Code of Practice on Data Protection

Scottish Borders COUNCIL

think !nformation

Contents

1. Introduction

The General Data Protection Regulation (GDPR) provides a legal framework for the appropriate handling and disclosure of personal data. It sets out six general principles which must always be considered whenever we process personal data. It also gives individuals the right to establish whether we hold any information about them, and establishes an Information Commissioner who acts as regulator on Data Protection matters.

To ensure compliance with Data Protection and encourage best practice we have developed the following guidance.

It includes:

- Information about Roles and Responsibilities
- Basic Data protection definitions
- A Statement of the six Data protection principles
- Our Information Governance Training Policy
- A guide to the lawful disclosure of information
- Information about keeping personal data accurate and up-to-date and guidelines for checking addresses and contact details
- Information about computer security
- Guidelines about engaging contractors and some tips for good contract management
- Notifying the Information Management Team
- Data Protection Impact Assessments

This code of practice should be read in conjunction with the Council's other relevant policies and guidance available on the Intranet including:

- Subject Access Request Guidance and procedures;
- Information Governance Policy;
- CCTV Code of Practice;
- Policy on use of e-mail and the internet;
- Computer Security Policy and Standards;
- Password Policy;
- Security Incident Reporting and Management Procedure;
- Privacy Notice Guide and examples;
- GDPR Staff Handbook;
- Data Breach Guide;
- Data Protection Impact Assessments prompt list and template

This code of practice applies to all employees and elected members of Scottish Borders Council, and compliance with it and any associated procedures are a condition of employment. Violations of the code of practice may result in disciplinary action.

2. Data Protection definitions

Personal data
Personal data is any information relating to a living individual who can be identified from that information. Please note that personal data includes expressions of opinion and indications of intention in respect of an individual.

Special Category personal data
Special Category personal data is information specifically relating to the following:

- The racial or ethnic origin of the data subject
- The data subject's political opinions
- The data subject's religious beliefs or other beliefs of a similar nature
- Whether the data subject is the member of any trade union
- The data subject's physical or mental health condition
- The data subject's biometric or genetic data
- The data subject's sexual life or sexual orientation
- The commission or the alleged commission by the data subject of any offence
- Any proceedings relating to the commission or the alleged commission by the data subject of an offence.

Data controller
A data controller is a person or organisation who decides how, and for what purposes, personal data is held and processed. Scottish Borders Council is registered as a data controller.

Joint data controllers
These are people or organisations (for example, Scottish Borders Council, NHS Borders and Police Scotland) who jointly process and share information for the same purpose.

Data processor
This role is carried out by any person other than an employee of the Council who processes personal data on the Council's behalf and in accordance with the Council's instructions. Contractors and agents may qualify as data processors.

Data subject
A data subject is an individual in respect of whom the Council holds or processes personal data.

3. The Data Protection Principles

Personal data must be held and processed in accordance with the following general principles. It is crucial that all employees who process personal data familiarise themselves with these rules.

Personal data must be:

1. Processed fairly and lawfully and in a transparent manner in accordance with at least one condition set out in the GDPR;

2. Collected for specified, explicit and legitimate purposes and not further processed in any way incompatible with those purposes;

3. Adequate, relevant and not excessive in relation to the purpose for which it was collected;

4. Accurate and up to date;

5. Kept for no longer than is necessary;

6. Protected by appropriate technical and organisational measures which guard against unauthorised or unlawful processing of personal data, or accidental damage to, or loss or destruction of, personal data;

ACCOUNTABILITY

The Council must demonstrate that it complies with Data Protection legislation by having appropriate policies and procedures in place and by documenting the personal data it is processing, why it is processing and legal basis for doing so.

4. Training

All staff must complete the Information Management Awareness module and staff who use IT equipment must also complete the Information Security module. Both training modules must be completed on an annual basis.

