's file?

A – Maybe. If you cannot clearly identify the other individual(s) then this is not personal data and can be used in this way. However, if you can clearly identify the other individual(s) then you have to consider whether it is necessary to have their photograph within another individual's file. It is unlikely that this will be necessary and therefore you should avoid doing this unless there is a clear justification for doing so.

Q9 – Can my Team use closed Facebook Groups to communicate with service users and/or staff?

A – Maybe. You will need to refer to the Council's Social Media Policy and determine if a Data Protection Impact Assessment is required (refer to Q1 above).

Q10 – I have been asked to share personal data with an external organisation, am I allowed to do that?

A – Maybe.

If there is routine data sharing between the Council and the external organisation, it may be that there is already a Data Sharing Agreement in place which will set out how you share safely and securely with them for an agreed purpose. You can check whether there is a Data Sharing Agreement with your manager or the Data Protection Officer.

If this is a one-off request to share data, then the external organisation should make their request in writing. You should then determine whether there is a legal obligation to share information with them (e.g. HMRC, any regulatory bodies, etc.) or the sharing is justified. A record of the data sharing must be kept. You may wish to obtain advice from the Data Protection Officer before sharing personal information.

END OF POLICY