# information governance policy

V 2.0


Scottish Borders COUNCIL

think !nformation

# CONTENTS

# SCOPE

Applies to all: employees, elected members, Community partners, suppliers, agents and representatives, volunteers and temporary staff working for or on behalf of Scottish Borders Council.

Includes all information created, collected or processed by the council (regardless of format, storage, how it is obtained or sharing) as well as historic information passed to the Council from previous Councils.

# OUR DUTY

Scottish Borders Council is committed to creating, managing and keeping records that document its principal activities.

Information must be processed and protected diligently, lawfully and ethically through good data security, accurate information and informed openness.

When managing information we all need to:

- Make sure we comply with legal obligations
- Treat it as a valuable resource
- Make sure it is accessible and available
- Treat it as the Council's information and manage it actively
- Make sure it is accurate and meets customer's expectations
- Make sure we know how we are meant to handle information

# POLICY STATEMENT

Scottish Borders Council regards information as a valuable corporate asset. Data security, accurate information and informed openness are at the heart of the Council's approach to information management.

The Council will take a risk based approach to information governance focussing on safeguarding customers, providing business transparency and ensuring legislative compliance.

The policy sets out the roles and responsibilities for:

- **Governance**
  - To promote the implementation and monitoring of information management arrangements through a defined governance structure, with clear responsibilities and accountabilities that encompasses everyone within the organisation from the Chief Executive as Accounting Officer to the responsibilities of staff.
  - To provide corporate management of incidents, risks, annual information audit reports and information governance arrangements through an Information Governance Group (IGG) who will approve and oversee any improvement plans.
  - To provide a comprehensive Training and Awareness Plan and dedicated Information Management Team to ensure that appropriate knowledge and skill sets are maintained.

- **Legal Compliance**
  - To carry out the Council's duty to be legally compliant when managing data and information; to provide an improved service, reduce reputational risk and monetary fines.

- **Information Security**
  - To make sure data and information is secure (regardless of format). Security is regularly reviewed to ensure that the Council has adequate safeguards in place to: protect existing data and information; be prepared for new information and communication technologies used to improve the way it delivers its services; promote transparency and to safeguard its customers and commercial partners.

- To make sure incidents will be recorded, reported appropriately, investigated thoroughly and acted on promptly, with lessons learned disseminated throughout the Council.

- **Records Management**
  - To promote transparency and information quality assurance so that information is more easily accessible to help deliver operational efficiencies and provide a more effective and timely response to access requests.

- **Informed Access**
  - To make sure data sharing is risk assessed, legally compliant and arrangements are documented and monitored to safeguard customers.
  - To make sure data requests are handled effectively and timely to fulfil legal obligations, promote a spirit of openness and accessibility, whilst safeguarding individuals.
  - To take a proactive approach through data publication, in line with legal obligations, to provide an improved service for customers and reduce the need for individual requests
  - customers are informed of the data and information we hold, what we do with it, what information they have access to and how they can access it (e.g. through Data Protection subject access requests, Freedom of Information requests and so on).

# GOVERNANCE

The approach will be risk based in relation to governance, focussing on customer safety, business transparency and legislative compliance. There will be an **Accountable Officer** who has overall responsibility with a **Senior Information Risk Owner (SIRO) and a Data Protection Officer (DPO)**. The SIRO will report to the Accountable officer, oversee risk and provide strategic management of Information Governance across the organisation.
The DPO will provide advice to senior management and officers on their data protection obligations; monitor compliance with data protection laws including managing internal activities; advise on training of staff and conducting internal audits; and act as the first point of contact for the supervisory authorities and data subjects.

There will be an **Information Governance Group** that will:

- approve policies and strategies
- manage information management risks
- review incidents
- monitor reporting
- agree work plans on a risk based approach
- communicate Information Management position for the organisation to an Accountable Officer
- agree an Information Management Training and Awareness Programme that will meet the diverse needs of the Council where access, nature, format and sensitivity of data differs according to the roles that staff fulfil.

It will be made up of: the SIRO, the DPO, Strategic Information Asset Co-ordinators who will represent the business and key advisors for IT, Training and risk management/assurance.