Some employees will require further training, specifically those staff who;

- Process a significant amount of personal data on a day to day basis or;
- Have specific responsibilities in respect of personal data;
- Have a lead role in Data Protection and Information Governance responsibilities

This training will consist of;

- In-house informal training run by services
- Face to face training with IM team at service led meetings/toolbox talks
- Access to training materials for specific roles

Services are encouraged to consider their Data Protection training needs and monitor their employees' understanding of the implications of the Data Protection legislation.

Line managers may wish to request tailored training for their staff particularly if they are dealing with sensitive personal data. If so, they should in the first instance contact the Information Management team to discuss their requirements.

Councillors
The Information Management team will make Councillors familiar with the basics of Data protection as soon as reasonably possible after they are elected as part of the Elected Members Induction Programme.

Review
The Information Governance Group will monitor the Training and Awareness Programme and review on a quarterly basis.

5. Processing personal data fairly and lawfully

As part of the first Data Protection principle, the Council is required to process personal data fairly, lawfully and in a transparent manner.

Employees must ensure they;

- Hold and process personal data only to support the Council activities which it is legally empowered to carry out and only in compliance with its wider legal duties.
- Inform the person in respect of whom the personal data is collected the purpose for which the data will be held, processed and the period it will be retained for.
- Inform the person of the parties to whom the data may be given and the purpose for doing so.
- Complete a Data Protection Impact Assessment to document that all possible implications were considered to ensure that only what is necessary is processed.
- Consult with the Information Management Team when designing a new form asking for personal data (who must approve the design before it can be finalised).
- Document the legal basis for the processing in the central register of Data Processing

REMEMBER

The Council cannot rely on consent as a legal basis for any processing activity that falls under its statutory or core functions

For more information on informing data subjects please refer to the staff handbook on privacy notices

6. Ensuring that personal data is accurate

Services must develop appropriate procedures for checking that the personal data they hold is accurate. These procedures should cover both the initial collection of personal data, and subsequent checks and updates of personal data.

Employees **must ensure** that when they collect and input personal data;

- It's recorded accurately
- It's updated promptly
- To remove old and redundant data from systems
- To regularly sweep systems to identify inaccuracies and delete as required

It is **extremely important** that employees check that;

- Contact details are entered accurately
- The correct individual's contact details has been selected
- Another organisation's record of an individual's information has been verified independently before using as far as is practicably possible

In instances where information is held on a system for more than one person with the same name, employees should check other details such as date of birth to identify the correct person. If there is any doubt as to the accuracy of an address, employees should refrain from sending correspondence until the address has been verified.

Employees should also consider whether it is appropriate to send out certain documents by post, and whether they should make use of recorded delivery or other secure delivery services.

REMEMBER

Failure to accurately record personal data may result in a significant data breach. Addressing an envelope incorrectly or copying an incorrect address onto a letter can have serious consequences.

Employees must report **immediately** to their line manager or the Information Management Team if they suspect a data breach may have occurred.

For further information, please see the staff guide on Data Breaches

7. Protecting personal data

To protect personal data, employees must always ensure that when:

In the office:

- unauthorised persons do not enter Council offices;
- Their computer screen cannot be seen by unauthorised people (for example, visitors to the office);
- Their computer screen is locked when leaving their desk;
- Files containing personal data, and in particular files containing sensitive personal data, are saved in appropriately secure drives and folders;
- Access to personal data is restricted to only those who need to see the information;
- Sensitive and confidential paper files are stored securely and are not at risk of being accessed by unauthorised persons;
- Check carefully before handing over any information or computer equipment to unfamiliar individuals;
- Any personal data taken off Council premises is kept securely and no unauthorised person has access to it.

