Data Sharing Policy

Contents

Version	Date	Changes	Circulation	Retained
0.1	04/07/2016	First draft for review	Teresa Maley (Information Manager)	No
0.2	18/07/2016	2nd draft for review by key advisors	Kathryn Dickson, Procurement Sandra Blacklock, Procurement Nuala McKinlay, Legal Services Hannah Macleod, Legal Services	No
1.0	21/07/2016	IGG Approved		Yes
1.1	27/02/2020	Updated to reflect new legislation – remove DSA template and consent form added data request forms	Jaimie Taylor (Information Manager)	

2.1	12/02/2024	Review	Jenna Paterson (Information Manager)	
2.2	12/02/2024		Nicola Driver	
2.3	14/02/2024		Gillian Laing	
2.4	08/08/2024	Review	Nathan McBain	
3.0	12/08/2024	Final document	Jenna Paterson	
4.0	24/09/2024	Amendment	Gillian Laing	

Scope

The Data Sharing Policy is for anyone involved in sharing information in the organisation including employees, elected members and third-party contractors sharing information on our behalf.

It also enables those that make decisions on sharing information, including Contract Managers, Strategic and Operational Information Asset Owners to carry out their specialised roles.

Why?

We need to share information in a specific way to make sure we fulfil our **legal duties** to:

- look after information securely and safely.
- be open and transparent.

Following the Policy means you will be implementing the Council's Information Governance Policy and making sure you are meeting your legal responsibilities. It will also provide assurance to external authorities, such as the Information Commissioner's Office, that you are considering data protection obligations prior to sharing information.

1. Deciding to Share Personal Data for the First Time

A record of your decision needs to be recorded. If you are not the Operational Information Asset Owner then you should make sure that **this is agreed with and recorded** by the Operational Information Asset Owner.

You **MUST** always check whether you could achieve the objective by providing 'anonymised data' (information without personal data in it).

If the request needs personal information, before deciding, you should consider whether it is a one-off request or whether the sharing will be on an ongoing basis. **If it is on an ongoing basis then the Council's policy means you must put a Data Sharing Agreement in place (DSA). Before doing this, you should carry out a Data Protection Impact Assessment (DPIA). A DPIA and DSA will often be complementary documents, and it**

is recommended that a DPIA is completed prior to, or in tandem with, the DSA. Additionally, privacy notice may require to be reviewed / updated to ensure this use of information is captured and individuals are informed about the collected and use of their information. (For more information, please refer to DPIA Guidance.)

Before data sharing, you must always check:

- if it is justified and necessary
- if you have a lawful basis to share
- what are the risks (will individuals be damaged, are they likely to object, would it undermine trust in the organisation?)

Once you have decided to share the data you must consider key points and follow good practice to make sure:

- you have a legal basis to share the information
- only necessary information is shared
- it is only shared with relevant individuals/organisations (need to know)
- information is shared securely
- information is not to be held outside of the United Kingdom or European Economic Area (EEA)
- individuals are informed that their information is being shared through a 'Privacy Notice'
- if official-sensitive information is being shared then it is protectively marked
- the data sharing is recorded in the Council's central DSA register maintained by the Information Management Team

It is important to note that the Council should not seek consent from individuals to share their information with other organisations if it is happening as part of the Council's statutory and core functions (you must decide if you will still need to share the data if an individual refuses to consent to it). In these circumstances, seeking consent would be seen as artificial and will be unlawful. However, you do have to inform individuals about the data sharing in a privacy notice. (Please see the staff guide on privacy notices for more information.)

2. Can I Share Information?

It can be important to share information to be able to provide a better service for customers as well as uphold the law.

There are 5 main ways in which we share Council information and these are managed differently:

- **Anonymised data**
- **Third party data processing**
- **Information requests**
- **Data sharing**
- **Ad-hoc data sharing for crime prevention and tax reasons**

2.1. Anonymised Data

If you wish to share information openly, without any agreements, then it needs to be anonymised with no risk of re-identification. This means removing any personal information so individuals cannot be identified from the information.

Sharing data openly can help the public understand more about what you do and allow other organisations to improve their services.

There are fewer legal restrictions when publishing this type of data. It also removes the need to continually respond to information requests as people can access the information online, either by being shown it or finding it for themselves, without any formal process.