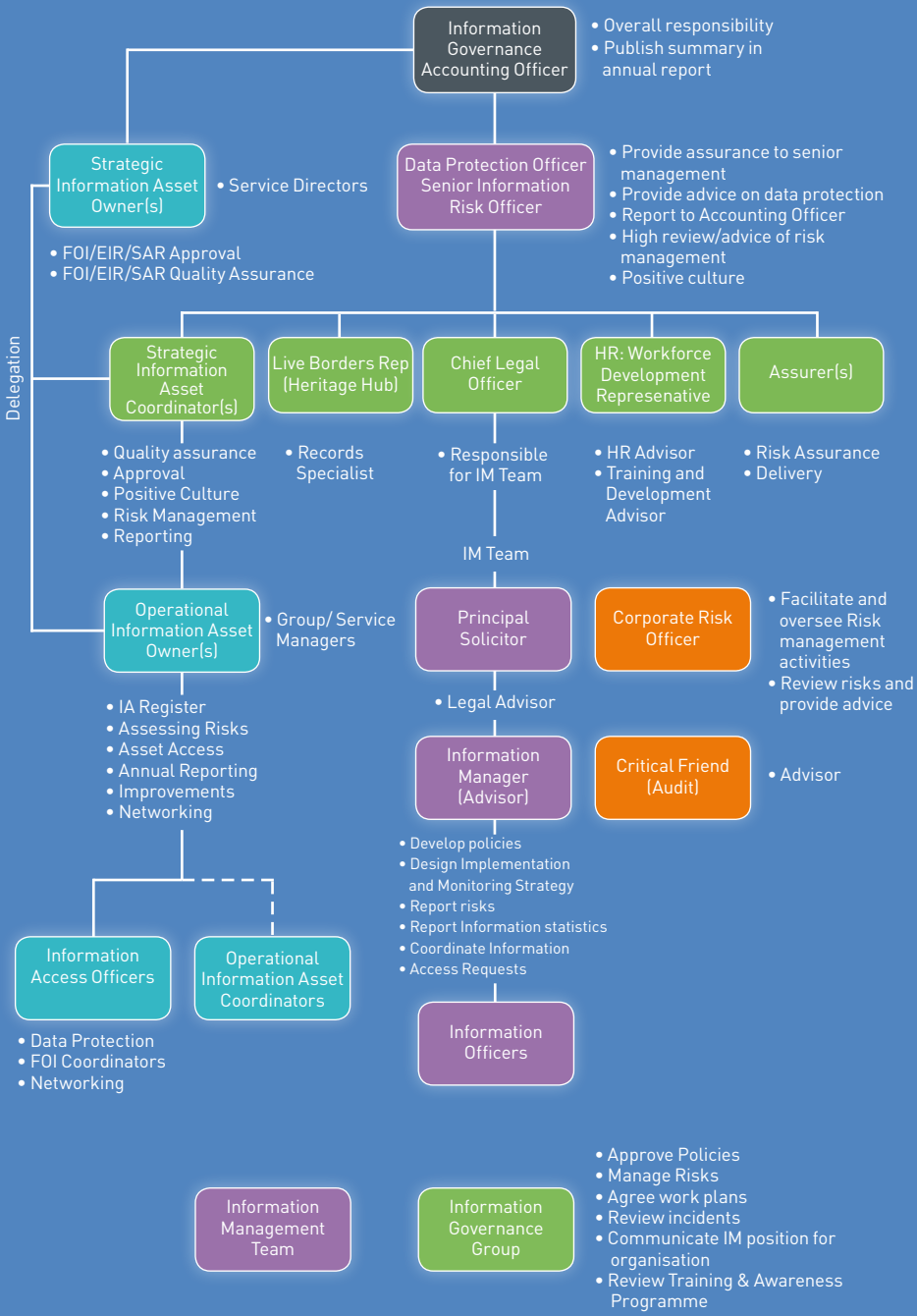
There will be an **Information Management Team** led by the **Chief Legal Officer** that will support the Governance Board by delivering: relevant policies/ procedures and guidance; improvement, monitoring and risk management strategies; statistical reporting to IGG and coordination of information access requests for the organisation. The risk management strategy will be based on the organisation wide Risk Management Policy and Procedures.

Each business area will have strategic and operational **Information Asset Owners**. They will create: a positive culture around information management, manage and report on risks to the IM team within their department and manage/report on the relevant business Information Assets (IAs).

