ISLINGTON

Information Asset Owner Policy

A council-wide information policy

Version 1.3
December 2020

Copyright Notification

Contacts

If you need any further information about this document or any clarity about the contents of the document, please contact: The Information Governance Team (dp@islington.gov.uk).

Revision History

Date	Version	Reason for change	Author
May 2014	0.1	First version	Leila Ridley
July 2014	0.2	Following consultation with CGG, DSWG and Information Leads.	Leila Ridley
December 2014	0.3	Changes following HASS SMT discussion.	Leila Ridley
December 2014	0.4	Addition of Information Lead R&R.	Leila Ridley
January 2015	1.0	Formal approval and adoption by CMB.	Leila Ridley
March 2018	1.1	Annual review	Leila Ridley
March 2019	1.2	Annual review	Lisa Ford
December 2020	1.3	Annual review. Changes to incorporate UK GDPR, update SIRO and Board details	Lisa Ford

Table of contents

1. Purpose of this document

This document sets out the council's approach to managing its data. It explains the concept of an Information Asset and defines the role of the Information Asset Owner who is responsible for each Information Asset. This document also sets out the primary responsibilities of an Information Asset Owner for managing the risks to personal data and business critical information held within a department. It should be read in conjunction with the Information Risk Policy.

The council uses the Information Asset Register as its Records of Processing Activities (ROPA) to ensure we meet our Article 30 obligations of the UK General Data Protection Regulation (UK GDPR).

2. Background

The council holds a wealth of information. This information can be in different formats and held in a variety of locations and systems. It is essential that the council understands the information it holds so that we can adequately manage and protect it. Article 30 of the UK GDPR requires organisations to maintain a record of the personal data that it processes, the council has extended its use of the Information Asset Register to incorporate these requirements.

When considering changes to business processes or ways of working, it is particularly important that the council understands what information it holds, who is responsible for the information, the legal status of the information, and how it can legally be used. Having a robust and well-documented understanding of this allows the council to drive its transformation agenda by helping services to become more efficient in storing, locating and retrieving the information.

To manage this information, the council needs to have Information Asset Registers which are managed by Information Asset Owners. Information Asset Owners are senior members of staff who have been appointed by their Corporate Director to be responsible for one or more identified information asset(s). This person will be responsible for ensuring that the Information Asset is accurately stored and maintained on the Information Asset Register. The corporate Information Asset Register will be owned by the corporate Information Governance Team.

The Information Asset Owner (IAO) is appointed by the Corporate Director and will provide assurance to the Senior Information Risk Owner (SIRO) on the security and use of their assets. They are responsible for ensuring that specific information assets are accessed, handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

Performing the role well brings significant benefits. It provides a common, consistent and unambiguous understanding of what information the council holds, how important it is, how sensitive it is, how accurate it is, how reliant the council is on it, and who is responsible for it. It helps ensure that the council can use the information to operate transparently and accountably, for example to meet open data standards, to unlock previously unavailable data and to improve public service.

3 What is an Information Asset?

The council needs to understand its information and how to manage and protect it. To enable the council to manage and protect its information, it is vital to understand what is meant by the term 'information asset'.

"An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.[1]"

For information to be defined as an asset it needs to be of value to the organisation. The council needs to consider the risk associated with the information and understand both the content and lifecycle of the information.

This is not about system ownership but data ownership – who takes service level responsibility for how a dataset is managed and used.

Information assets should not be a list of systems that an IAO manages, but should focus on the information that needs to be managed within and between systems. This could cover both sensitive personal data and non-personal information that is critical to business. Information Assets could be held in paper, electronic and other formats (for example microfiche or other old technological formats). The information could be in structured information systems or in unstructured environments, such as shared drives.

4 Identifying your Information Assets

4.1 How to identify your information asset

Assessing every individual file, database entry or piece of information is not realistic. Therefore, the council needs to group information into manageable portions.

Information assets need to be defined at a level of granularity that allows its constituent parts to be managed usefully as a single unit i.e. if it's too broad there won't be enough detail, too fine and the council will have thousands of assets.

To assess whether something is an information asset, ask the following questions:

[1] The National Archives Information Asset Factsheet

Value: Does the information have a value to the organisation? How useful is it? Will it cost money to reacquire? Would there be legal, reputational or financial repercussions if you could not produce it on request? Would it adversely impact operational efficiency if you could not access it easily? Would there be consequences of not having it?[2]

Risk: Is there a risk associated with the information? Is there a risk of losing it? A risk that is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?

Retention: Does the group of information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?

4.2 How to group your information

Group according to your business needs and objectives, not your technology. Each asset may contain individual items that need different technology solutions to address the same business need.

If a piece of information could logically belong within two different assets, choose one. This will avoid conflicts of ownership and control. However, assets can reference other assets and you should take care to manage these potentially complex relationships, for example a housing file may also include benefit information such as entitlement or fraud.