However, it is important that the anonymisation is effective. You must assess whether there is a risk of re-identification before releasing the information. This needs to be recorded in the Information Access Register (see Recording Data Sharing below). If you think re-identification could happen, ~~then~~ you should either: anonymise further or share it with a smaller group using a data sharing agreement with a specific purpose. For more information and examples read ICO Anonymisation Code of Practice.

There are also some restrictions regarding health/social care records, for which you should follow the Anonymisation Standard for Publishing Health and Social Care Data.

2.2. Third Party Data Processing

When a third party (out with Scottish Borders Council) processes data on your behalf at your instruction – by holding it, storing it, gathering it, providing it to others – you will need a contract to comply with Data Protection **whether there is a cost involved or not**.

The contract also must be monitored to make sure that the third party are complying with instructions given.

Standing Orders state that if you are setting up a new contract or are not sure if your contract is compliant then you should read the Purchasing Handbook (paragraph 3.1 in particular). For more information contact the Procurement Team.

Regardless of the value of the contract, **any type of purchase transaction for where personal data is involved (or might be involved) must be brought to the attention of the Procurement Service before contact with any possible external provider.**

2.3. Information Requests

'Data sharing' only covers personal information provided between organisations where there is an agreed purpose.

Other requests for Council Information from organisations or individuals are 'Information Requests'. They can include Freedom of Information Requests, Subject Access Requests (SAR) and Environmental Information Requests (EIR).

If you have a routine request for Council information from an individual, and the information is published or you can provide the information without delay, then you can share this information.

However, if

- you do not hold the information
- you need time to look into it
- it covers multiple services
- you don't want to release some or all the information or
- you think you might not be able to make the deadline

Then, as soon as you receive it, please pass this on to the Information Management Team through the FOI or dataprotection mailbox. They will make sure it is logged, dealt with under the correct legislation and coordinate a response in line with legal timescales.

2.4. Data Sharing

If your service routinely shares personal data with another organisation and there is an agreement in place to share the data then you are free to share the information as long as this is necessary and you follow the instructions set out in the agreement.

If you are unsure, ~~then~~ ask your line manager or operational information asset owner who should be able to help.

If there is no agreement in place, ~~then~~ you should provide the request to your line manager to make a decision on whether it should be released.

2.5. Ad-hoc Data Sharing for Crime Prevention and Tax Reasons

Under Data Protection you are allowed to share personal information for crime prevention and tax reasons. This can be shared proactively or at the request of another authority.

You must make sure the request is justified and recorded. You are responsible for what is released.

When sharing information you must make sure you record the request or release of data so that we can show what has been released and why.

This can be done by making sure that requests are provided on a Standardised form (please see appendix C and D for examples of these forms) and document the reason why information was released in one of the following ways (speak to your line manager for details within your service):

- on a register held by the service (for routine requests) or
- send the request to the Information Management Team through the dataprotection mailbox to register and co-ordinate a response on behalf of the Council (if it is an organisation wide request or not routine for your service).

If these are regular requests then you must have a data sharing agreement, which means you do not need to record each individual request on a register, just the data sharing agreement. However, you should still obtain a standardised (and countersigned) form each time a request is made as evidence you followed best practice.

3. Recording Data Sharing

If you share 'anonymised data', carry out 'data sharing' with another organisation including 'data sharing for crime prevention and tax reasons' then you need to make sure that:

- it is recorded within an Information Access Register
- you retain a copy of the requests

Information Access Register

All data sharing, including data sharing for crime prevention and tax reasons and emergencies, needs to be recorded. When recording these requests you need to document:

- Requestor
- Purpose for sharing
- Description of personal information
- Was information shared?
- Reason for sharing or not sharing
- When was it shared
- Whether it was shared with or without consent
- If OFFICIAL-SENSITIVE information – marking arrangements

See Appendix B for an Information Access Register Form template.

4. Data Sharing Agreements

If you routinely share data with an organisation, you must have a Data Sharing Agreement. They justify your data sharing and provide assurance that you are following the Data Protection Principles.

The Information Management must assess and agree the agreement.

You need to have a Data Sharing Agreement legally to comply with Data Protection.