Information Access Requests, including Freedom of Information (FOI), Environmental Information Regulations (EIR) and Subject Access Requests (SAR), will be approved and quality assured by each business area. The level of authorisation required will be determined by the Service Director.

In some cases there will be **Information Access Officers** and **Operational Information Co-ordinators** within the business area that provide a supporting role. The level of support will be determined by the business.

**Managers** and **staff** will also have a role in raising issues around information management for their area and making sure Information Asset Owners know of them. They will attend training and understand and implement Information Management policies, procedures and guidelines relevant to their role. Managers will also raise awareness of relevant information, making sure staff have carried out training and are aware of policies, procedure and guidelines for their business area.


Information Governance Accounting Officer
• Overall responsibility
• Publish summary in annual report
Strategic Information Asset Owner(s)
• Service Directors
• FOI/EIR/SAR Approval
• FOI/EIR/SAR Quality Assurance
Data Protection Officer Senior Information Risk Officer
• Provide assurance to senior management
• Provide advice on data protection
• Report to Accounting Officer
• High review/advice of risk management
• Positive culture
Delegation
Strategic Information Asset Coordinator(s)
• Quality assurance
• Approval
• Positive Culture
• Risk Management
• Reporting
Live Borders Rep (Heritage Hub)
• Records Specialist
Chief Legal Officer
• Responsible for IM Team
HR: Workforce Development Represenative
• HR Advisor
• Training and Development Advisor
Assurer(s)
• Risk Assurance
• Delivery
IM Team
Operational Information Asset Owner(s)
• Group/ Service Managers
• IA Register
• Assessing Risks
• Asset Access
• Annual Reporting
• Improvements
• Networking
Principal Solicitor
• Legal Advisor
Corporate Risk Officer
• Facilitate and oversee Risk management activities
• Review risks and provide advice
Information Manager (Advisor)
• Develop policies
• Design Implementation and Monitoring Strategy
• Report risks
• Report Information statistics
• Coordinate Information
• Access Requests
Critical Friend (Audit)
• Advisor
Information Access Officers
• Data Protection
• FOI Coordinators
• Networking
Operational Information Asset Coordinators
Information Officers
Information Management Team
Information Governance Group
• Approve Policies
• Manage Risks
• Agree work plans
• Review incidents
• Communicate IM position for organisation
• Review Training & Awareness Programme

# LEGAL COMPLIANCE – *legal duty*

The Council, its staff and representatives, have a duty to be compliant with legislation in relation to information management. This legislation includes, but is not exclusively:

- Computer Misuse Act 1990 (CMA 1990)
- Data Protection Act 2018 (DPA 2018)
- The General Data Protection Regulation 2018 (GDPR)
- Environmental Information (Scotland) Regulations 2004 (EIR 2004)
- Freedom of Information (Scotland) Act 2002 (FOISA 2002)
- Freedom of Information (Amendment) (Scotland) Act 2013 (FOIASA 2013)
- Protection of Freedoms Act 2012 (PFA 2012)
- INSPIRE (Scotland) Regulations 2009 (INSPIRE)
- Local Government Act 1986 (LGA 1986)
- Local Government (Scotland) Act 1994 (LGSA 1994)
- Local Government in Scotland Act 2003 (LGSA 2003)
- Public Records (Scotland) Act 2011 (PRA 2011)
- Re-use of Public Sector Information Regulations 2015 (RPSI 2015).

All staff have a responsibility to be compliant with the law to reduce the risk to the Council's reputation and subsequent monetary fines. The Council has established and maintains policies and procedures to ensure compliance with Data Protection, Freedom of Information, Environmental Information and Human Rights legislation in relation to information management.

Ensuring compliance with legislation is a key driver in the design and development of Information Governance training courses within the Council's Learning and Development planning and monitoring.

The Information Governance Group will oversee and report on annual assessments and audits of the Council's compliance with legal requirements relating to Information Management.

# INFORMATION SECURITY – *good data security*

**Securing Assets and Resources**

Information security is the responsibility of everyone. We need to securely manage our digital and physical assets and resources to protect existing data and information. Separate policies and procedures that set out responsibilities, guidelines and best practice should be followed to minimise unauthorised use, modification, destruction, disclosure of information or disruption to Council services.