Working away from the office:

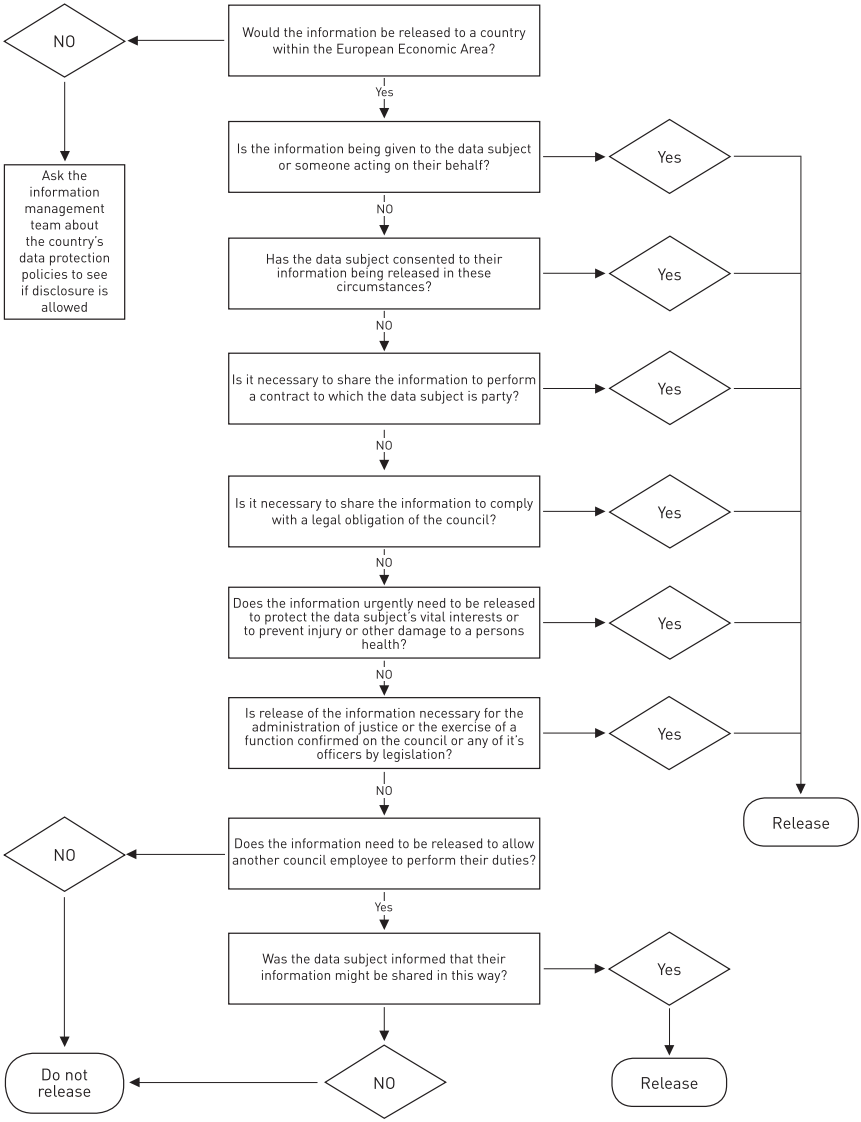
- Must have their line manager's approval before taking equipment and information off Council premises;
- Be aware of what their responsibilities are and be able to meet them;
- Equipment/files are kept secure and are never left unattended on any form of transport;
- Visitors and other members of the household should not be able to access the data;
- Personal data is kept securely locked away when employees are not home;
- Information must not be visible or capable of being photographed when in a public space (for example libraries or public transport);
- Should not use SBC equipment in any place where unauthorised persons or members of the public may be able to view personal data and/or confidential information.

Disposing of:

- Computers ensure that any personal data is deleted from the hard drive;
- Paper files containing personal data is done securely by placing it in the confidential waste bins (HQ only); or placed in the appropriate confidential-waste bags; or shredded.

8. Releasing information

As a general rule, personal data can only be released in accordance with all the Data Protection principles. However there are certain circumstances in which the release of personal data is exempt from some or all of the Data Protection principles. The flow chart below may help you decide whether you should release information.



Personal data may be given to other council employees so they can perform their duties provided that they do not intend to use the information for a new or different purpose.

