Information Management Strategy

Cyngor Bwrdeistref Sirol
Pen-y-bont ar Ogwr
BRIDGEND
County Borough Council

www.bridgend.gov.uk

Overview

Information Management (IM) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences. The management of the information is subject to legislation and regulations and the Council has a duty to ensure that information is managed, stored and shared according to:

– Freedom of Information Act 2000
– Data Protection Act 2018
- General Data Protection Regulation 2016
– Environmental Information Regulations 2004

Information management encompasses all the information that makes up the Council's corporate memory and knowledge - such as Council Tax data, customer correspondence, financial data, staff newsletters, e-mails and supplier invoices.

This strategy has been developed to support the Council's aim to develop a more robust and consistent approach to improving how we manage our information. The strategy aims to ensure transparency and consistency of the information we handle on behalf of our service users. Its purpose is to ensure that the vast array of records that Council individuals and teams produce, process and manage are organised effectively to improve decision making for the benefit of Council stakeholders: for example, customers, staff, Members, and suppliers.

A key driver for improved IM is to improve the quality, completeness and accessibility of customer records; specifically those required to support customer requests for and information regarding Council services.

Strategic Context

Local authorities have to address their approach to managing their records and information. In addition to external legislative requirements, the Council also has its own business objectives that demand a more innovative and corporate approach to IM.

WASPI

The Wales Accord on the Sharing of Personal Information (WASPI) provides a framework for service-providing organisations directly concerned with the health, education, safety, crime prevention and social wellbeing of people in Wales.

In particular, it concerns those organisations such as local authorities that hold information about individuals and who may consider it appropriate or necessary to share that information with others in a lawful and intelligent way.

The accord has been endorsed by Welsh Government as the single information sharing framework for Wales to which Bridgend has committed.

For more information please go to www.waspi.org.

ICO

The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

From data protection and electronic communications to freedom of information and environmental regulations, the ICO was set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Find out more about our responsibilities and obligations under the legislation covered by the ICO, please go to www.ico.gov.uk.

DPA

The Council needs to collect and use certain types of information about people with whom it deals. These include current, past and prospective employees, suppliers, clients/customers. In addition, it may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments, for example business data.

This personal information is dealt with according to the principles as detailed in the Data Protection Act 2018. Please see the Council's website for our Data Protection Policy and associated statutory obligations in relation to the legislation.

FOI

The Freedom of Information (FOI) Act entitles anybody to ask a public authority in England, Wales and Northern Ireland, including Government Departments, for any recorded information that they keep. This Act gives us all greater access to information about how decisions are taken in government and how public services are developed and delivered.

The FOI Act operates alongside the Data Protection Act, which allows people to access information about themselves (e.g. personnel records, or information held by credit reference agencies) and the Environmental Information Regulations, which give people access to information about the environment.

A number of additional Acts govern the responsibility of the Council with regard to the public disclosure of Council agenda, minutes, reports and customer related data. These include the; Local Government (Access to Information) Act 1985 and Local Government Act 1972.

Information Ownership

The Council needs a consistent approach to the ownership of information repositories in use. Roles of information owner will be identified and clarified across each Service.

The role which these individuals and teams perform will also be consistent from repository to repository as well as across service units.

Any new information ownership governance structure needs to ensure that it is flexible enough to reflect the needs of the service using and processing the information. A key recommendation for the implementation of an overarching IM Strategy is to perform an appraisal of information ownership as the information within repositories is being examined for consolidation or rationalisation. The responsibilities of the owners of information and the processes they adhere to also require corporate definition to ensure consistency.

Data Roles and Responsibilities

All roles will be clearly identified via job descriptions and reference to the job functions referenced in this policy.

Data Protection Role

The Council has a statutory Data Protection Officer with specific responsibility for data protection. The DPO can be contacted directly at foi@bridgend.gov.uk.

SIRO

The Senior Information Risk Owner (SIRO) for Bridgend is the Monitoring Officer,who takes overall ownership of the organisation's Information Risk Policy.

