Information Asset Owner Handbook

October 2017

Information Matters

take your time and get it right

Contents

1. Getting Started

1.1 Why does information matter?

Information and data are the key assets of the Council of the future. Becoming the Council we want to be: a Council where we can understand and anticipate our customer's needs; a Council where we can prevent, rather than treat harm, and a Council where we can use technology to achieve our priorities for our people and place, instead of simply using it to digitise existing customer and staff transactions. This will only be possible if our information and data is fit to support us.

Realising the value of our information and data to evolve as an organisation means we have to start managing it differently. We need a strong, consistent corporate approach to the management and governance of data and information, so that we have clear assurance around our information assets, and have information and data which is fit to enable our transformation. Because of who we are, a great deal of our information is about the people we serve. Being the custodian of this type of information about people's lives is a huge responsibility, so making sure we properly steward our people's information is critical in maintaining the trust between us and our customers we need to achieve our ambitions.

Our information and data is the cornerstone of us being open and transparent, because it allows us to explain and justify the decisions that we have made, evidence the processes we have followed, and comply with our legal and statutory responsibilities. This includes compliance with our data protection responsibilities: changes to data protection legislation place increased emphasis on the Council being able to proactively evidence how the way we use and govern our data complies with the law.

1.2 Who are Information Asset Owners and why do we need them?

Information Asset Owners are senior business managers who are responsible and accountable for the specific, defined information assets within their remit. Information Assets are identifiable collections of information or data which have value to the Council for its business. This could be a collection of physical case files, the data in a system or database, collection of files and folders on a shared drive, or the data produced and held within a CCTV system.

Because the Council serves the people and place of Aberdeen in such a diverse range of ways, the range and volume of information and data we create, receive and use to do this is huge. Because everyone who works here creates or uses information in some way, every day, to do our jobs, managing our information is everyone's business, and we all share responsibility for making sure we do it right.

That said we need to make sure that the Council has the right leadership, accountability and ownership for the management of its information.

This is your role as one of the Council's Information Asset Owners.

1.3 The Information Asset Owner role in brief

As an Information Asset Owner, you have five key areas of responsibility, and are accountable to the Council's Senior Information Risk Owner (SIRO) for undertaking them in accordance with the guidance in this handbook:

1. **Knowing your information asset(s)**
2. **Managing your information asset(s) throughout their lifecycle**
3. **Understanding risks and providing assurance**
4. **Fostering a culture where information is valued, respected and protected**
5. **Ensuring your information asset(s) are fully used for public good**

This handbook outlined the specific actions you need to take under each of these responsibilities, the tools available to support you, and where you can go for further advice and support.

1.4 Other Key Information & Data Roles

The Information Management Team
The Information Management Team are responsible for setting, owning and driving information and data governance standards and practice across the organisation. This team hold the corporate Information Asset Register on behalf of the Senior Information Risk Owner.

Senior Information Risk Owner
The Senior Information Risk Owner (SIRO) is accountable to the Council's Chief Executive Officer for the management of the information risks across the Council. This role chairs the Information Governance Group.

Data Protection Officer
The Council's statutory Data Protection Officer is responsible for monitoring the Council's compliance with Data Protection law, providing advice on data protection across the organisation and acting as the point of contact for the public and the Information Commissioner's Office. The Data Protection Officer is also responsible for fostering a culture throughout the organisation where customer's data is respected, valued and protected.

Information Governance Group
The Information Governance Group brings together specialist roles across the organisation in Freedom of Information, Data Protection, Risk Management, Performance, Information Security, Information and Data Management, and Information Preservation, Business Support, Organisational Development, and Corporate Investigations. The group monitors the Council's information governance performance and implements measures to improve assurance in this area.

1.5 Appointing appropriate Information Asset/ Data Stewards

As an Information Asset Owner, though you retain overall accountability for the information assets in your care, you can appoint one or more information asset or data stewards to help you carry our your role.

The best person to be appointed as an information asset/data steward is likely to vary depending on the information asset. For example, the right steward for data within a large line of business system which manages tenant data or social care case files is likely to be different from a steward for a collection of hard copy case files.

2. Information Asset Owner: Role and Responsibilities

As one of the Council's Information Asset Owners, your 5 key responsibilities are outlined below. Each responsibility has specific tasks associated with it.

Because the Council not only needs to make sure its information assets are managed appropriately, we also have to evidence that this is the case, you'll need to maintain certain records around the management of your information assets. For each responsibility below, there are actions you need to take, tools to support you, and the contact details of where you can go for further advice and support.

Working through the Information Assurance Checklist at Appendix 4 will ensure that you have the right evidence in place to demonstrate appropriate management of your assets.

2.1 Know Your Information Asset

Like any other thing of value that's essential for us to do our business, the Council needs to know what information it's got, where it's stored, what business it supports and how, who's using it and why, and what the risks around it are. We also need to know where the information comes from, where it goes, and who it's shared with.

2.1.1 What is an Information Asset?

An information asset is an identifiable collection of data stored in any manner, at any location, which is recognised as having value to the Council for the purposes of performing its business functions and activities. The collection should be managed as a single item. Further indications that a collection of information should be managed as an asset are:

- It is not easily replaced without cost, skill, time, resources or a combination.
- You should be able to see what the risks are to holding and using that information and it should be managed proportionately to the risk(s) it represents.
- The asset is the collection of information, and not the medium in which it is stored e.g. a collection of paper files, a database, a collection of documents on a shared drive etc.
- The inputs, outputs and stakeholders should be identifiable.