Assets can contain other assets – as you introduce more granularity into your grouping, it may be useful to retain the sense of high level assets. The council will develop a clear approach to the management and retention schedules of these assets where they operate at different levels.

The groupings of information within assets may change over time. You may have an asset which contains all the items archived into long term storage, therefore other pieces of information will be added to this asset over time.

5 Information Asset Register/Records of Processing Activities

An Information Asset Register (IAR) has been adapted to incorporate the Records of Processing Activities (ROPA) requirements. It is a mechanism for understanding and managing the council’s assets and the risks to them. It should include links between the information assets, their business requirements or processes and any technical dependencies that there may be. The IAR/ROPA is dynamic and should be consistently updated and improved to ensure the council develops a ‘mature’ understanding of the information that it holds.

[2] A record is a piece of information that has an intrinsic worth which makes it important enough to save and keep secure for its evidential value. In order to decide whether a piece of information is a record or not, its business context must be understood as well as its relevance and significance to the organisation. (MoReq2010)

5.1 What should an IAR /ROPA look like?

It is structured so that it is easy to see what information is affected by changes to your business requirements or your technical environment.

The council will collect the following fields about each information asset:

- Information Asset Owner
- Purpose of Processing (what the data is used for)
- Personal data
- Special categories of data
- The legal basis for processing (where data is personal or special categories of data as defined by the UK GDPR)
- Where the data originated/ source (who provided it)
- Who the data is shared with (both within and outside the organisation)
- Retention period
- PSN data
- Location of the data, whether paper or electronic, including the name of the system/location of database where relevant
- Details of the third party that processes this data on our behalf, where relevant

The council uses the assets identified in the IAR/ROPA to record data flows and system links to ensure that it can be adequately protected and assist the council to better understand its information architecture.

Each asset that is identified in the register must have an owner who is responsible for making sure that the asset is meeting its requirements and that any risks and opportunities are monitored. The owner need not be the creator or even the primary user of the asset, or the system owner of a business system, but they must have a good understanding of what the business needs from the asset and what the asset needs to be to fulfil those requirements.

It is essential that the IAR/ROPA is maintained and updated. The corporate IAR/ROPA will be owned by the Information Governance Team who will ensure that a maintenance schedule is maintained.

6 Information risks to manage

IAOs are responsible for managing risk associated with Information assets. Information assets face the following serious risks:

- Staff, contractors and outsiders may access them inappropriately, or disclose them to others (etc.).
- Inappropriate access to, or disclosure of, confidential information or personal data by staff, contractors and outsiders, whether accidental or deliberate.

- Inappropriate data sharing – too much or irrelevant data is shared internally i.e. a full list with all personal data is provided where only numbers of a specific category have been requested.
- Internal threat – staff acting in error or deliberately, or external parties obtaining information illegally and exposing it/acting maliciously to defraud the council or its residents.
- Information loss – particularly during transfer or movement of information, or as a result of business change.
- Records management – that information assets are not retained for longer than required. They should only be retained for long periods either by law or for business need, as outlined in the corporate retention and disposal schedule.
- Business continuity/disaster recovery – that the relevant personnel are aware of the agreed continuity and recovery for their services.
- Loss of digital continuity – i.e. losing the ability to use council information in the way required, when required. This means that the council should be able to find, open, work with, understand and trust the information. The lifecycle of a piece of information – and how long you need to use and keep it – is often different to the lifecycle of the IT system that is in place to access and use the information.
- Poor quality of information and poor quality assurance, for example, of datasets.
- Poor change management – business needs change, systems change. Information risk management may change and policies and processes must be kept up-to-date accordingly.
- Not maximising the public benefit from information (leading to a waste of public money and poor service delivery).

IAOs and Information Leads should refer to the Information Risk Policy for guidance on identifying and managing information risk.

7. Identifying your IAO

An IAO must have the power to make decisions about how Information Assets are managed. Therefore, this role must be a senior member of staff. It is recommended that this role is assigned to Service Directors.

The post holder must have the skills, resources and authority to discharge the responsibilities and take action on any deficiencies in the relevant processes.

Every year the council asks each director to sign a compliance statement, committing to having robust information management procedures are in place. An important part of this oversight is ensuring that sufficiently senior officers are appropriately trained and responsible for their data.

The compliance statement sets out the requirement for Corporate Directors to appoint IAOs in their Directorates. IAOs will be responsible for identifying Information Leads to help them manage the IAO responsibilities on a day-to-day basis. Corporate Directors can appoint themselves to this role, or devolve responsibility. However, that person must be of sufficient seniority to carry out the role. The Director remains accountable.

All IAOs must attend IAO training arranged by the Information Governance Team. This training is mandatory for all IAOs and must be attended at least every two years.

