Scottish Borders Council & Scottish Borders Licensing Board Statutory Records Management Plan

2017

Author: Teresa Maley, Information Manager
Service: Legal & Licensing/Information Management Team

CONTENTS

Introduction

Scheduled Scottish Public Authorities are required to submit for the approval of the Keeper of Records of Scotland a Records Management Plan to comply with the Public Records (Scotland) Act 2011.

The following is the joint plan that is submitted on behalf of

- Scottish Borders Council
- Scottish Borders Licensing Board

28 April 2017

Version Control and Review

Date/ author	Version number/Status	Notes	Review date (*final version only*)
Jan 2017 : Information Manager	0.1 DRAFT	Draft created for IGG update and discussion with NRS – PRSA team	
April 2017: Information Manager	0.5 DRAFT	First full draft for SIRO and IGG	
April 2017: Information Manager	0.6 DRAFT	Final draft for CMT	
April 2017: Information Manager	0.7 DRAFT	Additional evidence added	
April 2017: Information Manager	0.8 DRAFT	IGG amendments added	
April 2017 Information Manager	1.0	FINAL: Approved by IGG	April 2018
September 2017 Information Manager	1.1	FINAL: includes suggested amendments by the Keeper	

For more information contact the Information Manager

Mail: Information Management Team, Legal and Regulatory Services, Council Headquarters, Newtown St. Boswells, Melrose, TD6 0SA

E-mail: infoteam@scotborders.gov.uk

Phone: 0300 100 1800

Element 1

Senior Management Responsibility

This element is about the individual responsible for the overall management of the Scottish Borders Council's (the Council) Public Records. The Council's information governance structure is also described. It is compulsory to include this information in the Records Management Plan.

Statement of Compliance

The individual responsible for the overall management of Scottish Borders Council's public records is Brian Frater, Service Director Regulatory Services and Senior Information Risk Owner (SIRO).

The individual responsible for the overall management of Scottish Borders Licensing Board records is Nuala McKinlay, Chief Legal Officer and Clerk to the Scottish Borders Licensing Board.

The Council has an Information Governance Group (IGG) that is chaired by the SIRO. The Chief Legal Officer is a member of the group together with representatives from the business (including Council owned companies) and information, risk and HR specialists. The IGG reports to Corporate Management Team (CMT) and the Chief Executive through reports from the SIRO so that information issues and risks for the organisation are raised at the highest level of authority in the Council.

The IGG meets quarterly. From 2017, meetings will be themed to ensure all aspects of information governance are reviewed across the year. The themes are:

- Records Management - January-March
- Access to Information - April - June
- Information Security – July - September
- Information Governance – September to December

Since 2012 the Council has been working to complete an information management improvement plan that was agreed with the Information Commissioners Office (within the wider framework of part of corporate transformation). This has been delivered in two phases and is scheduled to be completed by the end of 2017.

Evidence of compliance

Evidence of	Evidence
Delegated responsibility to SIRO	Letter of endorsement from Tracey Logan, Chief Executive, Scottish Borders Council
Licensing Board follows SBC standards	Letter of endorsement from Clerk to the Scottish Borders Licensing Board
Chief Legal Officer role as Clerk to Licensing Board	Chief Legal Officer Job Profile
Purpose of IGG	Information Governance Group (IGG) – terms of reference
IGG calendar	IGG Minute 21 July 2016
How records management fits into the Information Governance structure	Information Governance Pack Information Governance Policy
Corporate endorsement of an Information Management Programme	CMT Meeting xx/xx/2012: item 7a Information Management Programme IG Improvement Plan, 7 Aug 2013 Internal Audit report, 31 Oct 2013
Information Management Project, 2016	IMP Blueprint and Business Case IM Project Board Minute, 21 March 2016

Future Developments

There are no plans to alter the governance structure at present

Assessment and Review

This element will be reviewed as soon as there is a change in personnel and The Keeper of the Records of Scotland will be notified of the change

Responsible Officer

Tracey Logan, Chief Executive of Scottish Borders Council

Element 2

Records Manager Responsibility

This element is about the individual who has day-to-day operational responsibility for records management within the Council. It is compulsory to include this information in the Records Management Plan.

Statement of Compliance

At Scottish Borders Council day to day responsibility for the records management function resides with the Information Manager, Teresa Maley. The Information Manager manages two Information Officers who make up the Council Information Team. This team is part of Legal and Regulatory Services led by the Chief Legal Officer. The functions delivered by the service are:

1. Information Governance and Policy
2. Records Management
3. Information requests and Subject Access Requests
4. Data Protection
5. Information Security (jointly with the Information Technology service)

The Information Manager is responsible for the Records Management Plan. This includes

- Preparing and submitting it to the IGG for corporate approval
- Submitting it to the Keeper of records for approval
- Implementing any improvements contingent on approval

Records Management standards, like other Information Governance standards with which the Council must comply, are cascaded through the business by a network of Strategic Information Asset Owners (SIAOs) and Information Asset Owners (IAOs). Common training, Information Asset Registers and programmes of work are delivered through or maintained by this network and the Information Team. Information Risks are assessed at corporate and business level and reported to the IGG to consider. This is a relatively new structure that is gradually becoming embedded in business processes and is monitored by IGG and Internal Audit.

Evidence of Compliance

Evidence of	Evidence
Records Management function included in a job description	Information Manager – Job Profile Information Officers – Job Profile
Agreement and monitoring at corporate level of creation of Records Management Plan	Information Management Business Case and delivery plan Internal Audit – Improvement Plan report 2017

Future Developments

There are no planned future developments.

Assessment and Review

This element will be reviewed as soon as there is a change in personnel and The Keeper of the Records of Scotland will be notified of the change

Responsible Officer

Nuala McKinlay, Chief Legal Officer

Element 3

Records Management Policy Statement

This element is about the Council's Records Management Policy. It is compulsory to include this information in the Records Management Plan.