Information technology software and hardware are not in themselves information assets, it's the information they contain which is important. So to identify your information assets, you should ask the following questions:

Does it have value to your business area/the organisation?
How much would it cost to replace the information?
Would there be legal, reputational or financial repercussions if it was lost?
Would it have an effect on operational efficiency if you could not access the information easily?
Is there a risk associated with the information?
Is there a risk of losing the information?

Is there a risk that the information is not accurate?
Is there a risk that someone may try to tamper with it?
Is there a risk arising from inappropriate disclosure?
Does the group of information have a specific content?
Does the information have a manageable lifecycle?
Were all the components created for a common purpose?

All collections of information which contain personal information MUST be managed as information assets in accordance with this Handbook.

2.1.2 The Information Asset Register

The Information Asset Register is the Council's central register, used to record all information of value held by the Council. It records the type and format of information held, which Information Asset Owner is responsible for it, its value to the organisation and who uses it, and what for. The Information Asset Register allows us to identify, from a single source, the information assets held by the Council for the purposes of performing its business functions and activities. As an Information Asset Owner, you're responsible for maintaining entries about your information assets in the Register.

Action for Information Asset Owner
Register, and keep up to date your entries relating to your information asset(s) in the Council's Information Asset Register.

Tools
Information Asset Register Guidance at **Appendix 1**.
Information Asset Register return template

Further help and support
The Information Management Team

2.2 Manage Your Asset Through its Lifecycle

2.2.1 Creating adequate information to meet business and statutory requirements

Good information management practice starts before information is created or captured. Making good decisions about what information we create and capture are critical for making sure that the Council has the right information in the right place at the right time.

The Council delivers its different services and activities for different reasons. For some services or activities, for example, child protection, it may be that we are obliged or empowered by law to undertake the activity, or achieve the outcome. For other activities, we may not have a clear legal basis but they may be undertaken in line with our organisational priorities because there is a clear public interest for us to do so.

It's really important that the Council understands and maintains a record of the reasons why we hold and process each of our information assets. Your entry in the information asset register will record the relevant basis on which the activity your information asset supports is undertaken.

In addition to this, there may also be laws which relate to how the Council is required to carry out particular activities, which affect the type of information we need to create, and the way we need to manage that information throughout its lifecycle.

Obviously, the Council needs to make sure that we comply with any such legal requirements, but we also need to make sure that the information we create, and the way we manage it is sufficient to robustly evidence the decisions we take and the processes we follow where there is no specific relevant law.

This is a critical foundation of the Council being able to demonstrate transparency, and being accountable, as a democratic organisation responsible for delivering for the people and place of Aberdeen, and for the stewardship of public money and assets.

Action for Information Asset Owner

Make sure that your information assets are fit to comply with any legal requirements which apply to your business area, and sufficient to robustly evidence the decisions and processes of your business.

Further help and support

The Information Management Team

2.2.2 Conducting Privacy Impact Assessments

Where your information asset contains personal data, the Council needs to have a high level of assurance about the way we use and govern this type of data about people. The best way to ensure that data about people is governed and used properly is to make sure privacy issues are properly considered BEFORE starting to collect or use personal information.

A privacy impact assessment is a tool which can be used to identify and address any impacts on a person's privacy as a result of implementing a new policy, procedure, initiative or information system in relation to personal data. The privacy impact assessment process is best completed at a stage when it can genuinely affect the development of a project or initiative.

It may also be the case that you are considering using an existing information asset in a new way; it's important to remember that undertaking a privacy impact assessment must be considered when making any change to the way personal information within one of your information assets is collected, stored, used, managed or otherwise processed.

Undertaking the Privacy Impact Screening Questions will allow you to make an informed decision about whether a full assessment is required.

Action for Information Asset Owner
Conduct a Privacy Impact Assessment prior to taking decisions or making changes to the management of your information asset, where your asset contains personal information.

Tools
Privacy Impact Assessment Guidance
Privacy Impact Assessment Templates (includes Screening Questions)

Further help and support
Governance Team, Legal & Democratic Services

2.2.3 Collecting or capturing personal information: making sure it's lawful, fair and transparent

All collection, capture or creation of personal information must be fair, lawful and transparent by law.

If you are an Information Asset Owner who is processing personal information as part of your business then there are extra actions that you need to take, to make sure that the Council is able to robustly evidence to our customers and to regulators that we're handling their information lawfully, fairly and transparently.

Data protection law means that capturing, collecting, requesting, creating or otherwise gathering personal information can only be done where there the Council has what is called a 'condition for processing'. Relevant conditions for processing personal information are outlined in the Council's Corporate Data Protection Procedures.

As well as being lawful, the way the Council processes personal information also needs to be fair. An important element of fairness is transparency. The Council needs to make sure that the people who we are collecting or capturing personal information about know why we are doing this, what their information will be used for, how their information will be shared by us and how long we will keep it for.

This provision of this information to our customers is called a 'fair processing' or 'privacy notice'. The change of data protection law which will come into force in May 2018 means the information that the Council must provide in these notices has changed. This means that even if you have Fair Processing or Privacy Notices in place they will need to be updated to comply with changes in the law.

Information about how to put together an effective, up-to-date and compliant fair processing notice are outlined in the Council's Data Protection Procedures (Privacy Notices).

Action for Information Asset Owner
Make sure you're clear that where asset(s) contain personal information, information provided to customers about the way their information is

processed by the Council (privacy notices) are up-to-date and comply with new data protection requirements

Tools
Corporate Data Protection Procedures (Privacy Notices)

Further help and support
The Governance Team, Legal & Democratic Services

2.2.4 Contractual Arrangements

The Council can't contract out its legal responsibilities for its data and information, so we have to make sure that wherever we have arrangements in place with third parties which involve our data and information, we have robust contractual arrangements in place which hold our contractors to the standards we require in relation to our legal responsibilities under information security, data protection, freedom of information and public records legislation.

Without a robust contract, the Council may be exposed to monetary penalties for the failure of a contractor. The entering into, for any contractual arrangements, on behalf of the Council should be done through the Council's Legal Team in Commercial and Procurement Services, who will ensure that contractual clauses are adequate to meet the council's requirements.

Action for Information Asset Owner
Ensure robust contractual arrangements are in place with all third parties who play any part in processing data or information on behalf of the Council.

Further help and support
Legal Team, Commercial & Procurement Services

2.5 Knowing who has access and why: ensuring the use of the asset is appropriately protected and monitored

For each information asset you are responsible for, you'll need to understand and actively manage who has access to it and why, and maintain a record of this.

This means that if your information asset has different levels of access to it (for example, some users have read access, and others can edit data), you'll also need to maintain records of this.

It may be that your information asset is within a system which maintains appropriate records of users and their access rights, if not then you will need to make sure that a separate record is maintained of who has access to your asset and why.

Different information assets will require different levels of audit trails around access and use for example, for sensitive personal information assets like social care case files it is likely to be necessary to be able to have an audit trail which allows any access to the case file to be recorded. This may not be the case for all types of information assets. You will need to consider the level of access control and audit trail that is appropriate to your information asset(s).

Action for Information Asset Owner
Ensure that access to your information asset(s) is appropriately managed and you maintain records of who can access your information asset and for what purpose

Further help and support
The Information Management Team

2.6 Procedures, Training & Awareness

One of the reasons that you need to keep records of who has access to your information assets and why, is to make sure that people with access have the right information, knowledge and skills to do so appropriately.

This means making sure everyone with access to your asset is familiar with the Council's Corporate Information Policy, Corporate ICT Acceptable Use Policy, and the corporate procedures that support them (listed below).

This also means making sure that you have the right local procedures in place to support staff with any specific information they need to access information assets appropriately. In most cases, it will be appropriate to include this type of information within existing local team or service handbooks, which set out how business is done in your area, rather than creating separate procedures.

As well as information, staff need to have appropriate training. As an Information Asset Owner, you're responsible for making sure staff accessing your asset have undertaken the right training for their role.

Action for Information Asset Owner
Ensure that anyone who accesses your information asset (and particularly personal data users) are familiar with the Council Corporate Information Policy, The Corporate ICT Acceptable Use Policy, the Corporate Managing Information Procedures, The Corporate Data Protection Procedures and the Corporate Freedom of Information Procedures

Tools
Corporate Information Policy
Corporate ICT Acceptable Use Policy
Corporate Managing Information Procedures
Corporate Data Protection Procedures
Corporate Freedom of Information Procedures

Action for Information Asset Owner
Where appropriate, ensure that local procedures and guidance for your staff include any information about any specific requirements around the creation, updating, modification, organisation, communication, protection and disposal of your information assets

Action for Information Asset Owner
Make sure staff accessing your asset have completed appropriate information and data related training for their role. This includes appropriate induction for new staff and undertaking of refresher training and awareness activities for existing users. Refresher training should be taken on an annual basis

Tools
Data Protection Essentials OIL Course
For your Eyes Only OIL Training
Face to face training on request

Further help and support
The Information Management Team

2.6 Personal Information Sharing

Where your information asset contains personal information and this information is shared, you'll need to make sure that appropriate agreements or protocols are in place to support these sharing arrangements.

Data or information sharing covers a range of situations, including the disclosure of data from the Council to a third party organisation or organisations, or, in certain circumstances, the sharing of data between different parts of the Council. Sharing of data or information can take different forms, including:

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

More information on the routine and ad-hoc sharing of personal data is available in the Council's Corporate Data Protection Procedures.

It's important to be clear that the Council is the Data Controller for all the personal information that we hold, and it is always our decision and not the organisation requesting personal data whether or not we share or disclose it.

When making the decision whether or not to share or disclose data, it is ALWAYS our responsibility to ensure that we are satisfied there sufficient grounds for us to do so legally. For more information on information sharing and disclosure look at the Council's Corporate Data Protection Procedures.

Since sharing of personal information is a form of disclosure, you'll need to make sure that where personal information from your asset is shared or disclosed, you keep a record of the decision.

Police Scotland have developed their own form which is used to request personal information from external organisations like the Council. All requests for personal information from Police Scotland must be made using this form (ADM8/9).

Where you do not have a local system in place to evidence when and why personal information has been shared or disclosed, the Council's Personal Information Disclosure Form (Appendix 3) must be used to record the request and evidence the disclosure decision, and all instances must be reported quarterly to your Services' Information Management Liaison Officer.

Actions for Information Asset Owner

Making sure appropriate Information Sharing Agreements/Data Sharing Protocols are in place where data from your asset(s) is routinely shared with third parties.

Making sure any Information Sharing Agreements or Data Sharing Protocols are recorded in the Council's ISP Register, held by the Governance Team in Legal & Democratic Services.

Making sure ad-hoc instances of data sharing from your asset(s) are documented and records are maintained.

Tools

Corporate Data Protection Procedures
Information Sharing Agreement Template
Personal Information Disclosure Form (**Appendix 3**)

Further help and support

The Governance Team, Legal & Democratic Services

2.8 Business Continuity & Disaster Recovery

In many cases, our information assets are so essential to our business that we couldn't function without them. Where your information asset(s) are critical to your business, you need to make sure that you're satisfied with the arrangements in place in relation to business continuity and disaster recovery. These will vary, depending on the format of your asset (for example arrangements around physical records may be within your direct management, but those for assets within an IT system may be managed by whoever hosts the system).

If your business area would struggle to function without access to one or more of your information assets, you need to make sure that your Business Continuity Plan takes into account any information assets which are essential for your business.

It can be the case that a business area is able to function without access to an information asset in the short or medium term, but that the asset is vital for the Council being able to carry out its business or comply with its legal responsibilities in the longer term. For example, the Council requires to retain certain types of information, such as records relating to adoption for very long time periods, so we also need to be confident in the arrangements we have for protecting these types of information assets.

Action for Information Asset Owner
Make sure that your Business Continuity Plan takes into account any information assets which are essential for your business.

Tools
Identifying and Protecting Vital Information Assets Guidance (**Appendix 3**)

Further help and support
David McIntosh, Emergency Planning & Business Continuity Manager

2.9 Securing & Protecting Information

Appropriate measures to secure and protect your information asset(s) are likely to vary depending on the format of your asset and the type of information contained within it (for example arrangements around physical records may be within your direct management, but those for assets within an IT system may be managed by whoever hosted the system). In either case, you should ensure that you are satisfied that measures in place are appropriate for your asset.

Regardless of the format of your information asset(s), securing and protecting information assets is as much about the 'human element' as any technical or physical measures in place, so it's important to make sure you're satisfied that anyone with access to your information asset(s) have the right knowledge,

awareness and training to mitigate this factor as much as possible, as outlined at Section 2.6, above.

Action for Information Asset Owner
Ensure that you're satisfied that the technical and physical measures in place to secure and protect your information asset(s) are adequate.

Tools
ICT System Risk Assessment

Further help and support
Information Management Team

2.10 Incidents and Breaches

As an Information Asset Owner, you should regard any data loss as a cause for concern, and take immediate action to improve matters for the future. When problems occur, our culture at the Council has to be one in which losses are identified and learned from. This should apply both to actual problems and "near misses". This is vital if the Council is to avoid making the same mistakes, as well as allowing the Council to be open with individuals who may be affected by problems.

The Council's Data Protection Incident Management Procedure has been updated in line with changes in Data Protection law, so it's really important that you're familiar with it, and make sure that all users of your information asset(s) also understands what action they have to take in relation to Data & IT related incidents and breaches. Failure to take timely and appropriate action in the event of a data breach could expose the Council to serious monetary penalty.

Action for Information Asset Owner
Make sure that any incidents or breaches affecting your information assets are reported and managed in accordance with the Council's Incident & Breach Reporting Procedure and that you maintain a record of any such incidents.

Tools
Corporate Data Protection Incident Reporting Procedure

Further help and support
Governance Team, Legal & Democratic Services

2.11 Retaining & Disposing of Information

Council information should be kept for as long as it is required to carry out business, or to comply with the Council's statutory responsibilities and legislative requirements. It is really important we make sure that we don't keep any information longer than we should: holding on to information we no longer require can have as serious consequences as not keeping information long enough.

It makes it harder to find the information we do need and costs the Council money (whether the information is in hard or electronic copy). Keeping information containing personal data for too long, or not keeping information up to date, is likely to also mean that the Council is in breach of Data Protection.

Making sure your information asset(s) are retained and disposed of appropriately is a key part of your role as an Information Asset Owner, and that where records are destroyed this is recorded. The Council's Retention & Disposal Schedule sets out the retention periods for different types of Council information and data.

A small proportion of the Council's information is identified on the Council's Records Retention & Disposal Schedule for permanent retention in the Council's Archive Service.

Where any of your information from one of your information assets is scheduled for permanent preservation, you should arrange a regular schedule of transfers to the Council's Archive Service.

Actions for Information Asset Owner

Ensure that information and data within your information assets are retained and disposed of in accordance with the retention guidance set out in the Council's Retention & Disposal Schedule, and that disposal action is recorded using a disposal log.

Where any of your information from one of your information assets is scheduled for permanent preservation, arrange a regular schedule of transfers to the Council's Archive Service.

Tools

Corporate Retention & Disposal Schedule

Records Disposal Log

Further help and support

Information Management Team

Archives Team (for records scheduled for permanent preservation)

2 Understanding the Risks and Providing Assurance

3.1 Managing Risks relating to your Information Asset

Because we rely on our information assets we need to make sure that we're actively managing any risks in relation to them. The kinds of risk likely to apply to information

assets will depend on many factors, but some key areas which may be helpful to get you started in thinking about the risks which may apply to your information asset(s) are:

Risk Category	Example of Risk
Governance and culture	• Lack of comprehensive oversight and control (e.g. inadequate training to fulfil the expectations put on staff to handle and protect sensitive data correctly) • When something goes wrong, handling it badly and not learning • Third parties letting you down • New business services do not take information risk into account
Information management and information integrity	• Critical information is wrongly destroyed, not kept or cannot be found when needed • Lack of basic records management disciplines • Inaccurate information • Information becomes unreadable due to technical obsolescence • Information is lost or exposed
The human dimension	• Despite having procedures and rules, staff, act in error, act incorrectly • Despite having procedures and rules, insiders, act incorrectly • External parties source your information illegally
Information availability and use	• Inappropriate disclosure of sensitive information • Failure to disclose critical information for case management/protection • Failure to utilise the value of the information asset • Failure to allow information to get to the right people at the right times
Technology	• Denial of service due to systems failure • Corruption of data leading to delay in services
Process disruption	• Established processes disrupted by new regulation
Proportionality	• Providing more information than necessary for completion of a process leads to the risk of a breach being more critical than it need be

Action for Information Asset Owner

Ensure that, wherever appropriate, risks to the business related to your information asset are included in service risk registers.

Tools

Risk Management Manual and associated guidance

Further help and support

Neil Buck, Performance & Risk Manager

3.2 Information Assurance Statements

The Council's Senior Information Risk Owner (SIRO) is responsible for providing assurance to the Chief Executive on the management of the Council's information risks. Your role in this is to provide the SIRO with regular assurance about the way your information asset is managed.

This is done using the Information Asset Assurance Statement.

Action for Information Asset Owner
Complete annual Information Asset Assurance return to the SIRO when requested

Tools
Information Asset Assurance Statement (**Appendix 4**)

Further help and support
The Information Management Team

4. Fostering a culture where information is valued, respected and protected

The Council relies of the trust of the people of Aberdeen to do its business effectively. The way we care for and protect the information we hold about our people and place is a key part of fostering this trust.

The Council must have visible and transparent measures in place to demonstrate that our people's data is treated with sensitivity, care and diligence. Everyone who works here must show by their actions as well as their words that they treat information with care and respect.

As an Information Asset Owner, you're responsible for managing your own information asset(s), but you're also responsible for fostering a culture that properly values, respects and protects information and data across the Council.

This means being seen to value, respect and protect the Council's information, taking part in corporate campaigns to improve information governance.

Action for Information Asset Owner
Foster a culture of where information is valued, respected and protected appropriately across the organisation, supporting corporate campaigns to improve information governance

Further help and support
Information Management Team

5. Using information assets for Public Good

Whilst you're accountable for the management of your information assets in accordance with this handbook, it's important to remember that all of our Information Asset Owners have a key role to play in making sure that the Council's information is fully used for the success of the Council as a whole and the good of the people and place we serve.

Action for Information Asset Owner

Work with the Data Office and with other Information Asset Owners across the organisation on data and information related projects and programmes to improve information assurance and ensure our data and information is fit to enable the Council's strategic transformation objectives

Further help and support

Caroline Anderson, Information Manager

Appendix 1: Information Asset Register Guidance

Appendix 1: Information Asset Register Guidance

Field No.	Field Name	Explanation of how to complete it	Worked Example	Explanation of worked example
The Information Asset				
1.1	Information Asset Name	This is a free text field where you should enter the name of your information asset.	Burial & Cremation Register and associated records	
1.2	Information Asset Description	This is a free text field where you should briefly describe your information asset.		
1.3	Information Asset Format	There are three options to choose from in the drop-down for this field: **1. Hard Copy** This should be used for information assets which are held in paper format. **2. Unstructured** This should be used for information assets which are held files or folders on Council's network drives or within the Council's email system. **3. Structured** This should be selected if your information asset is held in a database, line of business or case management system	Structured	
1.4	Type	This is where you should record the type of data contained within your information asset. You should select one option from the following drop-down: **1. Sensitive Personal Data** Select this option if your information asset contains any personal information at all which reveal:	Personal	

		• a person's racial or ethnic origin • a person's political opinions • a person's religious or philosophical beliefs • a person's membership of a trade union • a person's health • a person's sex life or sexual orientation • genetic or biometric data which are processed for the purpose of uniquely identifying a person. **2. Personal Data** Personal data is defined as any data relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly, or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. **3. Other Sensitive** There may be rare instances where your information assets contain non-personal information which is sensitive for other reasons. This may include, information about corporate emergency planning information, cyber security measures or sensitive financial information. This is category is not likely to apply to the majority of the Council's Information Assets. **4. Non Personal or Sensitive Data** If your information asset does not contain any sensitive personal data, personal data or sensitive data, as defined above, please select this option.		
Personal & Sensitive Personal Data (this section only needs to be completed if your information asset contains personal or personal sensitive data)				
3.1	Data Sharing	Yes or No	Yes	
3.2	Data Shared with externally	Enter the organisation with whom data is shared.	Funeral Directors	

3.3	Data Shared with internally	Enter the team or service with who information is shared with internally		
3.4	Data Origin	This field only needs to be completed if your asset contains personal or sensitive personal data. This is where you should record where the data within your information asset comes from. Select the most appropriate option from the drop down: **1. Customer Directly** In most cases, it will be our customers themselves who provide us with the personal and sensitive personal data about themselves we need to undertake our activities. If this is the source of the personal information contained in your asset, select this option. **2. Third Party** There may be times when we receive personal information about our customers from third parties. Because it may be the case that your information contains personal information which is received directly from our customers as well as personal information about our customers received from third parties, select both options if this is the case.	Customer directly	Information is provided by the person applying for the burial or cremation
3.5	Country data processed in (Personal Data or Sensitive Only)	If information from your asset is transferred outside the UK then you should enter the countries to which it is transferred here. For externally hosted (web or cloud based) systems enter the country where the third party stores the data. This information will be included in the Councils' contract with the third party. For web hosted systems, the location is the data is where the third party locates its servers.	UK	
Legal Basis & Requirements				
5.1	Statutory Requirement (have to)	If your information asset exists because it is necessary to support an activity or an outcome which the Council is required to undertake or achieve by law, put the piece of	Burial & Cremation (Scotland) Act 2016	The Council is required by this law to provide burial

		legislation from which the Council derives its obligation here.		grounds
5.2	Power (can do)	If your information asset exists because it is necessary to support an activity which we are empowered to undertake by law (rather than obliged to), put the piece of legislation from which the Council derives its powers in this field.	Burial & Cremation (Scotland) Act 2016 (empowered to provide crematorium)	The Council is empowered by this law to provide a crematorium.
5.3	Legislation which applies to the way we do this activity, if we do it	Enter here any legislation which relates to the way in which the Council carries out the activity which your information asset supports.	Burial & Cremation (Scotland) Act 2016	The piece of legislation specifies law In relation to how burials and cremations must be carried out in Scotland
5.4	Legislation relevant to information and record keeping (other than data protection)	Enter here any legislation which applies to your information asset which lays down specific requirements for the management of it. For example, the Adoption Agencies (Scotland) Regulations 2009 specified that Adoption Case Record must be retained for 100 years.	Burial & Cremation (Scotland) Act 2016	This legislation specifies the format that Burial & Cremation Registers need to be kept in (electronically) and the length of time they need to be retained.
Business Functions & Activities				
2.1	Function	Our information Assets support the Council to carry out our functions as an organisation. Our organisational functions are defined in our business classification scheme is a 3 level hierarchical model which sets out our functions, activities, and sub-activities. Choose the most appropriate function using the Records Retention & Disposal Schedule.	Communities	
2.2	Activity	Choose the most appropriate activity using the Records Retention & Disposal Schedule.	Bereavement Services	

2.3	Sub-Activity (BCS)	Choose the most appropriate sub-activity using the Records Retention & Disposal Schedule.	Cremations and interments	
2.4	Value (Business Criticality)	Select the most appropriate option for your information asset, from the options below: **1. Business Critical** Only select this option if your information asset is essential to undertake one of the Council's identified critical functions. **2. Service Critical** Only select this option is your option if your information asset is essential to undertake one of your service's identified critical functions. **3. Non Critical** Select this option if your information asset doesn't fall into either of the categories above. Selecting this option does not mean that you asset is not important to the Council, or essential for your team's business.	Business Critical	Providing burials and cremations is one of the Council's identified critical functions.
2.5	Entity	Select from the most appropriate option form the following drop down in terms of the entity (data word for 'thing') which your information asset most relates to: **1. Customer** Examples, social work case management system, school clothing grants database or **2. Employees** For example, personnel files, or HR system. **3. Place** For example, asset management files about council properties, or deeds. This would also include GIS data.	Customer	
System or Location Information				
4.1	System Name	If your information asset exists within case management	BACAS	

		system, line of business system or database, please enter the name of it here.		
4.2	System Location	This field records where your information is stored. For hardcopy records, this will be a physical location, for example, Marischal College, or Tullos Depot. For information assets within files and on the Council's shared drives, or systems which are internally hosted within the Council, enter the location as Internally Hosted. For information assets which are stored on systems or locations which are externally hosted or hosted on web based systems (cloud), enter the locations where the third party stores the data. This information will be included in the Councils' contract with the third party. For web hosted systems, the location is the data is where the third party locates its servers.	Council Private Cloud with Bright solid	
4.2	System Users	Enter here groups of staff who have access to your information asset.	Bereavement Services Staff	
4.6	System Provider	If your information asset is within a system provided by a third party company, enter the name of the company here.	Clearskies Scotland	
Version Control				
6.0	Register updated on	This field is so we can understand when entries in the register have been updated. Please enter the date of your entry in the format dd/mm/yyyy.	06/06/2017	

Personal Information Disclosure Form

October 2017

Any third party request for personal data Aberdeen City Council must be recorded.
This form must be used where no local arrangements are in place for recording third party personal data requests

Section 1: Data Requester	
Organisation	
Contact Name	
Address	
Contact Telephone	
Contact Email	

Section 2: Data Requested	
Data being requested	
Purpose data required for	
Potentially relevant Exemptions	

Section 3: Decision and Authorisation (to be completed by IAO)		
Will information be shared as per above request (please indicate)	**YES**	**NO**
Record basis for decision here		
Name of IAO/Authoriser		
Job Title		
Description of information shared		
Method by which information was shared		
Date information was shared		

Aberdeen City Council will process the personal information provided in this form in order to efficiently administer this request for information in accordance with our powers under the General Data Protection Regulation, and will be retained for three years regardless of whether we decide to disclose information or not, as part of our records of compliance with the General Data Protection Regulation.

This information will not be shared with any third parties unless we are required to do so by law. For your rights in relation to your information please see our Privacy Charter. If you'd like to find out more about the way the Council processes Personal Data please contact Fraser Bell, our Data Protection Officer.

ABERDEEN CITY COUNCIL / Shaping Aberdeen

Appendix 3: Identifying & Protecting Vital Information Assets

This guidance is intended for Information Asset Owners responsible for producing and updating business continuity plans for their Service or Directorate.

1. What are vital information assets?

Vital information assets are either:

- **Information the Council needs to continue operating vital services in the event of a business continuity incident or a disaster**. For example, it may be impossible for the Council to continue to provide social care services to vulnerable clients without access to client records held on the CareFirst system.

- **Information that the council cannot afford to lose for longer term business or legal reasons.** For example, whilst it may not have an immediate impact on the Council's ability to provide Social Work services, the Council is required by law to keep records relating to adoptions for 100 years. If this information was lost, it would be a very serious failure of the Council's duty of care to adopted people, and would have a serious impact on the lives of the individuals involved.

Examples of **business continuity incidents** include: being unable to enter a building for several hours or days (in the event of, for example, a bomb scare) or being unable to access the Council network for several hours or days); **disasters** include fire, flood, and the loss of electronic data through malicious electronic intervention, which can lead to the loss of information forever.