Personal data may be released if it is urgently needed to protect a person's vital interests, or prevent injury or other damage to a person's health.

Personal data may be released for the purposes of:

- Preventing or detecting crime;
- Arresting or prosecuting offenders;
- Assessing or collecting any tax or duty.

If there is a good chance that by not providing the information it would prevent one or more of these purposes, it can be released under an exemption. Employees should ensure that they have received a formal request before releasing any information. If the organisation is unable to produce the standard form, employees should seek further advice from the Information Management team.

Information provided should only be about a specific named person.

For information please refer to the Subject Access Request Guidelines and for requests relating to Social Work or Education please refer to the Subject Access Request Guidelines for Social Work and Education.

Subject Access Requests

Under Data Protection, any person whose personal data we hold on computer or in structured paper files has the right to request the information we hold about them.

All requests for access to personal data must be sent immediately to the Information Management team.

It is essential that the Council fully complies with this right and enables a person to access their personal data in as straightforward and simple a way as possible.

However, a distinction must be drawn between releasing personal data in the course of carrying out routine business and responding to requests for access to personal information under Data Protection.

Example

Information about Council Tax arrears may be given to the person who owes the Council Tax once their identity has been checked, but only under Data Protection can they insist on access to all personal data held about them.

On receipt of a request, the Council must provide the applicant with the information within 30 calendar days. Employees must be aware of and adhere to the subject access request procedure and respond to the Information Management team by the deadline which the team has identified.

Personal data may always be given:

- To the person the information is about or someone entitled to ask on their behalf;
- If the person the information is about, or someone asking on their behalf, asks for the information to be given or agrees to it being given e.g. a signed mandate by the data subject;

As long as the person providing the information has evidence to confirm that it meets one of the conditions above.

Other Rights

Individuals also have the right to:

- Be informed how their personal data will be used;
- Have inaccurate data amended;
- Object to certain types of processing;
- Restrict processing;
- Have data deleted;
- Have data transferred to other organisations.

Although some of these rights described above can only be applied in certain circumstances, the Council is still required to respond to the individual within 30 calendar days.

Employees must pass any request to the Information Management team as quickly as possible. The request will be recorded and the team will liaise with the relevant staff to ensure that the request is fully considered and appropriately responded to within the statutory time frame.

9. Risk to the council

The main risks to the Council are reputational damage leading to a loss of public trust; compensation claims from individuals and being fined for breaching one of the Data Protection principles.

This may occur through any of the following:

- Not issuing a privacy notice to individuals when asking for their personal data.
- Failing to record or update information accurately.
- Recording more information than what is required.
- Keeping information for longer than needed.
- Failing to respond to a subject access request in time.
- Revealing information about a third party in circumstances where it is not appropriate or lawful to do so.
- Failing to dispose of personal information securely by putting it into normal waste rather than a confidential waste bin/bag or shredding it.
- Failing to place personal information in an envelope when distributing through internal mail.
- Recording personal information in a database, spreadsheet or word processing file and not notifying the Information Management Team for recording in the central register.
- Failing to document the legal basis for processing personal data
- Relying on consent for processing personal data to meet statutory requirements and functions
- Failing to carry out a Data Protection Privacy Impact Assessment for any new processing activity
- Procuring and using a system/online service hosted in a country outside the European Economic Area, which does not have acceptable data protection laws (see appendix B).
- Failing to report a significant loss of personal information within 72 hours to the Information Commissioner.

10. Computer security

Employees must:

- Supervise employees from external organisations visiting Council premises.
- If an employee of an external organisation requires a password to access equipment, software or information, this must be arranged beforehand and deleted once the task is complete.
- Never give other people their password.
- Not allow other people to take away computers, pen drives, tapes printouts or any removable media unless this has previously been agreed with IT Services.
- Deliver printouts, tapes, pen drives, cds and other documents containing personal information that need to go from one department or office to another should be delivered to a specific person or secure area, and not left lying about for collection.