Statement of Compliance

Scottish Borders Council has a Records Management Policy with supplementary guidance on Appraisal and Retention of records. This is reviewed and approved by IGG. It applies to all recorded information – in any format – about or to support the Council's business activities.

Records Management guidance for all staff is published on the intranet, there are e-learning tools (including a mandatory Information Management Awareness module with a section on Records Management) and the Information Team delivers training according to the framework described in the Information Governance Policy.

Evidence of compliance

Evidence of	Evidence
Policy	Records Management Policy, January 2017
Approval of Policy	Minute of IGG approving Policy
Staff guidance on Policy	Intranet Information Management page : records management guidance (screenshot) Records Management Toolkit (under review)
Training plan that includes records management	See Information Governance Pack – training plan
E learning on Records Management	SBLearn Information Management e-learning slides - records management (screenshots)
Public awareness	Council webpages on records management (screenshot)

Future developments

There are no planned future developments.

Assessment and Review

The Policy is reviewed and re-approved annually by the IGG in the first quarter of the IGG calendar.

Responsible Officer

Teresa Maley, Information Manager

Element 4

Business Classification Scheme

This element is about the Council business classification scheme describing business activities undertaken by the Council. The Information Asset Register is also described here.

Compliance Statement

Scottish Borders Council has not yet adopted a global business classification scheme for records because of the diversity of systems deployed in services. Most service systems have a local business classification or file plan. The Council has no plans to implement a single corporate EDRMS but will be moving shared drives to Office 365 from 2017. The move to Office 365 presents an opportunity to assist services in using business classification to structure their information and promote use of the retention schedules more consistently than it has in the past. There is also a programme of rationalisation and streamlining of office systems where feasible.

Business Classification has been used to structure both the Council website and intranet to facilitate publication and searching for Council information.

In an attempt to standardise information management the improvement programme included, in stage 3 of the Information Management Project, an information asset survey (2016) and the creation of a corporate Information Asset Register (completed March 2017). This register used the Scottish Council on Archives Records Retention Schedule (SCARRS) business classification as the basis for the structure of the register so that the Council retention schedules could be linked more effectively to information the Council holds from 2017 onwards.

This was not the only reason for creating an Information Asset Register.

The Information Asset Register allows the business to treat information management as a normal part of its work using familiar tools and techniques, such as risk analysis and mitigation. The register is prepopulated into key areas of risk and each asset has an owner who must complete and review the details about the asset/s they have been allocated. It is easy to see if there are gaps in the knowledge about sensitive or high risk assets. This should alert the business very directly that swift action must be taken to remedy the situation. Information Asset Owners (IAO) must keep their section of the register up to date. Oversight of each directorate register is the responsibility of the Strategic Information Asset Owner (SIAO) for that directorate. This is to ensure knowledge about sensitive information is restricted to a small number of people. The global version of the register is only held by the Information Team with controlled access available to designated officers such as the SIRO and Chief Legal Officer.

To ensure the IAR is current, the Information Team will re-survey or update the register annually or when informed of changes by the SIAOs. To ensure that risks are routinely monitored the Information Team, on behalf of the IGG, will remind the SIAO's to assess risks quarterly. Whether they have or not will be reported at the quarterly meeting. In this

way, IGG can monitor reported use of the register against incidents of data breach or poor record keeping and take informed management decisions about deploying resources better to improve data compliance, security and quality.

The Information Team will also publish a short version of the register on the Council website so that the public can see what kind of information the Council holds and whether it is likely to be accessible.

As the IAR is a new initiative its effectiveness will be monitored by IGG and Internal Audit until embedded as a management tool. The Information Team will provide initial training in the maintenance and use of the register. Longer term the focus of training and guidance should emerge from management information derived from the business analysing their risks.

Evidence of compliance

Evidence of	Evidence
A local business classification scheme	
Information Asset Register in the IM Project	IM Project Business case
How the IAR is structured	IAR – Questionnaire Guide IAR – FAQ's Information Asset Register – template copy Information Governance Pack (in E1)
Office 365 and retention schedule review linked	Email and follow up meeting regarding retention schedule review (see Element 5)
Website	https://www.scotborders.gov.uk/site_map

Future Developments

The annual re-survey of the IAR in Jan 2018 will include checks to ensure business classification and retention schedules are identified.

Assessment and Review

Progress will be monitored by reports to IGG

Responsible Officer

Teresa Maley, Information Manager

Element 5

Retention Schedule

This element is about the Council's records retention schedule and how it is deployed.

Compliance Statement

The Council has a corporate records retention schedule and guidance on disposing of records based on SCARRS. The retention schedule is currently under review after several years of business re-structure and the recognition that routine disposal would be more effective if linked to existing business risk management processes and systems. It is planned to carry out a full review in 2017 but in the meantime the approved schedules apply.

The schedules are published on the intranet and on the Council website

The schedules apply to records in all formats.

The retention guidance includes a form for transfer of records to the Council Archives Service (managed by Live Borders Trust) where permanent preservation is the recommended fate.

There is guidance on using the confidential waste service to ensure paper records are safely destroyed and on planning office moves where the need for retrospective and large scale disposal may be identified.

Some Council records are held in Iron Mountain. In "IM Connect" nominated officers and administrators have permissions based access to the inventory of transferred records. The majority have a disposal or disposal review date attached at file, box or series level to promote timely disposal. There is a confidential destructions option included in the Iron Mountain contract.

Information Asset Owners can record the disposal date that applies to an asset in the recently created Information Asset Register. Regularly reviewing the register for risks will help to ensure records are held no longer than they should be.

The disposal of electronic records in shared drives or business systems is controlled by the end user (the Service) following the Council policy and guidance on records disposal. Where removal of data requires technical assistance from IT (IT Services are provided under contract with CGI) – because of access restrictions, for example, or scale of data disposal – an auditable process is followed that requires authorisation by an approved signatory. This is described in more detail in Element 6 Destruction Arrangements.