Data Sharing Agreements can take a variety of forms and can even be included in other agreements such as Service Level Agreements (SLAs), Memorandums of Understanding (MOUs) or Protocols.

They should include:

- Parties involved
- Purpose of data sharing
- Legal Basis for sharing
- Roles and responsibilities
- Data to be shared
- Processes to share the information
- Security and Training
- Breaches of Security

- Data Subject Rights
- Indemnities
- Term and Termination of agreement (including disposal of data)
- Review
- Entire Agreement
- Governing Law and Jurisdiction

You must have the agreement assessed, agreed and recorded by the Information Management Team before signing. For more information, please refer to the data sharing procedure which can be found on the intranet on the Information Management page. There is also a Template Data Sharing Agreement and guide ~~is~~ available.

5. Reviewing Data Sharing

The Operational Information Asset Owner should annually review Data Sharing Agreements and record this on the Information Asset Register.

When reviewing Data Sharing Agreements you should ask the following key questions –

- Is the data still needed?
- Have organisations and/or responsible managers changed?
- Do I need to update the agreement because the information or purpose has changed?
- Do I need to update my privacy notice?
- Are both sides complying with the Data Sharing Agreement? Including information security?

6. Compliance and Monitoring

All services must comply with this Policy.

Data sharing records will be assessed and reviewed through Internal Audit Programme.

An annual quality assurance audit will be undertaken by the Information Management Team to check whether the Information Access Register is being completed and Data Sharing Agreements are held within the Central Register.

7. Further Information

Please read this Policy alongside:

1. The DPIA Procedure, guide and template
2. Data Sharing Agreement template and guide
3. Staff GDPR Guide
4. Privacy Notice Guide
5. The Information Governance Policy
6. The Data Protection Policy

There is further information, guidance and materials available on the **UK Information Commissioner website**

APPENDIX A – Glossary Terms

Anonymised Data – where you cannot identify anyone from the information shared (normally groups of data like statistics)

Third Party Data Processing - sharing information with a third party under a contract for them to carry out your duties

Information Requests – individuals requests for Council information, such as Freedom of Information Requests, Subject Access Requests, Environmental Information Requests and Re-use Requests

Data Sharing – this is a specific term where you share personal data between services within Scottish Borders Council or with other organisations for a specific purpose. (It doesn't include 'third party data processing' or 'anonymised data'.)

Data Sharing For Crime Prevention And Tax Reasons – this is a specific form of data sharing which allow authorities to request or provide personal information under the Data Protection Act 2018 for crime prevention and tax reasons.

Privacy Notice - You must always have a reason for collecting personal information. A Privacy Notice informs individuals, who you are, how you will use their personal data and to whom it will be disclosed.

Data controller – is the organisation which is responsible for deciding how personal data is processed. The Council will normally be the Data Controller in relation to processing carried out by service areas, however, depending on the circumstances there may also be other data controllers e.g. partnership working may require arrangements to be made between multiple organisations/data controllers.

Data processor – is an organisation/individual responsible for processing personal data on the Council's behalf. System providers, contractors, third party organisations might be considered data processors if they handle/store personal data for the Council.

Data protection principles – These provide the framework of how personal data should be processed by an organisation in order to comply with data protection legislation.

Personal data – is any information which identifies a living individual.

Special category data – is particular types of personal data which are considered to be more sensitive e.g. information about health, religious beliefs, political opinions, trade union membership, sexual orientation, ethnicity, and biometric or genetic data.

Conditions of processing – refer to the lawful reasons which allow an organisation to process personal data.

Data Protection Officer (DPO) - is responsible for monitoring the Council's compliance with data protection principles and providing advice to Senior Management on data protection issues. They are also the key contact between the Council and the ICO.

DPIA – an assessment tool to evidence compliance against the data protection principles. It is Council policy for DPIAs to be completed on all occasions when new processes handling

personal data are introduced or changed. It is a mandatory, legal requirement, for organisations to complete a DPIA for all high-risk processing.

High risk processing – is when a process is likely to have a significant impact of the rights and freedoms of individuals, either because it will affect decisions made about individuals or could put them at risk if something goes wrong. The DPO is responsible for deciding whether processing is high risk.