Personal information should not be provided to suppliers/providers without written assurance of the following:

- There is a contract or data sharing agreement in place.
- Information will be used only for conducting one or more specific purpose .
- Information will not be given to any person not involved in the relevant test and will not be produced in any publication or manual.
- Information that identifies people (for example, giving names or addresses) will be anonymised before the information is used for the test, unless to do so would make the test useless.
- After carrying out the relevant test or tests, any printouts containing personal information must be destroyed and any cds or pen drives returned securely.
- A data protection privacy impact assessment has been completed.

In all statements of requirements for computer systems that process personal information, the following two requirements must be included:

- Forms or screens used for recording information must not allow more information than what is necessary to be entered.
- It must be able to produce a report showing all the information held on a specific person, together with the full text for any codes used, so any request for access to personal information could be met.

For a comprehensive description of our approach to computer security, see the Council's Information Security Policy, Information Security Acceptable Use Guide, Email, the Internet and Telephony Acceptable Use Policy, and Security incident Reporting and Management procedure.

11. E-mail

Employees must always be careful when using email and sending information by e-mail:

- Always check the email is being sent to the correct person both internally and externally;
- Don't send personal data within an email but attach the information as a document and password protect using win-zip/7-zip
- Avoid using email to send sensitive information unless you are using the Public Service Network (PSN) or encryption;
- Follow the Council's Information Security Policy and E-mail, Internet and Telephony Acceptable Use Policy;
- Be wary of using distribution lists as these may not be up to date;
- When sending information to multiple external recipients always use the blind copy (bcc) function.

For further guidance on what should be considered before sending personal data, employees should refer to the Check before You Send guide and the Information Security Acceptable Use Guide.

12. Contracting with external parties

All employees must be aware that in order to comply with Data Protection, the Council is obliged to regulate and monitor its arrangements with contractors.

The following procedure applies in all cases where the Council is considering contracting with an external party, and that external party will (either as part of the contract or in order to perform the contract) process any personal data on behalf of the Council:

- Notify the Procurement Team of any type of purchase involving personal data regardless of the value;
- Consult with the Legal Team before signing a contract involving personal data to ensure that before proceeding there is an agreement clearly stating:
    - The relationship and the obligations under Data Protection placed on each;
    - That appropriate organisational and technical measures will be put in place to ensure the security and protection of personal data.
    - The contractual provisions allowing the Council to check the contractor's compliance with Data Protection
- Contract Owners must monitor performance of the contract and ensure that the contractor implements and adheres to Data Protection

For further guidance on what should be considered before sending personal data, employees should refer to the Check before You Send guide and the Information Security Acceptable Use Guide.

Any employee aware of any arrangement with a contractor that is not appropriately regulated, and does not include any written provision to ensure that the contractor is taking appropriate organisational and technical measures in respect of personal data, must inform the Procurement and Legal team **immediately**.

For more information, please refer to the Procurement & Contracting Standing Orders policy and Purchasing Guidelines

13. Notifying the Information Management Team

The Council is required to document its data processing activities and evidence it complies with Data Protection legislation.

Information Asset Register

To meet this requirement the Information Management Team has created an Information Asset Register and will maintain a register of Data Processing, which will provide a record of:

- The personal data the Council holds and processes;
- The purposes for which the personal data is held and processed;
- The legal basis for the processing;
- How the information is being stored and looked after;
- How the Council is informing data subjects;
- The source of the personal data;
- Details of the people or organisations with whom the personal data is shared;
- The legal basis for the sharing;
- Any overseas countries that personal data may be transferred to.

REMEMBER

The Information Asset Register and Register of Data Processing are vital records that demonstrate and evidence how the Council looks after information and must be kept up to date. The Information Management Team **must be** notified of any changes.