Emails are disposed on a three year rolling cycle. The Archive Vault and Journal has the same retention period but is purged on an annual basis.

Evidence of compliance

Evidence of	Evidence
Retention schedules in place	SBC Retention Schedules
Management approval of disposal process	Approved Disposal Statement, January 2017 Approved Appraisal Statement, January 2017
Inventory with retention schedule attached	Iron Mountain Inventory with disposal date
Evidence of planned review linked to Office 365 Project	Letter and meeting request re retention schedule review

Future Developments

A full review of retention schedules and disposal guidance will take place in 2017. A project to replace shared drives with Office 365 in 2017 will include a widespread exercise to minimise duplication of documents and apply retention schedules rigorously. To this end the Council retention schedules will be reviewed alongside the project to clearly identify records that can be destroyed and to promote the routine use of the schedules in future.

Assessment and Review

The IGG monitors Disposal Policy and use of retention scheduling through reporting on the Information Asset Register

Responsible Officer

Teresa Maley, Information Manager

Element 6

Destruction Arrangements

This element is about how the Council makes sure it destroys records compliantly. It is compulsory to include this information in the Records Management Plan.

Statement of compliance

At the end of their business use records will usually be destroyed but a small proportion are selected for preservation as Council Archives.

Records are scheduled for destruction following the Council Records Management Policy and guidance on disposal. The Council retention schedule governs the time for which they are retained. There is also a policy on Confidential Waste to ensure that Council information does not end up in the wrong hands. The Information Asset Register now provides a place for the business to record and monitor when it should destroy records and whether confidential destruction is required or not.

The Council has a contract with Shred-it for the confidential destruction of paper records. Shred-it hoppers are provided at HQ where all paper records for destruction must be put. There are different arrangements for locality offices and for bulky destructions. Records stored in Iron Mountain may be destroyed using their destruction service under the terms of the framework or, where necessary, removed to check files do not require further retention in Iron Mountain. If they do not, the standard service with Shred-it is used. Destructions are certificated.

The disposal of electronic records in shared drives or business systems is controlled by the end user (the Service) following the Council policy and guidance on records disposal. Where removal of data requires technical assistance from IT (IT Services are provided under contract with CGI) – because of access restrictions, for example, or scale of data disposal – a managed, auditable process is followed that requires authorisation by an approved signatory. The Council IT Service was contracted to CGI in 2016 including management of deletion, back-up and restoration of Council data. The Council has a residual, in-house IT Projects Team that manages the contract and provides the business interface with CGI. Self-service business requests are logged with the CGI Service Desk who track and record all actions to resolve the request. CGI are required, under the terms of their contract, to maintain records of actions they carry out.

Currently, the process for prompting the reduction of data is reactive:

- CGI informs the Council IT team that a network drive is nearing capacity
- The service is informed and requested to delete data following disposal guidance and schedules - if this frees up sufficient space there is no further action
- If the drive is still reaching capacity after deletions have been made more server space is provided

It is acknowledged that shared drives contain much information that is duplicated, no longer actively managed or "orphaned" because of service changes. Services often struggle to authorise destruction of this information as there is lack of clarity over its status and ownership. The replacement of shared drives with Office 365 is seen as an opportunity to remove or relocate such information and ensure there is a process in place to prevent it happening in future. The Information Asset Register will also, over time, help to map the transit and use of information across the Council (including identification of primary versions) and provide clarity about the status of the information held.

CGI is responsible for managing the destruction of digital assets. The supplier list for destruction services is currently under review by CGI (April 2017). The process and supplier list will be available when the review is complete. This will include disposal of

- data on hard drives
- de-commissioning media from live use
- destruction of back up media

Obsolete IT equipment and hardware, after de-commissioning, is currently disposed of through an approved charity.

Evidence of compliance

Evidence of	Evidence
Standard process for destruction	Disposal Statement (see E5) Confidential Waste Policy Information Security Policy, June 2016 Guidance on Moving Office
Staff awareness	Mandatory training (e-learning)– Information Awareness title and menu pages
Certificate of disposal - paper	Shred-it: certificate of destruction (bulk uplift) Iron Mountain: signed preliminary disposal and email Iron Mountain: records inventory with destruction dates (see E5)
Electronic records - deletion process	Change of User Form & authorised signatories
Delegation of service delivery and use of authorised suppliers	Relevant sections of SBC/ CGI contract
Guidance and user forms	Intranet page- Your job/Information technology

Future Developments

From 2017 - review of retention schedules will include production of service, task and format specific guidance on destruction of records.

By end of 2017 – the Records Management Toolkit (that includes forms for Disposal Authority, destruction log etc.) will be re-written to take into account the documentation now available as a result of the Information Management Project 2016/2017.

In 2017 the Council contract with Shred-it came to an end. The Council is currently considering options mindful of the risk of increased fines under the new General Data Protection Regulation that a loss of sensitive data can attract. In the meantime, the Council will be operating under a rolling contract with Shred-it and continuing to follow existing arrangements.

From 2017 – a Property Asset audit will include locating "orphaned" records and managing their disposal according to Council record keeping standards. The agreed process for vacating Council properties that have been sold or leased will be revised to include a check for abandoned records before transfer – as is advised in Office Moves guidance. This extends to properties that are used by Council-owned companies, charities or partnerships whether leased or not. A change of ownership checklist and procedure will be published on the Council intranet and promoted through training and awareness sessions. The Council's Confidential Waste Policy must be applied in all cases to avoid costly fines and personal liability for loss of data.

Assessment and Review

The IGG will be consulted and must approve any change to the arrangements for management of confidential waste. As confidential waste management is a key deliverable in the Information Management Improvement Plan any risks arising from change of contract should be considered by IGG and added to the IGG risk register.

