IPSWICH
BOROUGH COUNCIL

Information Governance Framework 2021

Document Control

Organisation	Ipswich Borough Council
Title	Information Governance Framework
Author	Senior Information Governance Officer
Filename	
Owner	Information Governance Team
Subject	Standards and best practice for handling information.
Protective Marking	Not protectively marked
Review Date	November 2022

Revision History

Revision Date	Version Number	Reason for change	Author
25/10/18	0.1	First Draft	Carolyn Aldridge
12/11/18	0.2	Revisions following comments from Democratic Services Manager	Carolyn Aldridge
16/11/18	0.3	Revisions following comments from DPO & ICT Ops Manager	Carolyn Aldridge
25/04/2019	0.4	Revisions following comments from Head of People and Governance	Carolyn Aldridge
16/08/2019	0.5	Revisions following comments from Ops Mgr	Carolyn Aldridge
01/10/2019	1.0	Approved by Executive	Carolyn Aldridge
12/11/2021	1.1	Review	Alice Prince
22/12/2021	2.0	Revisions Approved by Deputy Chief Executive	Alice Prince

Document Approvals

Name	Date
Executive	01/10/2019
Deputy Chief Executive	22/12/2021

Document Distribution

Name

Contents

1. Introduction

1.1. The Information Governance framework sets out the way Ipswich Borough Council (the Council) handles information, in particular, the personal and special category (sensitive) data relating to our customers and employees. The framework determines how we collect and store data and specifies how the data is used and when it can be shared.

1.2. It is of paramount importance that information is efficiently managed and that appropriate accountability, standards, policies and procedures provide a robust governance framework for effective information management.

2. Purpose/Aims/Objectives

2.1. The purpose of this document is to outline an information governance framework (the Framework) that ensures the Council: -

- Meets its legal obligations for the effective management of information,
- Recognises the key enabling role of information in supporting the achievement of Council objectives,
- Ensures that information is treated as a valuable asset.

2.2. The Framework demonstrates the Council's commitment to having in place sound information governance arrangements, gives clear direction to managers and employees, and will ensure that legal requirements and best practice standards are met.

3. Scope

3.1. This Framework applies to all types of information and data, both electronic and manual, which is held, processed or transmitted by the Council.

3.2. The Framework applies to all employees, Councillors and others working on behalf of the Council e.g. partners, contractors, consultants, organisations acting as a data processor on behalf of the Council and any other agents of the Council who have access to information held by or on behalf of the Council. Non-compliance with this Framework and associated policies could potentially expose the Council and/or its customers to unacceptable risk.

4. Legal and Regulatory Framework

4.1. There are a number of legal obligations placed upon the Council for the use and security of personally identifiable information. There are requirements to disclose information appropriately when required.

4.2. To manage its obligations, the Council will issue and support policies and procedures ensuring information is held, obtained, recorded, used and shared correctly.

4.3. **Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR)**

Data Protection legislation aims to protect personal information about a living, identifiable person and applies to data in paper and electronic format.

We have a statutory duty to comply with the requirements of both the 2018 Act and the UK GDPR as we collect data about customers when conducting our business. The Council is also required to produce a privacy notice explaining how information is collected, processed and potentially shared. The Council publishes its privacy notice at www.ipswich.gov.uk/privacy.

4.4. **Freedom of Information Act 2000**

The Freedom of Information Act 2000 came into force on 1 January 2005 and provides the public with a general right of access to official information held by this Council. All requests must be in writing and we aim to supply the information within 20 working days, unless there is an exemption or a fee to pay.

The email address for freedom of information requests is:

foi@ipswich.gov.uk

4.5. **Environmental Information Regulations 2004**

The Environmental Information Regulations 2004 (EIR) came into force on 1 January 2005 and apply to environmental information held by public authorities.

The EIR provides public access to environmental information held by public authorities.

The Regulations do this in two ways:

- public authorities must make environmental information available proactively;
- members of the public are entitled to request environmental information from public authorities.

EIR requests fall under six main areas:

- The state of the elements of the environment, such as air, water, soil, land and fauna (including people).
- Emissions and discharges (gases and fluids), noise, energy, radiation, waste and other such substances.

- Measures and activities such as policies, plans, and agreements affecting or likely to affect the state of the elements of the environment.
- Reports, cost-benefit and economic analyses.
- The state of human health and safety and contamination of the food chain.
- Cultural sites and built structures (as they may be affected by environmental factors).