Where information contains personal data, unlawfully obtaining the information or disclosing it knowingly or recklessly could be a criminal offence by the individual.

IT Security will be regularly reviewed to ensure that the Council has adequate safeguards in place: for use of new information and communication technologies to improve the way it delivers its services, to promote transparency and to safeguard its customers and commercial partners.

**Incident Management**

Good incident management is also important when things don't go as expected. All incidents need to be reported as soon as possible so they can be dealt with swiftly and effectively.

It is the responsibility of every employee to report an incident to their line manager, the Information Management Team and IT using the Council policy and procedures. Responsibility for investigation will depend on the incident. It will be carried out by IT, the Information Team or the Information Asset Owner following the policy and procedures. Any incident will need to go through containment and recovery, assessment of ongoing risk, notification of incident to relevant bodies/people necessary (if a severe security incident or a data breach), evaluation and response

Incidents can be caused by malicious behaviour, human error, equipment failure or unforeseen circumstances (such as fire or flood). They include, but are not restricted to:

- Loss or theft of data/information or equipment on which it is stored.
- Corruption or destruction of information or equipment on which it is stored (if it is the original copy and is out with disposal policy).
- Provision of data to someone who it not entitled to see it.
- Attempts to gain unauthorised access to data (hacking, blagging, breaking in, accessing files without permission).
- Inappropriate access controls allowing unauthorised use.
- Changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent.

Incidents can include 'data breaches'. A data breach is the loss, theft, corruption, inappropriate access or sharing of data. Each incident will be investigated and judged on its individual circumstances and addressed accordingly. A data breach may lead to a disciplinary investigation and subsequent disciplinary action.

If a criminal offence is considered to have been committed the matter will be reported and further action may be taken to assist in the prosecution of the offender(s).

If the breach involves personal information (sensitive or otherwise) then this is a 'data protection breach'.

The Security Incident Reporting and Management Procedure must be followed in these cases. It will be the DPO's responsibility to notify the Information Commissioners Office (ICO) of all Data breaches in terms of the GDPR.

For 'PSN Compliance breaches' notification to the Cabinet Office will be undertaken by IT.

## RECORDS MANAGEMENT – *accurate data*

**Controls and Standards**

Records need to be effectively managed and this is the responsibility of all staff. Putting in place controls allows for trustworthy, accurate and accessible records. This promotes the open and accountable image Scottish Borders Council wants to portray and will have a positive impact on the Council's efficiency, effectiveness and reputation.

Controls should be put in place for creating, classifying, using, storing, preserving or disposing of organisational records according to a defined set of standards. To provide an effective service it is important that not all information is held indefinitely and to adopt a standardised approach to what should be kept and not kept.

These standards will be written and monitored through a Records Management Plan agreed by the Keeper of the Records of Scotland in line with our legal obligations. A range of procedures and guidance are available.

Information Asset Owners will manage assets, making sure they comply with common standards, approve and monitor improvements and report annually to the SIRO on their status.

**Quality Assurance**

Information Quality is important. Quality is generally defined, as 'fit for purpose', relevant and accurate.

All staff need to ensure that data is:

- substantiated at collection (or if not possible then subsequently verified)
- recorded in full
- recorded as accurately as possible
- recorded in a timely manner (where it is not possible to record data in real time this data should be recorded as soon after the event as possible)
- collected and recorded in keeping with national data standards where appropriate.

Information Asset Owners will work with managers to continually review the purpose of holding data and how to improve quality of information within their services.

# ACCESS – *informed openness*

Through our commitment to sharing information, Scottish Borders Council intends not only to fulfil any legal obligations, but also to promote a spirit of openness and accessibility.

**Data Sharing**

'Data sharing' is disclosing data between or within organisations. It can include:

- a reciprocal exchange of data
- one or more organisations providing data to a third party or parties
- several organisations pooling information and making it available to each other
- several organisations pooling information and making it available to a third party or parties
- exceptional one-off disclosures of data in unexpected or emergency situations or
- different parts of the same organisation making data available to each other.

**Data Sharing Protocols**

All data that is shared needs to be obtained legally, verified before use and recorded if you are the owner of the data. When data is updated any linked systems also need to be updated. When it is with another organisation it is important that an agreement or contract is set up with appropriate protocols/ instructions.