Internal Audit produced a report in March 2017 on the Information Management Improvement Plan and made recommendations to Corporate Management team regarding outstanding actions. IGG will monitor the risks arising from those outstanding actions which includes demonstrating that records destructions were carried out routinely and as scheduled.

Responsible Officers

Brian Frater, SIRO

Teresa Maley, Information Manager

Element 7 (Compulsory)

Archiving and transfer arrangements

This element is about the long term preservation of historical records and the process by which Council records are transferred at the end of their business use to Archives. It is compulsory to include this information in the Records Management Plan.

Statement of Compliance

The Council acknowledges that some of the records it creates have enduring value and as such should be accessible to the public and managed and preserved according to archival standards. These records not only preserve the corporate memory of the organisation and local democracy but provide a valuable historical resource that can be used by local residents, visitors and organisations in a variety of ways. Records suitable for transfer to the Archives are identified in the Council Retention Schedule. There is a form and a process for requesting transfer. After transfer, the Archives Service will weed out any duplicates and may process the records further following professional guidance provided by the Archive Manager, for example, on collecting policy, access restrictions or preservation techniques.

The Council had an in-house Archives Service until April 2016 when it transferred with other cultural services functions to Live Borders - a not for profit charity that delivers leisure and cultural services in the Scottish Borders. The Council retains ownership of the records transferred and complies with the Keeper of Records guidance "Proper Arrangements for Archiving Public Records" in terms of access to and good management of these records. The records donated to or purchased by the Archives, since transferring to Live Borders, to enhance collections are also owned by the Council. However, the Archives must consult with the Council before acquiring extensive collections. The Records Management and Archives functions have never been managed as one service at the Council and communication and collaboration between the two functions operates through regular meetings between Information Manager and Archives Manager. This continues under the new arrangements.

The Data Sharing Agreement with Live Borders and the Collections Policy describes the relationship between Live Borders Archives and the Council. The Archives Service has its own Collections Policy, procedures and guidance to ensure the records they preserve follow professional standards of care.

In addition to the Council Archive Service, that preserves and makes public historical records, the Council has a framework agreement with Iron Mountain to deliver records management services. The Archives Service is currently unable to provide space for the transfer of the larger collections of Council paper records (Planning Register or Architects plans and papers for example) these remain in long term storage at Iron Mountain with access managed by the service that created them. There is permissions based access to the records – to order standard services and supplies or deposit, retrieve/return, withdraw and destroy records – through the IM Connect self-service system. A variety of reports can be requested to assist good management and provide audit trails.

Evidence of compliance

Evidence of	Evidence
Council recognition that some records have historical value	Records Management Policy (see E3) Appraisal Statement (See E3)
Transfer Process/forms	Disposal Policy - records transfer form
Records held in archives (catalogue)	http://www.liveborders.org.uk/archives
Contractual arrangements in place	SBC/ Live Borders data Sharing agreement Live Borders Collections Policy
Standard processes followed by the Archives Service	Accessions database – screenshot Accessions receipt Archive List – example: Hawick Burgh Records Calm electronic catalogue – screenshot Collecting Policy –updated 2017 Document production slip

Future Developments

The working relationship with Live Borders will be monitored by the Information Manager and Archives Manager over the next year as it is a new arrangement. In particular, the practicalities of delivering Council responsibilities under FOI and Data Protection will be assessed. If required, a recommendation to create a service level agreement will be submitted to IGG to ensure public rights are not infringed by the new arrangement and the Council and Trust manage access in the most cost effective manner for both parties.

Assessment and Review

The Archives Manager, Paul Brough, is a member of the IGG to ensure the responsibility for proper management of Council Archives is fully represented on the Group and that any risks to service delivery are identified and mitigated promptly.

Standard contractual monitoring is in place.

Responsible Officer

Teresa Maley, Information Manager

Element 8

Information Security

This element is about the measures in place at the Council to ensure records are managed in a secure way. It is compulsory to include this information in the Records Management Plan.

Statement of Compliance

Keeping information secure is a requirement for the Council under the Data Protection Act. This applies equally to business information created by the Council and information that is received from others.

Information Management and IT (delivered by contractors CGI) are jointly responsible for service delivery of Information Security policy, training and monitoring. Corporate policy monitoring and review is the responsibility of the SIRO who is the point of contact should there be a data breach.

The Council has a suite of policies and guidance on information security available to staff. These are reviewed by IGG in the Information Security theme of the IGG calendar and are currently being updated to reflect the contracting out of service to CGI.

There are managed, auditable processes in place to ensure access to systems is authorised and the acceptable use of systems is monitored.

The management of security incidents is described in the Security Incident Reporting and Management process and was approved by IGG. There is a standard reporting form. The guidance is available for employees on the intranet and incident reporting (and lessons learned) is a standing agenda item on the IGG quarterly meeting.

There is an e-learning module on Information Security that is mandatory for all staff using computers in their work. Uptake of mandatory e-learning is reported to IGG as a standing agenda item.

Further guidance is available on the intranet including

- Portable devices and media
- Privacy by Design
- Security marking
- Protective monitoring

The Council works in partnership with Government agencies and completes an annual audit of information security and governance in order to use their systems (known as PSN compliance).