8. Roles and responsibilities of the Information Asset Owner

The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. The IAO should nominate at least one Information Lead to support them on a day-to-date basis. Roles and responsibilities of the Information Lead can be found in section 9.

The IAO has five core responsibilities. However, it is recognised that Information Leads will help to support the IAO to deliver these (full details of how this can be achieved can be found in Appendix A):

a) Lead and foster a culture that values, protects and uses information for public good.
b) Know what information the asset holds, and what information is transferred in or out of it and what systems it links to.
c) Know who has access and why, and ensure that their use is monitored.
d) Understand and address risks to the asset, provide assurance to the SIRO and ensure that any data loss incidents are reported and managed following corporate guidelines. Security of the network is the responsibility of Digital Services.
e) Ensure the asset is fully used for its intended purpose or for the individual it relates to, including responding to access requests.

IAOs need to be able to answer the following questions:

- Do I understand what information assets I am responsible for (including personal and non-personal data) and has that understanding been properly documented and shared with the SIRO and others that need that information?
- Have I assessed and logged information risks to those assets?
- Do I have a plan for managing risks, and maximising opportunities for using my information assets for the public good?
- Do my teams and third parties understand their roles and responsibilities in managing those risks and opportunities?

9. Roles and responsibilities of Information Leads

An Information Lead (IL) should understand the overall business goals of the organisation and the importance of the information assets in supporting these goals. Information Leads should understand the IAOs five core responsibilities and lead in ensuring the methods outlined in Appendix A are fully exploited to support delivery.

Information Leads will be expected to:

- Review the IAR/ROPA on a six monthly basis and ensure that it is maintained and updated when new assets are created.
- Ensure that retention periods for information are documented in the corporate retention schedule and liaise with the Information Governance Team if changes are required. Arrange for documented audits to ensure that information is deleted in accordance with retention periods.
- Ensure that decisions are clearly recorded against any information that is retained over its agreed retention period. Retention exceptions must have been discussed with the Data Protection Officer and approved by the SIRO.
- Champion the importance of maintaining data quality in business systems.
- Develop Information Architecture within their directorates and ensure that this is in line with corporate guidance and that information is stored in the correct location.
- Ensure that managers understand the importance of maintaining correct access controls of drives and systems to prevent unauthorised access and disclosure.
- Carry out regular audits of systems and drives to ensure correct access controls are maintained.
- Ensure that local information handling guidelines are in place and that these refer to corporate guidance where appropriate.
- Escalate issues of negligence or repeated failure to adhere to corporate policy to the IAO.
- Provide assurance to the IAO on a regular basis.
- Highlight any changes in retention or significant changes to the IAR/ROPA (outside of normal update process) to the Information Governance Team.
- Attend information sharing sessions with the Information Governance Team, IAOs and other Information Leads across the council, and disseminate relevant messages to IAOs.
- Attend mandatory IAO training arranged by the Information Governance Team. This training must be attended at least every two years.

10. Annual Reporting

IAOs will be required to provide annual assurance on the following areas to the Information Governance Team. The Information Governance Team will collate responses into an overarching report to the SIRO and CMB.

- That local procedures governing the use of data are in place and updated when required.
- That access control measures are in place for systems, which includes how access is granted and removed for users.
- That updates on data flows (links to other systems) and reasons are provided.
- That actions following security incidents are monitored and updated.
- That any records management responsibilities are captured (for example, the retention schedule is reviewed annually and that any system(s) used to store information have been reviewed to ensure information is deleted in line with retention. Where systems do not automatically delete information additional checks will be required to ensure any manual process has been carried out.
- That risk assessments of systems are carried out and documented, this should include whether retention and deletion capabilities are automated.
- Contracts with data processers have the agreed corporate clauses and compliance with these are monitored and documented.
- That appropriate Information Sharing Agreements are in place and reviewed where required.
- That actions identified during data audits are captured in the IAR/ROPA where required.

11. Governance, approval and review

11.1 Information Governance Board

This policy and the council's commitment to a robust governance framework are subject to continuous, systematic review and improvement. This council-wide policy will be governed by the Information Governance (IG) Board, chaired by the Corporate Director of Resources, who is also the council's Senior Information Risk Owner (SIRO). The IG Board has a clear terms of reference and reports directly into the Corporate Management Board.

11.2 Formal approval, adoption and review

This policy will be formally signed off by Corporate Management Board. It will be reviewed on an annual basis by the IG Board who will determine who will carry out this review.

11.3 The signatories agree with the content of this document

Name	Role
David Hodgkinson	Director of Corporate Resources and SIRO
Leila Ridley	Head of Information Governance and DPO
Lisa Ford	Information Management Lead

Appendix A – 5 Core IAO Responsibilities

Lead and foster a culture that values, protects and uses information for the public good

What you need to do	How you might do this
- Attend training – when you're appointed and review this as required - Actively contribute to your department's plans to achieve and monitor the right information handling culture - Ensure the handling of your information assets complies with the UK GDPR and Data Protection legislation and the council's compliance policies - Understand and document the business value of the information assets you are responsible for	- Identify Information Leads to support the day-to-day management and ensure they attend training - Attend the quarterly IAO meetings to share ideas - Talk to the Information Governance Team - Make sure that people who use your information assets understand the rules and are aware of the consequences of non-compliance. Use line management responsibilities and appraisal objectives to monitor this - Talk to the SIRO about what you can do to contribute to departmental plans for culture change - Set up a lessons learned log, so if things go wrong you can learn from them and ensure that policies and practices are changed - Talk to Islington Digital Services to ensure appropriate physical, procedural and technical security

Know what information the asset holds, and what information is transferred in or out of it

What you need to do	How you might do this
- Understand and address risks to your information assets, and provide assurance to the SIRO - Know who has access to your information assets and why, and monitor use	- Ensure that your information assets are maintained in the IAR/ROPA, which should include: - What assets are – what they cover, their content, what's sensitive and what personal data you're responsible for

What you need to do	How you might do this
- Understand whether a delivery partner or supplier has a dependency on your information to deliver a service - Ensure that council information is kept secure and data is only transferred in line with the council's removable media policy. - Make sure your information assets are fully used for the 'public good', including responding to access requests. This includes actively considering whether greater access to information assets would assist the public through proactive publication in line with transparency obligations	- The value of your information assets to the business – now and in the future. How important are they, and why? What would be the impact of losing or mishandling them? As part of this process you should consider the benefits of increasing access, or of information re-use - Your usability requirements for those assets – who needs to be able to find them, how do you need to work with them, to maintain the understanding and trust of that information? What retention and disposal schedules do you need? - Keep a record of all staff and contractors with access to records containing personal data – or who handle records containing personal data. For local systems, ensure a process is in place to remove that access as soon as it is no longer required - Manage agreements on the sharing of personal information between organisations where required

Know who has access and why, and ensure their use of the asset is monitored (in conjunction with system owners)

What you need to do	How you might do this
- Agree in writing that relevant access control regimes allow business to be transacted with an acceptable level of risk – or require that an acceptable alternative approach be adopted. You need to agree who has access to your assets - Ensure that you keep a record of individuals with access to, or who handle, records containing personal data - Keep a log of access requests	- Make sure you understand the council's policy on the use of information assets - Put in writing to the SIRO that access provided is the minimum necessary for business purposes – or request an alternative - Ensure that your directorate adhere to the council's IT Security Policies to protect personal data and business critical information

What you need to do	How you might do this

Understand and address risks to the asset, and provide assurance to the SIRO

What you need to do	How you might do this
- Ensure that significant correspondence about information risk handling are placed on the corporate record - Contribute to your directorate's risk register. To do this, you should identify and, where appropriate, formally accept significant risks introduced when personal information is moved between systems or shared with third parties - Make the case where necessary for new investment to protect the asset - Ensure all risk decisions taken are demonstrably in accordance with the council's risk management policies established by the SIRO - Make risk decisions where users believe it is not possible to comply with policies or controls, consulting others as necessary, and ensuring the decision and the reasons behind it, are placed on the corporate record	- Make sure you are aware of the full range of risks - You defined your usability requirements. Use this information to assess risks and opportunities: - Ensure digital continuity is maintained - Identify the technology that your information is dependent on to remain usable. Where are the assets held, and which search tools enable their discovery? - Identify the risks to the information asset that could arise from changes, for example technology change (changing suppliers, systems and so on) and organisational change (e.g. sharing agreements, who has access to the information) - Understand the impact of the council's Risk Policy. This should indicate where loses of confidentiality, integrity and availability are likely to have the most critical impacts on your business, and where the greatest proportion of your mitigation should be focused - Talk to the SIRO or the Information Governance Team about how the risk policy applies to the information assets you are responsible for

Ensure the asset is fully used for the public good, including responding to access requests

What you need to do	How you might do this
- Ensure you are able to use your information assets as appropriate to comply with Access to Information	- Identify the datasets you're responsible for which are disclosable under the Access to Information

What you need to do	How you might do this
Legislations[3] and transparency requirements[4] - Regularly review whether you could make better use of the information assets you are responsible for - Manage and approve agreements on sharing personal information between organisations and ensure access decisions are taken accordingly - Ensure access requests from other public bodies are logged with the Information Governance Team	Legislations. Public data is the objective, factual, non-personal data on which public services run and are assessed, and on which is collected or generated in the course of public service delivery. - Submit potential public data to the Information Governance Team for consideration for proactive publication

[3] Freedom of Information Act 2000, Data Protection Act 2018 and the Environmental Information Regulations 2004

[4] The Local Government Transparency Code 2014