All environmental information requests should be directed to:

foi@ipswich.gov.uk

4.6. **Local Government Transparency Code**

We are committed to being open and transparent about how we work, our decision-making processes and the services we provide. Central Government introduced the code to establish a clear framework of information that local councils should publish.

We will publish data at regular intervals, either quarterly or annually in line with the mandatory requirements of the code.

4.7. **Surveillance (including RIPA) and Closed Circuit Television (CCTV)**

The Regulation of Investigatory Powers Act 2000 (RIPA) is legislation governing the use of covert techniques by public authorities. If we need to use covert (secret) techniques to obtain private information about someone, we do it in a way that is necessary, proportionate, lawful and compatible with the Human Rights Act 1998.

We will only use RIPA for cases that involve crime. It applies to a wide range of investigations in which private information might be obtained. We are required to obtain an approval from a magistrate before starting a surveillance investigation.

There are cases where overt (open) surveillance may be needed; this will go through a strict process of authorisation and proportionality.

CCTV was introduced into Ipswich town centre in 1994. Cameras are monitored from a control room known as the Emergency Services Centre (ESC), which is based in the Council's headquarters, Grafton House.

The Audit Partnership Manager is the Council's Senior Responsible Officer whose role is to ensure the proper administration and adoption of RIPA.

All employees in the ESC are Security Industry Association accredited and the Council adheres to the Information Commissioner's Office CCTV Code of Practice and the new Home Office Surveillance Camera Code of Practice which ensures that the system is operated both effectively and legally, adhering to all current legislation including the Data Protection Act and Human Rights Act.

5. Key Policies

5.1. **Data Protection Policy**

Our Data Protection Policy sets out how the Council will manage the lawful and fair handling of personal data in line with the current data protection legislation and ensure

that all personal data processed by or for the Authority is subject to appropriate safeguards to ensure compliance with the Data Protection Act 2018 and the UK GDPR.

5.2. **Freedom of Information Policy**

This policy aims to set out the obligations of the Council to comply with the Freedom of Information Act (FOIA) 2000.

5.3. **Records Management**

Records Management is governed by a number of laws and regulations, several of which concern Data Protection and Freedom of Information.

Records management is the practice of maintaining records safely from the time they are created for council business activities, during retention and up to their eventual disposal. This includes classification, storage, security, destruction and, in some cases, archival preservation of records. A record can be on paper, digital or a physical object.

In line with good records management practice we have completed an information audit and established an Information Asset Register.

5.4. **Information Security Policies**

Information Security is delivered by both technical solutions and organisation policies. This includes Firewalls, Antivirus Protection, Intruder Detection Systems, User Passwords and Access Control. In addition, employees accessing data are required to adhere to Information Security Policies including:

- Corporate Information Security Policy
- Email Usage Policy
- Password Policy
- Internet and Telephone Usage Policy
- Protective Marking Policy

6. Roles and Responsibilities

6.1. **Corporate Management Team (CMT)** – Comprising of the Chief Executive, Deputy Chief Executive, Directors and Assistant Directors, CMT have overall responsibility for Information Governance arrangements within the Council.

6.2. **Senior Information Risk Owner (SIRO) -** The Audit Partnership Manager is the Council's Senior Information Risk Officer (SIRO) and has responsibility for managing information risk, and ensuring policies and processes are in place for the safe management of information.

6.3. **Monitoring Officer –** The Council's Monitoring Officer has responsibility for:

- considering requests to review any decisions where IBC have relied upon an exemption under the FOIA or EIR.
- determining whether exemption 36 (exemption from disclosure of information which might prevent the free and frank provision of advice or exchange of views, or which would otherwise prejudice the effective conduct of public affairs) can be relied upon.
- as statutory proper officer in relation to the access to information rules, for determining whether reports or parts of reports intended to be considered at a formal member level meeting should be marked "Not for Publication" on the basis that it is likely that the public will be excluded from the meeting when the report is considered because it contains exempt information. He/she is also responsible for ensuring that notices and papers are publicised as required under the rules.
- advising on any disputes as to a Councillor's entitlement to information.