All Council issued laptops and memory sticks are encrypted. There are standard authorisation processes in place for use of Council systems and data by third parties or external contractors

Evidence of compliance

Evidence of	Evidence
Information Security Policy in place	Information Security Policy (see E6) PSN certificate
Information Governance assurance	Letter to Keeper from SIRO regarding outsourcing of IT Services
Access control	Intranet – Your job/Information Technology (see E6): Change of user Form New User Form Authorised signatories Guidance on which forms to complete
Partial delegation of Information security function	CGI Contract -relevant sections (see also E6)
Government protective marking	Think Security-Protective Marking
Security process to prevent hacking	Protective Monitoring Policy
Staff guidance in place	Intranet – Your job/Information Technology (see E6)
Logging, management and monitoring of security incidents	Security Incident reporting and management procedure and form (Disaster Recovery- see Element 10)
Awareness campaign and training	Examples: Check before you send Think Security- Protective marking Poster set (see E12) E-learning screenshots (Information Security)

Future Developments

PSN accreditation is carried out annually by the Council (2017 in partnership with CGI to reflect the contracting out of IT service to CGI) monitored by a Project Board that is chaired by the SIRO.

A Data Protection, Records Management and Information Security awareness campaign, using the existing Think Information brand, will be run annually.

Assessment and Review

Information Security is tested and monitored by CGI as part of the contractual relationship with the Council. This includes physical security monitoring.

The IGG monitors Information Security quarterly through Incidents reporting, updating the risk register and by scheduled policy and guidance review.

Responsible Officers

Brian Frater, SIRO

Bill Edwards, Interim Head of IT

Teresa Maley, Information Manager

Element 9

Data Protection

This element is about the measures the Council has in place to comply with the Data Protection Act, 1998.

Statement of Compliance

Council compliance with Data Protection is managed by the Information Management Team with support from the Council solicitors. The Information Management function is led by the Chief Legal Officer to ensure that the processes for managing subject access requests (SARS), compliance with other aspects of the Data Protection Act and internal advice given are lawful. The Information Team consists of the Information Manager and two Information Officers. There is currently a structure of Data Protection Liaison Officers across the business so that Subject Access Requests can be logged, circulated and completed effectively.

The Council has a Data Protection Code of Practice and procedures that is reviewed annually by IGG. All policies, codes of practice, procedures, guidance, forms and training are about to be reviewed as scheduled on the IGG Calendar and in context of the new General Data Protection Regulation that comes into force in May 2018.

The IGG receives reports on data breaches and security incidents, manages the risk to the organisation of not complying with the DP Act and reviews policy, procedures and other guidance and training as described in the Information Governance Strategy

The Council, the Licensing Board and Elected Members are registered with the Information Commissioner. Details can be found on the ICO website

The mandatory e-learning on Information Management Awareness and Information Security includes sections on Data Protection. There is a data protection and information security training module included in the suite of training for Information Asset Owners

There is an Incident Management procedure and template. A log of data breaches is maintained by the Information Team. Incidents are initially reported to the CGI Service Desk and those relating to loss of data are forwarded to the Information Team for logging and to the SIRO for a decision on actions to be taken.

There is Guidance for staff on Information Sharing and Privacy by Design. Project Managers have been issued an information sharing pack containing the Council Code of Practice, a copy of the latest Pan Lothian ISP and model protocols such as SASPI /Scottish Information Sharing Toolkit.

Compliance with Data Protection was a key driver in developing the Council's Information Asset Register so that the risks are visible, managed at business level and monitored by IGG

FOI and DP co-ordinators will receive training from the Information Team on a two monthly basis from 2017.

There is advice for the public on the Council website about rights to personal data including an application form to make a SAR – forms, guidance https://www.scotborders.gov.uk/info/20060/access_to_information/349/ask_to_see_information_about_you

Evidence of compliance

Evidence of	Evidence
Notification to the ICO	SBC: https://ico.org.uk/ESDWebPages/Entry/Z5573350 Licensing Board: https://ico.org.uk/ESDWebPages/Entry/Z5573350 Elected Members, Community Councils, Assessor: https://ico.org.uk/ESDWebPages/DoSearch
Policy and guidance in place	Data Protection Code of Practice CCTV Code of Practice Incident Management procedures and form (see E8) Information Sharing Code of Practice and Privacy by Design guidance and checklist
Training and guidance is available	Mandatory Information Management and Information Security elearning (see E3 and E8)
Mandatory training uptake and delivery of training report	IGG Minute 21 July 2016
Access to personal information is managed compliantly	Subject Access request form Non-disclosure form Info Asset Survey - fields
Privacy Impact Assessments (PIA) are carried out	Example of completed PIA
Data Breaches are recorded and managed	Data breach log - extract
Informing the public about their rights	"Information About You" page on SBC website

Future Developments

A new project or work package may be required to implement GDPR (completion May 2018)

Assessment and Review

Data Protection is reviewed by IGG under Information Access in the April to June quarter of their calendar each year and under Information Security in the July to September quarter.

Responsible Officers

Brian Frater, SIRO

Nuala McKinlay, Chief Legal Officer

Teresa Maley, Information Manager

Element 10

Business Continuity and Vital Records

This element is about the identification of vital records that are essential to the continuity of services in the event of a disaster and the processes followed to ensure they are always available.

Statement of Compliance

Scottish Borders Council in accordance with their statutory requirements under the Civic Contingencies Act 2004 have in place a Business Continuity structure and promote Business Continuity best practice to local businesses.

The Business Continuity Officer sits within Emergency Planning service.

SBC maintains an electronic database of all Business Continuity plans and as part of the planning process each key service must complete a Business Impact Analysis. This analysis identifies key functions around internal processes, internal and external procurement and data storage. It will identify the process of recovery of these key functions and the timeline required to implement that recovery.

Each department maintains a Business Continuity Plan containing that analysis information and this is reviewed annually.

Templates of the forms used are attached

Managers, supported by the Corporate Audit and Risk Officer within Audit and Risk service, maintain their service risk registers and conduct an annual review of identified risks in accordance with the Risk Management Policy and practices.

CGI are responsible for maintaining the backup and retrieval of all electronic databases and records held on the Council systems.

The IAR allows the service to record whether an information asset is a vital record. The risks deriving from analysis of the IAR will feed into the service risk register as they are embedded in standard management practice.