Data Protection Impact Assessments

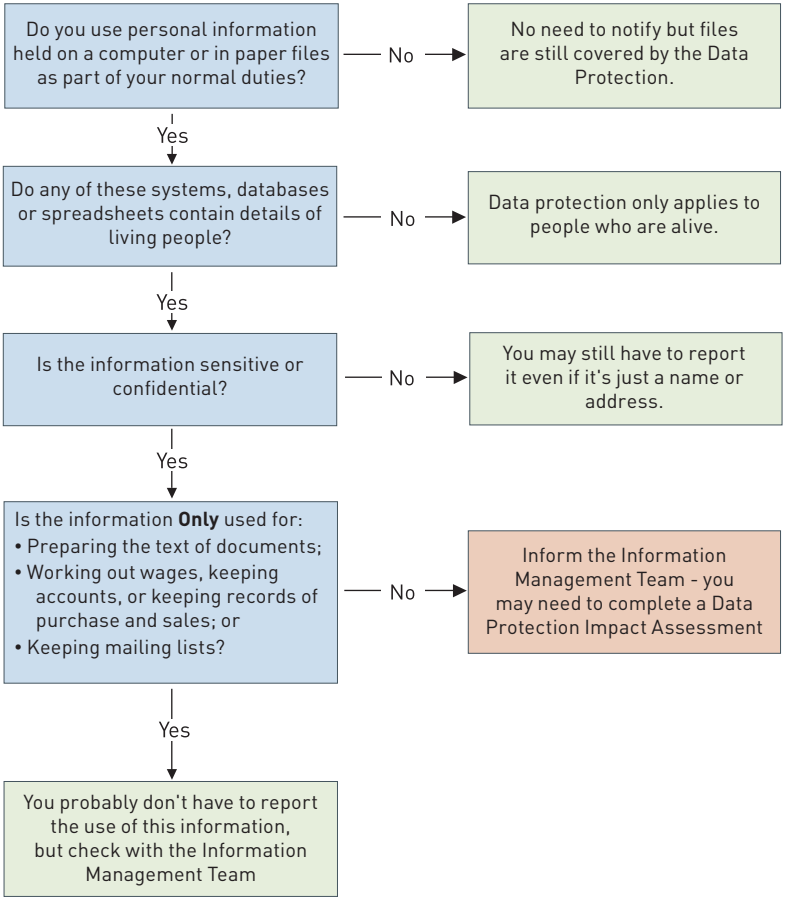
The Council is also required to notify and consult with the Information Commissioner before undertaking any processing that is considered to be high risk to the rights and freedoms of the data subjects. Therefore the Information Management Team must be notified as early as possible of any new decision to process personal data. This includes any consideration to:

- Process new sets of personal data;
- Create new databases;
- Introduce new systems;
- Change current processing activities.

A Data Protection Impact Assessment must be completed before any new processing takes place and a copy of the completed assessment should be provided to the Information Management Team for updating the Registers.

For more information on Data Protection Impact Assessments, please refer to Privacy by Design prompt list and guideline.

Quick Guide for notifying the Information Management Team



Personal Data Breaches

It is important for employees to be able to recognise and report personal data breaches. The Council is required to report certain breaches to the ICO **within 72 hours** dependent on the seriousness and the risk to the individuals affected.

A personal data breach is a breach of security that leads to an incident of personal data being lost or disclosed, accessed, altered or destroyed without authorisation. The Council must investigate every breach and document the actions taken to contain, eradicate and prevent the same breach happening again.

Therefore employees must report any suspected breach to their line manager immediately or the Information Management Team even if there is some uncertainty if it is an actual breach.

A personal data breach could be;

- Sending personal data to the wrong email address or postal address
- Sending personal data to an unsecured email address without password protection
- Releasing personal data to an organisation without the proper safeguards and documentation in place
- Disposing of personal data in a general waste bin
- Collecting personal data from an individual without informing them of their rights
- Not responding to correspondence from an individual looking to exercise one of the rights afforded to them under the legislation
- A colleague accessing personal data that they are not authorised to use

This is not an exhaustive list; please refer to the staff guide on data breaches for further information.