Strategic Information Asset Owner (SIAO) – is responsible for ensuring that all personal data complies with data protection legislation. They should support the completion of DPIAs in accordance with Council policy and are ultimately responsible for authorising whether processing commences and when. Strategic Information Asset Owners are Service Directors.

Operational Information Asset Owners (OIAO) - are responsible for managing information assets and risk at Service Level. They are responsible for ensuring that information risk is managed appropriately within their area and for providing assurances to the Strategic Information Asset Owner (OIAO). Operational Information Asset Owners are normally the service or Group Managers.

Information Commissioner's Office (ICO) – is the UK regulator for data protection legislation. They are responsible for advising on data protection compliance, and enforcement.

Information Risk – risks relating to information which could lead to non-compliance with statutory responsibilities and best practice. Like other risks, information risks should be recorded and managed through the Council's risk management framework.

APPENDIX B – Information Access Register Form

INFORMATION ASSET REFERENCE AND NAME	ORGANISATION REQUESTING INFORMATION	PURPOSE FOR NEEDING INFORMATION	DESCRIPTION OF DATA NEEDED	WAS INFORMATION SHARED?	REASON FOR SHARING/NOT SHARING	DATE SHARED/ DECISION MADE	CONSENT (EXPLICIT, IMPLIED, NO)	OFFICIAL-SENSITIVE?	MARKING ARRANGEMENTS	AGREED BY
From the Information Asset Register	Type in name unless internal then type in SBC/Dept/Service	Type in a brief summary of why the organisation requires the information	Provide the categories of information being requested such as name, address, Date of Birth etc.	Yes or No	State what the lawful basis for releasing the information or why you decided that you could not comply with the request	Click here to enter a date.	Choose an item.	Yes or No	**EG.** As per policy **OR** description of process agreed with partner/dept and why.	Click here name and role of individual.
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“
“	“	“	“	“	“	“	“	“	“	“

This register is for all ‘Data Sharing’ Information Requests including ‘anonymised data’ requests/ publications, ‘data sharing’ and ‘data sharing for crime prevention and tax reasons’. You can record the data sharing agreement where it exists rather than each time a request is made under that agreement but should monitor from time to time that it is current

APPENDIX C – Example of an External Organisation's Data Request Form

HM Revenue & Customs

REQUEST FOR INFORMATION TO BE PROVIDED UNDER THE TERMS OF SCHEDULE 2, PART 1 OF THE DATA PROTECTION ACT (2018)

Declaration – I am making enquiries which are concerned with: -

[ ] The prevention or detection of crime. *

[ ] The apprehension or prosecution of offenders. *

[ ] The assessment or collection of any tax or duty or of any imposition of a similar nature

I can confirm that the data sought is required for the purpose or purposes set out above and that failure to provide it would, in my view, likely to prejudice that or those purposes.

It is essential that the subject of the information is not made aware of our suspicions or enquiries.

Please only provide information currently within your possession and do not seek further information on behalf of HMRC. Ultimately this material could be used in a court or tribunal case.

I certify that I have considered the issues of necessity and proportionality under the Human Rights Act 1998. I consider that the requested disclosure is necessary and proportionate, and that the conditions of Article 8(2), European Convention on Human Rights, are satisfied.

HMRC Data Protection Registration Number Z9034158, Expiry Date 22 May 2020

Details requested:

Signed:	**Position:**
Name (Block letters)	**Date**

APPENDIX D – Example of a SBC Data Request Form

DATA EXEMPTION REQUEST FORM

Request for Disclosure of Personal Data to Scottish Borders Council
Under Sections 2(Part 1) and 4(Part1), Schedule 2 of the General Data Protection Regulations/Data Protection Act 2018

To:	Department:

Address:

I am making enquiries that are concerned with (*delete as appropriate):

Crime and Taxation * (a) the prevention or detection of crime
* (b) the prosecution or apprehension of offenders
* (c) the assessment or collection of any tax or duty or of any imposition of a similar nature

Detail of information required:-

The information sought is needed to:

Location/Address:

I confirm that the personal data requested is required for that/those purpose(s) and failure to provide the information will, in my view, be likely to prejudice that/those purpose(s).

I understand that if any information on this form is omitted or wrong, I may be committing an offence under
Part 6, Section 166 of the Data protection Act 2018.

Name/Signature:	Date:
Email Address:	Telephone Number: