Bolton
Council

Information Governance Framework

Author (name):	Helen Gorman
Author (designation):	Borough Solicitor
Email address for automated reminders:	informationgovernance@bolton.gov.uk
UK GDPR/DPA check completed (name and date)	Patricia Ashcroft July 2022
Approved by:	Executive cabinet member corporate resources
Date approved:	
Date uploaded to intranet:	
Review Date	
Key words	Information Governance; Data Protection: GDPR;

Version control

Version	Author of Changes	Date	Summary of changes made	Approved by (meeting / committee)
1	Andrew Roberts	Nov 2018	New overarching framework bringing together Information Governance related policies	Executive cabinet member corporate resources
2	P. Ashcroft	July 2022	Updated to reflect current practices	

1. Introduction

Information governance, or IG, is the overall strategy for information at an organisation. Information governance balances the risk that information presents with the value that information provides. Information governance helps with legal compliance, operational transparency, and reducing expenditure associated with legal discovery. The policies and procedures that sit under this framework guide how employees handle information. Information governance encompasses more than traditional records management. It incorporates information security and protection, compliance, data governance, electronic discovery, risk management, privacy, data storage and archiving, knowledge management, business operations and management, audit, analytics, IT management, enterprise architecture, business intelligence, big data, data science, and finance.
The fundamental principles are contained in the following: -

- Privacy Law – UK GDPR and the Data Protection Act 2018
- Common Law – the duty of confidentiality
- Human Rights Act 1998

Some information which the Council holds can be described as public and is freely available for publication e.g. food safety inspection ratings whilst some information is non-public e.g. personal identifiable data such as social care information which identifies an individual.

It is essential that the council has a robust information governance management framework, to ensure that information is effectively managed with accountability, structures, governance processes, documented policies and procedures, staff training and adequate resources. This is now more important than ever since the introduction of the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 which provide the public with enhanced rights over their personal data.
Under Article 5 (2) of the UK GDPR the council must be able to demonstrate compliance with the Regulation and this is known as the “accountability principle”.
Taking responsibility for what we do with personal data and demonstrating the steps we have taken to protect people’s rights not only results in better legal compliance but it also shows how we respect people’s privacy. This can help to develop and sustain people’s trust.
Furthermore, if something does go wrong, then being able to show that we actively considered the risks and put in place measures and safeguards can help provide mitigation against any potential enforcement action**.**

We are increasingly encouraged to provide efficient, effective services by working more closely with our own organisational and external partners. By joining up our information resources, we can deliver a better service to the public. Often, this involves sharing personal information about individuals. The Data Protection Act 2018 and the UK GDPR and Information Commissioner’s Office Code regarding data sharing exist to regulate the processing of personal data including the obtaining, holding and disclosure of such data and by adhering to their principles we can ensure that we can share personal information, without compromising the rights of individuals.

Purpose

This Information Governance Framework document provides an overview of the processes, and controls we have in place. Staff need to understand the roles and responsibilities to ensure we are performing to the right standards, spend public money responsibly, and that we continue to keep the public, the data we collect, and our staff safe and secure.

2. Each employee and their role

Senior Information Risk Owner (SIRO) and DSIRO (Deputy Senior Information Risk Owners)

The Senior Information Risk Owner (SIRO) has overall responsibility at a strategic level for managing information risk in the council and chairs the Information Governance Steering Group (IGSG). The membership of the Group and the terms of reference for the IGSG are available on the intranet

The SIRO has overall responsibility for:-

- Information risk and incident management framework within the council
- Information risk policy
- Annual information risk review
- Providing a focal point for communicating information risk policy and issues
- Following up with identified information risks
- Fostering and leading an appropriate information security culture
- Ensuring incident reporting process is in place, and process for Serious Incidents requiring investigations (SIRI)
- Ensuring there are Data Protection Impact Assessments (DPIAs) for new projects
- Advising the Chief Executive and the CLT about information risk
- Providing guidance to Information Asset Owners
- Identifying Information Asset Owners for all assets, and ensuring they understand their responsibilities
- Oversight of and prioritisation of Information Governance activities

Each directorate has a Deputy SIRO (DSIRO) who can deputise for the SIRO in respect of any of the above responsibilities but who also has the following specific tasks:-

- Attend the Information Steering Group
- Sign off on DPIAs
- Sign off on actions arising from serious data breaches
- Provide a lead within their directorate for IG issues such as recurring data breaches and training requirements

The current SIRO is Helen Gorman who is the Borough Solicitor.