For **inter-agency sharing** the Pan Lothian and Borders Partnership General Protocol for Sharing Information must be used. This includes sharing with: Borders NHS Board, Lothian NHS Board, City of Edinburgh Council, East Lothian Council, Midlothian Council, Scottish Borders Council, West Lothian Council and Lothian and Borders Police Force.

Employees engaged in joint working need to ensure that they understand relevant terminology used by the different partners and any Information Governance requirements or conditions that may apply (e.g. Caldicott principles).

(including 3rd parties providing services on behalf of the Council), the Council remains responsible for ensuring that the data is treated in line with legislative requirements.

The Council needs to impose data protection responsibilities through its contract with 3rd parties. Staff are responsible for this. They must follow Council Purchasing Guidelines and bring any purchase transaction of any value where personal data might be involved to the attention of the Procurement Service. This is so that all data processing with a 3rd party that includes personal data has a contract that ensures compliance with the following legal obligations:

- 3rd party only acts on instructions from the Council;
- there is security in place that is equivalent to that imposed on the Council under the Data Protection legislation.
- monitoring to make sure instructions are followed and security is maintained.

When **sharing with colleagues** in another part of the organisation employees must ensure that they do not divulge information to colleagues who do not have the right to access it. Where it includes personal data this right must be in keeping with the data protection principles.

**Data Sharing Monitoring**

Where employees have any concerns that data may be being accessed inappropriately by colleagues they should report it immediately to their line manager and/or Information Asset Owner.

Managers are responsible for notifying Information Asset Owners of data sharing and IAOs should record data sharing for annual reporting to the SIRO. They are both responsible for ensuring that data sharing policies and procedures are correctly implemented in their departments.

**Data Requests**

Individuals have the legal right to request access to information that the Council hold: either about a subject (FOI/EIR), specific types of spatial data (INSPIRE) or themselves (subject access request (SAR)). They can also request to re-use data (RPSI). When responding to these requests legal requirements around supplying the data in a specific format should be complied with.

Scottish Borders Council will fulfil its legal obligations with effective and timely responses that protect individuals' rights while promoting a spirit of openness and accessibility in our responses through a commitment to share information.

When disclosing information it must be in line with the relevant Council Policies and Procedures depending on the type of request. Quality assurance and approval of responses is carried out within each business area. The level of authorisation required will be determined by the Service Director.

**Data Publication**

Through a Publication Scheme the Council will keep customers informed of the data and information we hold, what we do with it, what information they have access to and how they can access it. (For example, information on Data Protection subject access requests, Freedom of Information requests and so on).

The Information Management Team is responsible for coordinating this.

By routinely publishing official information on its website, the Council aims to take a proactive approach to transparency of services and reduce the need for customers to make individual requests underthe Freedom of Information (Scotland) Act, Environmental Information (Scotland) Regulations or other statutory provisions.

When staff are publishing information (this includes all forms of communication including public launches) they need to take into account the Council's legal obligation not to publish any material which in whole or in part appears to be designed to affect public support for a political party.

Line Managers and Directors should work with the Information Asset Owner where possible to have a proactive approach to publication of information within their service area.

## POLICY COMPLIANCE

Non-compliance with this Information Governance policy could have a significant effect on the efficient operation of the council and may result in financial loss, reputational damage and an inability to provide necessary services to our customers.

If any employee is found to have breached this policy, they may be subject to the council's disciplinary procedure.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.

# REVIEW

The Information Governance Group (IGG) will carry out:

- an annual review of Training and Awareness Campaign to make sure it is fit for purpose.
- an annual review of Risk Management Strategy
- a quarterly review of risks and completion of mitigation measures, particularly where it outlines a policy change
- a review of this policy at least once every two years. (If requested by the IGG significant changes to policy will be reviewed by Corporate Management Team (CMT) for approval.)

You can get this document on tape, in large print, and various other formats by contacting us at the address below. In addition, contact the address below for information on language translations, additional copies, or to arrange for an officer to meet with you to explain any areas of the publication that you would like clarified.

CHIEF EXECUTIVES
Scottish Borders Council | Newtown St Boswells | MELROSE | TD6 0SA
tel: 01835 824000

Scottish Borders COUNCIL

think !nformation

Printed in the Scottish Borders. Designed by Scottish Borders Council Graphic Design Section. July 2018.