The role acts as champion for information risk. The SIRO must understand how the strategic business goals of the organisation may be impacted by information risks, and how those risks may be managed.

The SIRO implements and leads the Council's Information Governance Board, its risk assessments and management processes within the organisation and advises the Board on the effectiveness of information risk management across the organisation.

Information Asset Owner

The Information Asset Owner for Bridgend is the Group Manager, ICT.

The IAO is a mandated role, and the individual appointed is responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the Council is fully exploited.

Information Sharing Protocol (ISP) Facilitators

The WASPI framework (see previous) recommends that an approved ISP Facilitator be assigned to the development of each new ISP. Their role will be to provide advice and guidance throughout the development process.

All ISP Facilitators have been appropriately trained in the development of ISPs within the WASPI framework and will be able to provide background information regarding WASPI to the partner organisations. Each ISP Facilitator has a good understanding of information sharing related legislation.

ISP Coordinators

An ISP Co-ordinator needs to be identified for the development of each new ISP. This person will undertake initial research as to whether an ISP is required, and if so, then manage the development process by initially identifying the partner agencies involved and arranging the meetings.

Only one ISP Co-ordinator is generally required for each development however, where a large number of organisations are involved in the sharing of information, it may be that more than one person assists with the work.

The WASPI Support Team can be contacted via the website. www.waspi.org.

System Owners & Administrators:

The Systems Team within the ICT Service Unit provides customer support for all computer software and systems. Each system has a dedicated System Owner, their role is to develop and maintain the software on behalf of the service unit. The service unit using the software also has an Administrator role who acts as a representative on behalf of the service.

They are responsible for the role of Information Asset Owners and must actively manage and monitor the whole of the information lifecycle from the creation of documents through to deletion.

Heads of Service and Group Managers are responsible for ensuring that their staff are compliant with all policies and procedures relating to the management of information throughout its lifecycle and are aware of their responsibilities as set out in these policies.

Periodic Reviews and Continual Compliance

The storage, retention and disposal of information are subject to periodic reviews in addition to regular audit exercises and risk assessments to ensure compliance and secure information management.

It is recommended that staff carry out their own periodic risk assessments and reviews of procedures at service level. Internal Audit will support services with on-going continual compliance.

Audit trails should contain sufficient information to demonstrate all necessary historical activities relating to the system and the stored data.

Audit trails will need to evidence the authenticity of the capture and storage of information including any changes to it.

For further information please contact the Data Protection Officer or the Chief Internal Auditor.

Codes of Practice and Policies

The Codes of Practice are intended to be used in conjunction with current legislation, including the Data Protection Act, Freedom of Information as well as secondary legislation (such as Regulations) and guidance published by the Information Commissioner's Office. It is the responsibility of staff involved in information management and sharing to familiarise themselves with these sources and to seek advice from Legal when necessary.

All of the listed Policies and Codes of Practice are available on the intranet and at the following link: http://www.bridgenders.net/legal/Pages/Data%20Protection%20Introduction.aspx

Data Protection

The Data Protection Policy can be found on the intranet.

The Data Protection Act 2018 makes provision for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information.

Data Breaches

This Code of Practice has been developed to assist the Council in responding effectively to data breaches. The Council holds substantial amounts of personal and special category data (sensitive) and care must be taken to avoid a data breach.

Document Retention and Disposal

The Council's Data Retention Policy can be found on the intranet.

This Policy is based on the Retention Guidelines for Local Authorities produced by the Local Government Group of The Records Management Society of Great Britain. The destruction guidelines for paper copies are based on the Local Government Classification Scheme.

Retention and disposal schedules are listed for each document type and format depending on the content.

Disclosure of Special Categories of Personal Data – Elected Members

The purpose of this Policy is to outline the acceptable disclosure and use of special categories of personal data by all Councillors within the County Borough. Under data protection legislation the Council must consider a number of aspects when deciding whether to disclose special categories of personal data (sensitive data) to Councillors. Thsee will be identified in this policy.