DSIROs are:

- Place: Jon Dyson
- Chief Executive’s: Phil Rimmer
- Children Services: Paul Rankin
- Adult Services: Karen Kenyon
- Public Health: Lynn Donkin

Caldicott Guardian

The Caldicott Guardian is responsible for ensuring that all personal/patient identifiable information handled by social care services and public health respectively, are compliant

with existing law and standards and they act to safeguard the rights of service users. The Caldicott Guardian ensures that satisfactory information governance policies are in place for their service and adhered to by all staff and providers in their service area.
The current Caldicott Guardians are Karen Kenyon, Lynn Donkin and Paul Rankin.

Information Asset Owners

Each directorate will have Information Asset Owners who are accountable for information assets within their business unit. Information assets in this context will include physical and electronic data such as employee and customer records etc. They are able to understand how information is held, used and shared, and address risks to the information.

Information Asset Administrators

The role of the Information Asset Administrator is to provide support and assistance to the Information Asset Owner in undertaking their information management tasks.

Data Protection Officer

The Data Protection Officer is a statutory role required for all public authorities by the UK GDPR. It is a legal requirement for the council to appoint a Data Protection Officer (DPO). The DPO monitors internal compliance, informs and advises on the council’s data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority. The DPO also ensures compliance with Article 30 of the UK GDPR which requires that a Record of Processing Activity (ROPA) is maintained which covers processing purposes, data sharing and retention.

The Data Protection Officer is Patricia Ashcroft

All staff and Members, contractors and partner organisations

All staff are responsible for handling information in a safe and secure manner. They must follow the Council's information security policies and any specific security procedures for their area.

They must report any potential security breach using our breach reporting procedure.

3. Policies

The key policies and procedures in the framework are:

- Data Protection
- Freedom of Information
- Information Security
- Data Sharing
- Records Management (Retention, and disposal of records)
- What to do in the event of a data breach

Data Protection

The UK GDPR and Data Protection Act 2018 (DPA 2018) regulates how an organisation can use (process) personal information about individuals. The council has produced a policy to ensure it meets the requirements of the Act and has clear procedures and arrangements in place to manage compliance across all areas.

The council is registered as a ‘Data Controller’ with the Information Commissioners Office (ICO). A data controller must ensure that any processing of personal data for which they are responsible complies with the above legislation. Failure to do so risks enforcement action, prosecution, and compensation claims from individuals.

The council has published a Corporate Privacy Notice together with service specific privacy notices. These explain the rights that citizens have over their personal data.

The notices include the rights that people have to amend and erase personal data as well as how long it will be stored for.

The council also has a statutory duty to undertake Data Protection Impact Assessments (DPIA) where there is a significant risk to personal data being compromised. Details of how and when to use a DPIA can be found here.

Freedom of Information (FOI)

An FOI policy and publication scheme has been established to ensure that the council meets its legal obligations under the Freedom of Information (FOI) Act. It outlines the approach to responding to requests for information made under the FOI Act. The council is committed to openness and transparency about the way in which it operates.

The FOI policy aims to ensure access to information in order to promote greater openness, transparency in decision making and to build public trust. Access to information about decisions the council take can help local people to influence local service provision.

The Freedom of Information Act gives any member of the public the right of access to information held by the council about how it runs the business. It does not include access to personal information (information that identifies a living individual) which is dealt with under the UK GDPR. Nor does it include access to environmental information (see below).