Vital information enables the organisation to continue functioning in the event of a disaster or incident, and contain the information needed to re-establish the organisation in the event of a disaster that destroys all other information. In the case of the Council, vital information may apply to the Council as a whole, or to a specific service or directorate. Vital information can be held in any format, including paper and electronic formats.

2. Why do vital information assets matter?

Identifying your service's vital information, taking measures to protect it, and ensuring (so far as possible) that it is always available when needed, whenever its needed, will mean that you service's staff will be able to continue providing services to customers in times of crisis, and that you have the irreplaceable information you need in the medium and longer term. A clear understanding of vital information is part of good information management practice, and should tie in with your service's business continuity planning arrangements.

Your service's business continuity plan should consider what the consequences for your area of responsibility would be if you were unable to access your information for a few hours or days, or were to lose your information forever, and the vital information backup measures that you install should reflect how critical your information is, and how urgently you would need access to it.

3. Who is responsible for my service's vital information assets?

Information Asset Owners are responsible for making sure that a vital information asset is identified as such, and appropriate measures are put in place to protect it. Information Asset Owners should make sure that relevant Business Continuity Planning and Disaster Recovery arrangements include provision for vital information assets.

All staff are responsible for working sensibly with vital information and so it is necessary that all staff know what your service's vital information is, and what the service's business continuity and disaster recovery arrangements are.

4. How do I tell which information assets are vital?

What constitutes a vital information asset will vary from service to service. This guidance gives you a toolkit to help you identify your section's vital records.

When identifying your service's vital information, consider the following points:

1. What are the core functions and activities of your service? This may be protecting children, maintaining roads or processing benefits claims. For help, look at the Council's Business Classification Scheme which outlines all of our functions and activities.

2. What information do you need to enable you to perform these core functions, or to provide evidence that you have done so? This should be included in your service's file plan.

3. Identify which of this information is vital: can the functions or activities the information relates to be re-established in the event of the loss of this information? If so, the information is not vital (although in some cases you may still consider their importance to be sufficient that they are worth protecting). If not, the information is vital and measures should be put in place to protect it.

It's important to consider the following points, when you're identifying whether information is vital or not:

- **Not all information is vital:** around 2-10 % of any organisation's information is likely to be vital, although this will vary from case to case. Setting up

special protection measures can be expensive, so do not be tempted to include everything.

- **Vital information is vital for varying lengths of time**: information is not necessarily vital forever.
- **Information may not fall neatly into vital and non-vital categories**. It may be more helpful to divide your information into 4 different categories, as in the table below.

1. Vital Information Assets	
Business Critical Information Assets An information asset which is vital to carry out one of the Council's identified critical functions. To meet this criterion the Council must be unable to carry out one of its business critical functions without access to this information asset.	Examples: • Children's and adult social care case files held on the CareFirst system • Payroll information held on the PSe system, and associated databases
Service Critical Information Assets An information asset without which a service cannot function. These information assets are essential to the core business of the service.	Examples: • Any information vital for the delivery of a council function or activity, other than those which have been identified as Council critical functions • Information subject to a legal requirement to be kept for a certain amount of time • Historical records needed for evidential or other legal purposes
Information Assets vital in disaster situations These records are vital in case of a disaster because they are critical for emergency procedure and crisis management purposes.	Examples: • Key staff contact details • Staff records • Next of kin details • Business Continuity plans
2. Important Information Assets	
Information which is important to the continued operation of	Examples: • Procedures

the organisation. It can be reproduced or recreated from original sources, but only at considerable time and expense.	• Some policies • Minutes of some meetings
3. Useful Information Assets	
Loss of this information would cause temporary inconvenience to the Council.	Examples: • Most correspondence
4. Non-Essential Information Assets	
This information has no value beyond the immediate purpose for which they were created	Examples: • Staff circulars about one-off events which are now completed • Advertisements

5. Protecting Vital Information Assets

Now you've identified your vital information assets, you should make sure that, where appropriate, they are included in your Business Continuity & Disaster Recovery arrangements, and make sure that adequate measures are in place to protect them:

5.1 Protecting vital information assets held electronically

Electronic vital information assets will usually fall into two broad categories:

- Information Asset held in specific business system or application

For an vital information assets held in a specific business system or application, ensure that an ICT Security Risk Assessment has been carried out for the system, and agree with the Council's IT & Transformation Service the appropriate level of protection required for the system.

- Information Asset held outwith business system (on network shared drives)

For vital information assets outwith business systems (on network shared drives), backup copies are regularly made and should the any of the information be accidentally deleted, it can be restored from the backup copies of the server. **No Council information, vital or otherwise, should be stored on local hard drives**. Backup regimes and procedures, including the length of time needed to restore lost

data, may vary, and so if you have identified vital records which are currently held on network drives, you should contact the Council's IT & Transformation Service, to make sure of what the procedures and timescales are for restoring the information asset in the event of an incident, and if these meet with the needs of your service.

5.2 Protecting vital information assets held in hard copy

For vital information assets which are held in hard copy (usually paper) there are a variety of backup options. Deciding which to adopt is about balancing what is practical, given your location, environment and resources, with what is desirable, given the nature of the information. You should aim to provide reasonable protection for most information and extreme protection in a small minority of cases: Adoption records, for example, require a high level of protection by law. Weigh up the costs of different levels of protection against the potential cost of the loss of the information. It may also be helpful to consider the volume of information that need to be protected now, and how that may change in the future; what the retrieval rate is likely to be; and whether any special environmental conditions are needed for storage. For hard copy information you should also consider the following points:

- **Check the environment for potential hazards**

There may be vital information that can only be retained in hard copy. In these cases you should look for different types of environmental threat to the area where they are stored, for example are they stored close to hazardous chemicals, or beneath water pipes likely to leak. Steps should be taken to protect the information from these potential hazards, or alternative accommodation should be found.