Evidence of compliance

Evidence of	Evidence
Responsibility for Disaster Recovery and Business Continuity	Information Security Policy (see E8)
Business Continuity Plan	BCP Analysis – Emergency Planning
Delegation of service	CGI Contract and letter from SIRO (see E6 and E8)
Standard process in place	BCP template
Vital records, back-up and data recovery process	Business Applications Systems – 2016 IT-DR – Titles and content extract and sign off
Awareness	Business Continuity leaflet

Future Developments

There are no planned future developments

Assessment and Review

Information risks are reviewed and monitored quarterly through the IGG risk register.

Each Service maintains and reviews annually its Business Continuity Plan with support from Emergency Planning service.

Each Service maintains and reviews annually its Business Plan and Risk Register with support from Audit and Risk service.

Responsible Officer

SIRO, Brian Frater

Element 11

Audit Trail

This element is about how the Council knows where a record is, who has had access to it to read, copy or change it and, at disposal, how authorization to delete was managed.

Statement of Compliance

At Scottish Borders Council there is a basic audit trail in most of the electronic systems used. However, some systems are specifically designed to be capable of recording the creation, use, editing, sharing and disposal of records as well as who can access them. These include

- Seemis – education records
- Framework – Social Work and Health records
- Uniform and IDOX – Planning, Building Standards, Licensing
- SharePoint EPM – Projects and Programmes records
- Business World/ERP – HR, Procurement, Finance
- Lagan CRM – Customer Services, Council Tax

Paper records that have been transferred to Iron Mountain can be tracked in terms of ingest, amendment of the inventory, transit to/from the repository, permanent withdrawal or destruction. An audit trail of the movements of each box or file can be reported through the online management system IM Connect.

The Council Archives Service uses a combination of paper document tracking systems (retrievals/returns in search room) and the Axiell/CALM cataloguing software (ingest, loans etc.)

The Council's Information Sharing Code of Practice recommends the use of disclosure logs when sharing information and these can provide an audit trail for individual information requests.

The FOI and Data Protection request logs similarly record information disclosed and where it emanated. This audit trail may be used, for example, in providing information to the FOI Review Group when an applicant is dissatisfied with our response to their request and asks for it to be reviewed.

Version control is used for key Council documents such as Committee Papers and Project reporting. There is guidance on version control in the RM Toolkit. The Toolkit is due a major update to reflect business changes and the guidance and training now available as a result of the Information Management Programme.

Evidence of compliance

Evidence of	Evidence
Audit trail – records in transit (paper)	Example: Iron Mountain– file transits by location (summary)
Audit trail – creating auditable records (digital)	Process for creating Planning and Building Standards records

Future Developments

The role of audit trails in providing evidence for disposal policy being applied in the Council network drives will be considered when the Office 365 project is scoped (2017).

Assessment and Review

The IGG monitors compliance with the Improvement Plan through the risk register. This includes, for example, demonstrating that disposal policy is being carried out.

Responsible Officer

SIRO, Brian Frater

Information Manager, Teresa Maley

Element 12

Competency Framework

This element is about the roles and responsibilities of staff involved in records management. It is also about how organisational training and development needs are identified and delivered.

Statement of Compliance

The Information Team, that is the Information Manager and the Information Officers (2), have records management duties included in their job descriptions. The post of Council Records Manager (created in 2000) was deleted in 2014 and the responsibilities of the post were divided between the two roles. By the end of 2017 all of the Information Team will have completed the ISEB certificates in Freedom of Information and in Data Protection.

The current Information Manager is a qualified Archivist with over 30 years of experience in Archives, Records and Information Management and is a member of ARA and IRMS. She attends ASLAWG and the SOLAR FOI and Data Protection Group.

The Live Borders Archive Manager is a qualified Archivist with a similar length of professional experience. A professional qualification is an essential requirement of the Archive Manager post.

A programme of staff development and training was agreed by IGG and is outlined in the Information Governance Pack. The Information Team are tasked with delivering this on a routine basis to improve the quality of information management and security across the Council. There was an awareness campaign in 2016 using the "Think Info" brand that the Council developed. It is planned to run another this Summer 2017. The Information Team have been involved in project related tasks to develop tools such as the Information Asset Register during most of the last year. Now that phase is complete it is likely that a large part of their role will be the delivery of training, creation of guidance and campaigns following the framework IGG agreed in the information Management Strategy, including

- Core skills training
- Training for Strategic /Information Asset Owners
- Awareness sessions for FOI Co-ordinators
- Members training support
- Ad hoc training delivered on the back of a new risk or incident
- E-learning (Mandatory)
- Creation and review of guidance, for example, when a legal framework changes or Council re-structure requires guidance to be refreshed or re-written

Evidence of compliance

Evidence of	Evidence
Information Team tasked with Records Management service	Information Manager Job Profile (see E2) Information Officers Job Profile (see E2)
A corporate training programme	Information Governance Pack (see E2)
Training tools	Mandatory E-learning (see E3 and E8) Awareness Posters set SB Learn – Information Management (E-learning) Staff Guidance on intranet Framework –i staff guides
Monitoring uptake of training	IGG Minute 21 July 2016 (see E8)

Future Developments

There are no future developments planned but the Records Management Plan will be updated if changes to personnel lead to re-structure of the Information Team

Assessment and Review

IGG monitors uptake of mandatory e-learning and training the Information Team delivers

Responsible Officer

Information Manager, Teresa Maley

Element 13

Assessment and Review

This element is about how the Council monitors the currency of and compliance with its agreed record keeping policies and standards.

Statement of Compliance

The Records Management Plan as a whole will be scheduled for review annually in the January to March quarter of the IGG Calendar alongside the records management policy, other documents and guidance. The Keeper will be informed of further improvements or personnel changes by the Information Manager. The IGG will monitor the implementation of any improvement actions arising from the approval of the Records Management Plan in keeping with the monitoring process recommended by The Keeper of the Records of Scotland.