6.4. **Data Protection Officer (DPO) –** In accordance with data protection legislation the Council has appointed a DPO whose responsibilities include monitoring internal compliance, providing advice on our data protection obligations, advising on Data Protection Impact Assessments (DPIAs) and acting as a contact point for data subjects and the supervisory authority.

6.5. **Information Management Group (IMG) –** The IMG consists of representatives from each of the service areas. The group meets at least 4 times a year to develop and co-ordinate information governance arrangements across the council and report to CMT on any issues that require their attention. The IMG is chaired by the SIRO and supported by the Information Governance Team.

The Terms of Reference for the IMG are attached as Appendix A.

6.6. **Information Governance Team** - The Information Governance team provides guidance to the Council and individuals to promote awareness and ensure personal information is processed legally, securely, efficiently and effectively.

6.7. **Information Asset Owners (IAOs) -** IAOs carry out Data Privacy Impact Assessments, put in place Information Sharing Protocols, determine access to the information asset, check that all those accessing the asset have received the right training, manage the information in accordance with the records management policy and maintain the Information Asset Registers for their service area.

6.8. **Information Champions** – Each service area has one or more information champion, who are responsible for collating responses to information requests

6.9. **All Employees -** All employees, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

Employees Training and Awareness

7.1. All employees and Councillors must complete appropriate Data Protection training and receive regular refresher training.

7.2. Employees are aware that as the data controller, the Council will be responsible and accountable for how data is handled and transmitted. If the Council's processes and relevant law are not followed, any misuse or loss of data may leave an individual open to potential disciplinary action.

8. Incident Reporting

8.1. All incidents of a breach in the data protection regulations must be reported to the Data Protection Officer (DPO). The reporting form is available on the Council's Intranet in the "Help & How To > Information Governance & Data Protection" section.

As much information as possible should be provided and reported within 24 hours of the incident being identified. Reports of data protection incidents should be emailed to dataprotection@ipswich.gov.uk.

8.2. An information security incident includes, but is not restricted to the following:

- The loss or theft of data or information;
- The transfer of data or information to those who are not entitled to receive that information;
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system;
- Changes to information or data or system hardware, firmware or software characteristics without the Council's knowledge,
- The unauthorised use of a system for the processing or storage of data by any person

8.3. The DPO will decide whether an internal investigation is required and appoint an investigating officer if necessary. The DPO will also decide whether the incident needs to be reported to the Information Commissioner.

8.4. All Data Security incidents will be reported to the relevant CMT member and a report taken to the Corporate Management Team (CMT) on a monthly basis.

9. Review

9.1. This policy document will be updated and/or amended as necessary to reflect changes in legislation and best practice.

10. Appendix A

Information Management Group (IMG) – Terms of Reference

Purpose:

- To develop and co-ordinate excellent information governance arrangements across the Council.
- To take direction from CMT.
- To report to CMT, the Data Protection Officer (DPO) and SIRO (Senior Information Risk Owner) any issues that require their attention.

Membership:

- The group will comprise of at least one representative from each Service area who has a key role in access to information and information governance.
- Directors / Assistant Directors will identify who should be a member of the group.
- In the event that that individual cannot attend a meeting, an alternative representative should attend on their behalf.

Key Aims & Objectives

- To monitor and appraise the information and data needs of the Council and ensure that the Council delivers quality customer interaction and delivers services efficiently.
- To facilitate information audits within each service area and review them on a regular basis.
- To provide assistance to the Information Asset Owners, (IAO) in carrying out their duties.
- To monitor and appraise the outstanding FOI/DP cases. To identify any outstanding actions, liaise and co-ordinate with the relevant service areas to ensure that the requests are completed within the relevant timescales. If necessary escalating the requests to the IAO.
- To promote and raise awareness of retention and disposal policies and procedures for all documents and records.
- To ensure that information and data is treated as a corporate asset, shared by all. Develop any relevant policies and procedures to be presented to CMT for approval, ensuring that IBC is complying with relevant legislation.
- To promote Information Management as a key corporate activity, essential to the provision of excellent customer interaction and efficiently delivered, high quality services.

Frequency of Meetings

- The group will meet 4 times a year, or as frequently as necessary, to discuss different issues, processes, procedures and exchange information in relation to Information Management.
- Any recommendations will be forwarded to CMT.

Administration

The Information Governance team will provide administrative support by scheduling meetings, circulating the agenda, and producing minutes after each meeting.