The council has clear procedures and arrangements for handling queries from members of the public.

Individual Rights

Under UK GDPR individuals have the following rights:

- The right to be informed
- The right of access to their personal information
- The right to rectification
- The right to request erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

The right of access to personal information (known as a Subject Access Request or SAR) is the most frequently used.:

Where a Subject Access request is made officers should liaise with the Information Governance team as soon as possible upon receipt of the request: SubjectAccess@bolton.gov.uk

Information Security

Information security is the practice of protecting information from unauthorised access and disclosure. The council has effective safeguards in place to make sure that personal and other information is kept securely and does not fall into the wrong hands. The council has clear procedures and arrangements in place to ensure that technical and non-technical controls are in place to safeguard and protect information the Council processes.

The council will maintain and protect all information assets both owned or used by the council to a high standard of confidentiality, integrity and availability. The council will ensure that information assets and hardware are disposed of securely in line with industry standards.

Important information assets will include paper records stored on or off site, computers, mobile phones, emails, data files, software, recorded information e.g. CCTV, voice recordings.

The council will maintain an Information Asset Register to track, manage and dispose of these assets in line with legislative requirements and council policy and will provide support and training to all Council Information Asset Owners.
The council will ensure that any security incidents that occur are managed in line with current procedures for an Information Security Breach. It is the duty of all staff and other parties accessing or processing council data to immediately report any actual or suspected breaches in information security in line with council procedure.
Relevant policies include:

- Information Security Policy
- Acceptable use of ICT policy
- Disposal of confidential waste policy

Records Management (retention, and disposal of records)

Bolton Council's records are a major component of its corporate memory and as such are a vital asset that support ongoing operations and provide valuable evidence of business activities over time.

The council recognises that the efficient management of its records is necessary to:

- Support its core functions.
- Comply with its legal and regulatory obligations.
- Contribute to the effective overall management of the council.
- Ensure services are responsive to all customers by enabling access to records to meet relevant legislation and provide assurance that records are being kept securely.

The council has a retention schedule which describes the length of time that certain records should be kept for and the date when they can be destroyed (If appropriate).

For further information and technical advice please contact the Information Governance team: informationgovernance@bolton.gov.uk

4.0 What to do in the event of a data breach?

A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A breach is more than just about losing personal data. It includes:

- Access by unauthorised third party
- Deliberate or accidental action / inaction by the council or its contractor
- Alteration of personal data without permission (integrity breach)
- Loss of availability of personal data (availability breach)

All staff are responsible for **immediately** on becoming aware of an incident alerting a senior manager in their service of a data breach. This should take place by phone or face to face. If no manager is available immediately contact information.security@bolton.gov.uk The senior manager must establish:

- What has happened,
- When it happened (date and time)
- How and why it has happened,
- How it came to light
- Details of the people affected.
- Who was involved

If there is a likelihood of a risk to people's rights and freedoms the breach must be notified to the ICO **within 72 hours of becoming aware of the breach**. The responsibility for reporting the breach to the Information Commissioners Office (ICO) within 72 hours (and data subjects if appropriate) will lie with the Data Protection Officer or the Head of Information Governance.

Any individuals whose personal information has been lost or released where there is a high risk to the individuals must be notified ASAP. The responsibility for notifying rests with the relevant senior manager in consultation with the Information Asset Owner. Further guidance can be found on the intranet in a document titled: **Data Breach Management Procedure**

If the initial risk assessment of the breach indicates that an incident is a very significant risk it can be escalated to an Information Security Incident Panel. The Panel will be comprised of the DPO, the Head of Information Governance, the SIRO, the DSIRO for the service, and whoever these core members consider appropriate, but could include representatives from e.g. CICT, HR, Customer Services or the Press Office.

5.0 Training

All staff and Members must undergo basic training in respect of data protection. More in-depth training will be provided to those officers who handle sensitive data or large volumes of data. All staff and members must comply with the council's ICT Acceptable Use Policy and the Codes of Conduct.