In addition, some of the elements in the plan will be scheduled for review by IGG during the other review periods. The calendar is as follows

- Records management – January to March- would include annual review of RMP but individual elements of the plan also covered in other quarters
- Access to Information -April to June
- Information Security – July to September
- Information Governance – September to December

Internal Audit, have allocated 25 days in their Internal Audit Annual Plan 2017/18 for Information Governance. They are adopting a Continual Audit approach by performing a 'critical friend role' through the review of the IG Framework including roles and responsibilities, policy development and implementation, and assessing progress with implementation of improvement actions. They will also assess preparedness for the GDPR that comes into force May 2018.The audit will include any improvement actions arising from the approval process of the Records Management Plan. A copy of the Keepers recommendations will be shared with them by the SIRO for this purpose. In particular, they will assess whether the IGG RMP monitoring regime is analogous to that specified by the Keeper.

Evidence of compliance

Evidence of	Evidence
IG Assessment timetable	IGG Calendar in Information Policy and Governance Pack (see E2)
Risk Management at Scottish Borders Council	Risk Management Strategy Risk policy
Internal Audit monitoring Information Governance	Internal Audit Annual Plan 2017/18

Future Developments

No future developments are planned at this time

Assessment and Review

Any change to the IGG calendar will be reviewed during the Information Governance review period

Responsible Officers

SIRO, Brian Frater

Information Manager, Teresa Maley

Element 14

Shared Information

This element is about how Council information is shared with other organisations and individuals and how the Council manages information it receives.

Statement of Compliance

The Council works collaboratively with many external bodies to deliver services. Many are public bodies that have information governance arrangements in place that are similar to our own and an understanding of the implications of sharing information. However, the Council recognises that there is a high risk in assuming that information can be shared and will be handled compliantly by the recipient. As there is an increasing range of ways information is expected to be shared - from the creation of new joint services, contracting out the delivery of services or disclosing information for a specific incident, information request or piece of work – the Council knows that it must be vigilant in managing the process. At the very least we must:

- fully consider the requirement to and effect of sharing information;
- document what will be shared, by whom and how in contracts, Memoranda of Understanding or information sharing agreements;
- record disclosure; and;
- actively and routinely monitor any agreement or procedure.

If we don't do this the consequence could be failure to deliver services effectively further down the line or fines from the Information Commissioner.

To this end the Information Management Project created an Information Sharing Code of Practice that was approved by IGG in 2016. A guide to Privacy by Design – which is a key feature of the new General Data Protection Regulation – was approved at the same time. The Information Management e-learning module – that is mandatory for all staff – was updated to include data sharing.

As new collaborative working arrangements are generally delivered through the Corporate Transformation Programme a briefing was delivered at the Programme and Project Managers monthly meeting in June 2016. A Projects pack was created with the key compliance documents and examples of the Information sharing protocols the Council could use. Project managers were advised to consider information management at the outset of projects – including in pilot phase if they are made aware of it – and to ensure their Privacy Impact Assessment is included in all project documentation and reviewed as the project progresses. The Information Team has noted an increase in requests by staff and project managers to discuss information sharing early in the development of service improvement or review and plans to repeat the message in the next Security and Data Protection awareness campaign.

From April 2017, Business World ERP system will be used to record and manage contracts and offers the chance to develop an effective contract monitoring process that not possible in the systems it replaces. IGG will monitor the effectiveness of contract management through its risk register – the Improvement Plan includes a requirement to monitor 3rd party data processors because of the risk of data loss or breach under the Data Protection Act.

The Council has also recognised the need to identify and mark confidential or personal information appropriately. The Information Security policy describes the government marking scheme that it uses (only the classes Official and Official Sensitive apply to Council information) and how to use it in conjunction with additional security measures such as encryption and secure mailboxes. There is a managed and auditable vetting process for the issue of GCSX mailboxes.

To assist the promotion of good practice in information management key partners are represented on the IGG. Currently, SB Cares, Live Borders (Archives) and the Integration Joint Board (through the People representative) have representation on the group.

Evidence of compliance

Evidence of	Evidence
Security marking of records and messages	Info Security Policy (Protective Marking) see E8
Sharing Information procedures and forms	Information Sharing Code of Practice (see E9)
Building privacy into working practice	Privacy by Design guidance and prompt list (see E9)
Building good practice around information sharing into business as usual	Projects briefing and diary note of awareness session
Staff awareness	Information management E learning includes data sharing (see E3)
Monitoring information sharing agreements	3rd Party monitoring log
Managing access to secure information sharing	Change of user form and authorized signatories (see E6) Non-disclosure form (see E9)
ALEO complies with SBC record keeping standards	Letter of endorsement from Managing Director of SB Cares
Information Sharing Agreement	SB Cares Data Sharing Agreement
Managing access to systems or data	Information Security Policy (see E8)
Staff guidance on information requests	FOI Procedures Information Sharing Code of Practice and forms (see E9)

Future Developments

The introduction of Business World ERP system from April 2017 will allow an effective contract monitoring process to be put in place

Data Protection policies and procedures will be reviewed by IGG from April to June 2017 in keeping with the IGG calendar. Actions arising from the review may lead to a further project to ensure that the Council is fully compliant with the new GDPR (by May 2018).

Assessment and Review

The IGG monitors information sharing under the Access to Information and Information Security themes of the calendar. The membership of the Group is reviewed under the Information Governance theme or when a risk is raised around a transformed service.

Responsible Officer

Information Manager, Teresa Maley

ANNEX A: Evidence Submitted

Please find a list of evidence submitted in support of each of the elements of the plan below.