For more information on reporting breaches, please refer to:

- Security Incident Assessment Form
- Security Incident Reporting and Management procedure

REMEMBER

The Information Management Team must be notified of any potential breach immediately

Appendix A – Roles and Responsibilities

Although all employees share responsibility for complying with Data protection, there are certain responsibilities assigned to officers in specialised roles. The roles are as follows:

Senior Information Risk Owner (SIRO)

The SIRO maintains overall responsibility for information governance within the Council.

Data Protection Officer (DPO)

The DPO is the Council's critical friend for Data Protection and is there to guide the Council to ensure that it complies with Data Protection legislation.

Strategic Information Asset Owners (SIAO)

The overall responsibility and accountability for management of information resides with the Service Directors who are the SIAOs. Day to day responsibilities are delegated from the SIAOs to the OIAOs (Service Managers).

Strategic Information Asset Coordinators (SIAC)

Each department has a SIAC who sits on the Information Governance Board as a representative of the Service Directors. The SIACs work closely with the Information Management team to ensure that their area of business meets the requirements of Data Protection and other Information Management legislation.

Each department has a Strategic Information Asset Coordinator.

Strategic Information Asset Coordinators are responsible for assisting their department or business area to meet the requirements of Data Protection. Their duties including the following:

- Working with appropriate officers to ensure that any personal data held or processed on computer in their department is processed in line with Data Protection.
- Making sure staff understand and accept their data protection responsibilities.
- Giving the Information Management team information on all proposed new systems which involve processing personal data. This must be done before the system is procured or introduced.
- Arranging for staff in their business area to receive training in relation to data protection.
- Keeping in touch with the Information Management team and IT.

Operational Information Asset Owners (OIAO)

Service Managers are the OIAOs with responsibility for operational management of information. Their task is to ensure that policies and procedures are followed; recognise actual or potential security incidents; consult their SIAC on incident management; and ensure that information asset registers are accurate and kept up to date.

The Information Management team

The Information Management team provides advice and assistance on a range of Information governance matters, and drives compliance with the Data Protection and associated laws. An employee who has concerns about a Data Protection issue should contact the Information Management team as soon as possible.

The Information Management team is responsible for issuing guidance and procedures on meeting Data Protection requirements and associated laws. Their responsibilities include the following:

- Recording all personal data held or processed on computer for which the Council is the recognised data controller, or is acting as a data processor.
- Working with Strategic Information Asset Coordinators, Operational Information Asset Owners and employees across the Council to make sure that all personal information held on computer and in paper files is processed in line with Data Protection.
- Providing Strategic Information Asset Coordinators, Operational Information Asset Owners and other employees with advice on their responsibilities for protecting and lawfully processing personal data.
- Regularly reviewing the procedures for dealing with subject access requests and other data protection matters, and making sure these procedures are followed.
- Regularly reviewing this code of practice and checking that it is being followed.
- Coordinating subject access requests.
- Dealing with any day-to-day enquiries about data protection.

Information Access Officers

Information Access Officers ensure that subject access requests are dealt with appropriately and promptly by the services and departments they represent. Information Access Officers must ensure that subject access requests are sent to all those within their service who may hold relevant information.

Each department must identify an Information Access Officer who will organise their department's response to any subject access request circulated by the Information Management team. Each department is expected to give appropriate consideration to allocating resources for responding to subject access requests.