- **Consider duplicating and dispersing across two location**

This affords a fairly low level of protection, but is relatively cheap. It may be considered adequate especially if there is more than one building across which copies can be spread.

- **Keep records in boxes**

Stout cardboard boxes will offer some short-term protection from fire and water. Paper tightly packed in cardboard boxes is less likely to burn, and cardboard boxes offer a reasonable protection from water.

- **Prioritise what information should be saved in an emergency**

Your Business Continuity Planning and Disaster Recovery arrangements should record what information should be saved first in the event of a crisis. Think about the location of this information - can it be removed from the building quickly in the event of emergency?

5.3 What method should I adopt?

When deciding what reasonable methods you need to adopt to backup and protect your vital information, it is necessary to balance the financial cost, time and practical implications of the methods against the seriousness of the damage that would result if your vital information were unavailable for a period of time, or destroyed. Consider the following:

	High	Medium	Low	Very low
How serious would the consequences be if the records were destroyed or stolen?				
How serious would the consequences be if the records were unavailable for several hours?				
How serious would the consequences be if the records were unavailable for a few days?				
What is the cost of the backup and protection measures?				
What is the volume of records that need to be protected now?				
What is the volume of records likely to need protection liable to be in 10 years' time?				
How likely is it that another copy already exists elsewhere?				

This matrix will not provide you with a simple answer, but is intended to help you to consider the issues involved. For example, if the consequences of losing access to particular information for a few hours are very low, but the consequences of losing access to the same information permanently would be very high; this may inform the level of protection which is appropriate. If the consequences of theft or destruction would be extremely high, then you may need to adopt stringent security and protective measures.

If you'd like further help and support, contact the **Information Management Team.**

Appendix 4: Information Asset Assurance Checklist template

Assurance Statement	Yes/ No	Remedial Action Required	Completion Date	Review Date
Know Your Asset				
The Information Asset Register				
I know which Information Asset(s) I am responsible for				
My Information Asset(s) is up to date on the Council's Information Asset Register				
Manage Your Asset Through its Lifecycle				
Conducting Privacy Impact Assessments				
Where required, Privacy Impact Assessments have been conducted in relation to my information asset				
Contractual Arrangements				
Robust contractual arrangements are in place with all third parties who play any part in processing, hosting or supporting my Information Asset(s)				
Creating Information				
The data and information robustly evidence the decisions and processes of my business				
My Information Asset(s) meets any legal requirements specific to my business area				
Collecting or capturing personal information				
Where asset(s) contain personal information, information provided to customers about the way their information is processed by the Council (privacy notices) are up-to-date and comply with new data protection requirements				
Knowing who has access and why				
I know who accesses and uses my Information Asset(s) and why, and have records to evidence				

Procedures, Training & Awareness				
I am satisfied that users of my Information Asset(s) are aware of and understand their responsibilities under the Council Corporate Information Policy, the ICT Acceptable Use Policy, and procedures which support them				
I am satisfied that there are appropriate local procedures or guidance in place around the creation, organisation, use, protection, communication and retention and disposal of data in relation to my Information Asset(s)				
I am satisfied that all users of my Information Asset(s) have undertaken the right level of training and awareness activity in relation to the proper use of my Information Asset(s)				
Personal information Sharing				
I know where my Information Asset(s) is shared and appropriate Information Sharing Protocols (ISPs) or agreements are in place to support this sharing				
All ISPs are recorded on the ISP Register held by Legal & Democratic Services				
Decision making about ad-hoc instances of sharing from my Information Asset(s) is appropriately recorded and reported				
Business Continuity & Disaster Recovery				
I am satisfied that appropriate Business Continuity and Disaster Recovery arrangements are in place in relation to my Information Asset(s)				
Securing & Protecting Information				
I am satisfied that the technical and physical measures in place to secure and protect my information asset are appropriate				
Incidents & Breaches				
I manage all incidents, breaches and 'near				

misses' in relation to my Information Asset(s) in accordance with the Council's Data & IT Incident Reporting Procedure and maintain a record of any such incidents				
Retaining & Disposing of Information				
I am satisfied that my Information Asset(s) is retained and disposed in accordance with the Council's Retention and Disposal Schedule, and are recorded in my disposal log				
Understanding the Risk & Providing Assurance				
Managing Risks relating to your Information Asset				
I actively manage the risks in relation to my Information Asset(s) and make sure that these risks are included on Service Risk Registers wherever appropriate				
Culture				
Leading and fostering a culture that values, protects and uses information for the public good				
I am satisfied that users of my Information Asset(s) are aware of an understand the Council's Corporate Managing Information, Data Protection and Freedom of Information Procedures				
I am satisfied that there are appropriate local procedures or guidance in place around the creation, organisation, use, protection, communication and retention and disposal of data in relation to my Information Asset(s)				
Ensuring that your information asset is fully used for Public Good				
I play my part in corporate projects or programmes to improve information assurance and ensure our data and information is fit to enable the Council's strategic transformation objectives				
I ensure that Subject Access requests in relation				

to my Information Asset(s) are responded to in accordance with statutory requirements and timescales				
I ensure that FOI and Environmental requests in relation to my Information Asset(s) are responded to in accordance with statutory requirements and timescales				