Element 1 Senior Management Responsibility	
Item No	**Description**
001	Information Management Programme Assurance Report
002	Corporate Management Team Agenda item 7 - Information Management Programme (2012)
003	Chief Executive Letter
004	Chief Legal Officer Job Description (21 Feb 2014)
005	Information Governance Improvement Plan (07 August 2013)
006	Information Governance Policy
007	Information Governance Group Terms of Reference
008	Information Governance Group meeting minute (21 July 2016)
009	Information Management Programme (29 April 2013)
010	Information Management Project Business Case
011	Information Management Project Board Meeting Minute (21 March 2016)
012	Information Governance Pack
013	Licensing Board Letter (25 April 2017)
Element 2 Records Manager Responsibility	
Item No	**Description**
014	Internal Audit Report on Information Governance (10 March 2017)
015	Information Management Project Delivery Plan
016	Information Management Project Business Case
017	Information Management Project Business Case Executive Summary
018	Information Manager Job Description
019	Information Officer Job Description
Element 3 Records Management Policy Statement	
Item No	**Description**
020	Records Management Toolkit
021	Information Governance Group meeting minute (17 November 2016)
022	List of Information Management Guidance for staff (SBC Intranet)
023	List of Information Technology Guidance for staff (SBC Intranet)
024	Records guidance for the public (SBC Website)
025	Records Management Policy
026	Records Management ELearning Slide 1
027	Records Management ELearning Slide 2
028	Records Management ELearning Slide 3
Element 4 Business Classification Scheme	
Item No	**Description**
029	Information Asset Questionnaire Guide
030	Information Asset Register FAQ
031	Information Asset Survey Template
032	SBC Intranet Structure
033	Planning and Building Standards process
Element 5 Retention Schedule	
Item No	**Description**
034	Appraisal of Records for Permanent Preservation v1.0
035	Disposal of Records v1.0
036	Environment & Infrastructure Retention Schedule v1.1 (June 2012)

037	ELL Department Retention Schedule v1.1 (June 2012)
038	Iron Mountain Inventory with Destruction Dates
039	Records Retention Schedules Review meeting request
040	Records Retention Schedules Review – Outcome note
041	Resources Retention Schedule v1.1 (revision June 2012)
042	Social Work Department Retention Schedule v1.1 (Revision June 2012)
Element 6 Destruction Arrangements	
Item No	**Description**
043	Signed Preliminary Destruction Listing
044	Disposal of Confidential Waste Management Policy v1.0
045	Services Agreement – Governance Issue 2
046	Services Agreement – Records Provisions
047	Services Agreement – Key Personnel Issue 2
048	Services Agreement – Substantive Terms Issue 2
049	Information Management ELearning content page
050	SBLearn content page – Information Management
051	Information Security Policy
052	SBC Intranet – Your Job/IT page
053	IT Authorisation Signatories List
054	Iron Mountain Destruction request email
055	SBC Change of User Form v2
056	Think Security – Think Office Moves Guide
057	Shred-it certificate 1
058	Shred-it certificate 2
Element 7 Archiving and transfer arrangements	
Item No	**Description**
059	Screenshot of Accessiondb
060	Accessions Receipt
061	Archive List (Hawick Burgh)
062	CALM Screen shot
063	Collecting Policy (revised 2017 v3.0)
064	Document Production Slip
065	Final Collections Agreement between SBC and Live Borders
066	Live Borders Data Sharing Agreement (01 June 2016)
067	Records Transfer Request Template
Element 8 Information Security	
Item No	**Description**
068	SIRO letter re CGI (25 April 2017)
069	Check before you send leaflet
070	GCSX and Call Log Process
071	Services Agreement - Security Management
072	Services Agreement – Commercially Sensitive Information
073	Services Agreement – Governance
074	Services Agreement – Records Provisions
075	Services Agreement – Business Continuity and Disaster Recovery
076	Services Agreement – Business Continuity and Disaster Recovery issue 2
077	Services Agreement – Key Personnel issue 2
078	Services Agreement – Substantive Terms issue 2
079	ELearning Menu – Information Security
080	ELearning – Information Security Menu
081	Protective Monitoring Policy v1.0
082	PSN SBC Customer Certificate
083	Security Incident Assessment Report Form

084	Security Incident Reporting and Management Procedure v1.4
085	Think Security – Protective Marking Guide
Element 9 Data Protection	
Item No	**Description**
086	CCTV Code of Practice 2013
087	Data Protection Code of Practice
088	Information Asset Survey
089	Data Breach Log
090	Information Governance Group Meeting Minute (21 July 2016)
091	Privacy Impact Assessment Pilot (3GS)
092	Privacy by Design Guidance and Prompt List
093	SBC Non-Disclosure Form
094	Sharing Information Code of Practice
095	Subject Access Request Form
096	SBC Website – Data Protection
Element 10 Business Continuity and Vital Records	
Item No	**Description**
097	Business Continuity Plan Template (June 2012)
098	Business Applications
099	Business Impact Analysis
100	Business Continuity Leaflet
101	IT Disaster Recovery process - extract
Element 11 Audit Trail	
Item No	**Description**
102	Iron Mountain Audit Trail
103	Planning and Business Standards Process
Element 12 Competency Framework	
Item No	**Description**
104	Information Management Awareness Poster set
105	ELearning – Framework-i
106	Framework-i generic guidance
107	SBC Intranet – Information Management section
108	SBC Intranet – Information Technology
109	SBLearn – Information Management Training
Element 13 Assessment and Review	
Item No	**Description**
110	Internal Audit Programme of Work 2016-17
111	Risk Management Policy Statement
112	Risk Management Strategy
Element 14 Shared Information	
Item No	**Description**
113	Information Sharing for Programmes and Projects – briefing
114	FOI Procedure Guidelines
115	Letter to Registrar General for Scotland (13 April 2017)
116	SB Cares Data Sharing Agreement
117	Third Party Register 2013
118	Procurement Terms & Conditions procedure
119	SBC Intranet – Contract guidance