Individual members of staff

Individual members of staff are responsible for protecting personal data held or processed on a computer, or held in paper records, within their care. They do this in the following ways:

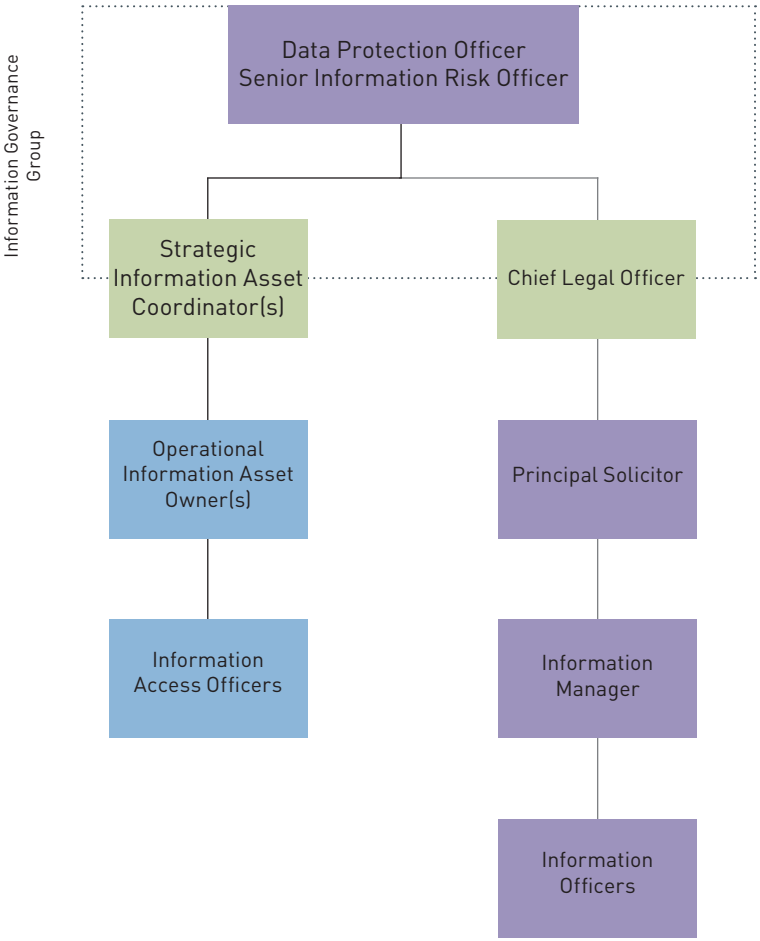
- Making sure personal data is processed only in line with the details reported to the Information Management team and telling their Strategic Information Asset Coordinators about any exceptions.
- Reporting all proposed new systems or changes to existing systems to the Information Management team before the new system or change is introduced.
- Following agreed procedures for holding or processing personal data.
- Only giving personal information to people or organisations when to do so is compliant with Data Protection.
- Taking reasonable steps to check the identity of an enquirer, especially those calling in person or phoning.
- Making sure personal information is secure and adequately protected at all times.

Councillors

Councillors are responsible for protecting personal data held or processed on a computer, or held in paper records, within their care. They do this in the following ways:

- Making sure personal data is processed only in line with the agreed purpose or to which the data subject has consented.
- Following agreed procedures for holding or processing personal data.
- Only giving personal information to people or organisations when to do so is compliant with Data Protection.
- Taking reasonable steps to check the identity of an enquirer, especially those calling in person or phoning.
- Making sure personal information is secure and adequately protected at all times.

Information Management Structure



Appendix B – Data protection authorities in the European Union and European Economic Area and Third Countries

The following countries have the same data protection principles as the UK and so it is appropriate to transfer information to them in keeping with the sixth data protection principle.

European Economic Area:

Austria	Greece	Norway
Belgium	Hungary	Netherlands
Bulgaria	Iceland	Poland
Croatia	Ireland	Portugal
Cyprus	Isle of Man	Romania
Czech Republic	Italy	Slovakia
Denmark	Latvia	Slovenia
Estonia	Liechtenstein	Spain
Finland	Lithuania	Sweden
France	Luxembourg	United Kingdom
Germany	Malta	

Third Countries:

Andorra	Isle of Man	Switzerland
Argentina	Israel	Uruguay
Faroe Islands	Jersey	Guernsey
New Zealand		

REMEMBER

The Information Management Team must be consulted before any agreement to transfer data out with the EEA.

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. GS 20.06.18