Information Governance – Quick reference guide for Elected Members

Information governance (IG) is a term used to describe how information is used. It covers system and process management, records management, data quality, data protection and the controls needed.

- Applies to information in all formats including paper and electronic.
- Covers Records Management, creation, storage, use, archiving and deletion of data.
- Creates a framework of policies, procedures, processes, and controls.

Information Governance sits under several Acts and Regulations.

Data Protection

Data protection legislation sets out good information handling principles that Members must follow. There are two main pieces of legislation that you should familiarise yourself with:

- UK General Data Protection Regulation (UKGDPR)
- Data Protection Act 2018 (DPA 2018)

The legislation replaced the Data Protection Act 1998 and was designed to enhance the right of people whose data is held (known as **data subjects**). Its aim was to give them more control over what happens with their data and for better transparency/awareness thus ensuring people can trust you to use their data fairly and responsibly.

Principles of Data Protection

All personal data must be

A) Used in a lawful, fair, and transparent manner
B) Collected for specified purposes
C) Adequate, relevant, and only what is necessary
D) Kept up to date
E) Kept no longer than is necessary
F) Kept secure to maintain confidentiality and integrity

You must be able to demonstrate compliance with these principles. Further information on the principles can be found in the **Information Governance: A guide for Elected Members.**

Responsibilities

A **Data Controller** is an individual or organisation that determines the purpose for which personal data is collected and used. The Controller is ultimately accountable for the personal data.

When you collect, use, and store personal data when undertaking casework, you are the **Data Controller.** You are accountable for the data you process and must ensure that it is used in the right way.

When you collect, use and store personal data when undertaking official Council duties such as attending a Committee, the Council is the **Data Controller** and is accountable. To ensure compliance with our data protection obligations, you must follow the Council's policies and procedures when acting in this role.

Councillor Privacy Notice

The Council has produced an Elected Members Privacy Notice, which Members can use to advise their constituents about the Members processing of constituents' personal data. This can be found online via: Members Privacy Notice

Members should signpost constituents and any third parties to the Councillor Privacy Notice whenever you collect personal data for casework, for example, by using the email footer found in the **Information Governance: A guide for Elected Members.**

Data Security and Complaints

The Information Commissioner is the regulatory body in the UK. Examples of data loss incidents would include loss of paper/cards which contain personal/confidential information of third-party individuals, including citizens, businesses, or employees, this also includes commercially sensitive information (including contracts).

Sometimes a loss of data may occur because this information is accidentally disclosed to unauthorized persons. This would include emails sent to incorrect recipients externally and internally or to generic mailboxes, or faxes sent to the incorrect number or lost due to a fire or flood or stolen as result of a targeted attack or the theft of a mobile computer device.

If you become aware of any incidents, you should seek advice in the first instance from Democratic Services.

Access to Information

Several pieces of legislation provide individuals with the right to request access to information. Each provision sets out a framework to provide access to information, including timescales, so it is essential that requests are recognised, recorded, and responded to promptly and correctly.

UK General Data Protection Regulation and Data Protection Act 2018 regulates the processing of personal information and gives individuals rights over their own personal information, including having access to a copy of the information. You have **one calendar month** to respond to these requests.

The Environmental Information Regulations 2004 which provides access to environmental information held by (or on behalf of) public authorities. You have **20 working days** to respond to these requests.

The Freedom of Information Act 2000 which provides access to most other recorded information held by (or on behalf of) public authorities. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. You have **20 working days** to respond to these requests.

All information that relates to the Council's official business will be open to disclosure under FOIA and EIR, whether it is held on the Council's corporate IT systems/equipment or on Members' personal devices and Apps.

However, information held by Councillors *for their own purposes* will not be covered by FOIA or EIR and Councillors are under no obligation to disclose it to the public.

Information requests can be received by letter, email or verbally**.** If you receive a request for information, you must act on it promptly. Further information can be found in the **Information Governance: A guide for Elected Members.**

Training

Being aware of the various laws and regulation surrounding information handling is key to enabling you to comply with your obligations as Data Controllers. The Council have the following mandatory training available via Cardiff Academy which can be accessed here:

Cyber Ninjas – This course is specially designed for our elected members, and it's split into short modules. Each features a training video, followed by a quiz - and you'll need to answer correctly 2 out of 3 questions.

By the end of this course, you will:

- Understand the impacts of new data protection laws and how they directly affect you.
- Be confident with your cyber security and be armed with some simple but effective ways to keep hackers at bay.
- Be the one leading our efforts to prevent further cyber-attacks and data breaches

Cardiff Council Webinar – This module provides an overview of the requirements of the Councils Information Governance and ICT Security policies.

Things to Remember

Register- Members are individually responsible for personal data they manage in their role of ward representative and the Information Commissioners Office requires Councilor's to register as separate Data Controllers. Check your registration here

Be Aware – Familiarise yourself with the Information Governance Members Guide, E-Learning modules and Council Policies and processes.

Keep people informed - The Council has produced an Elected Members Privacy Notice which you can use to advise your constituents about the processing of constituents' personal data. This can be found here.

Uphold Individual Rights – Be aware and transparent in the use of personal data. Individuals have numerous rights under UK GDPR.

Report- Any security concerns should be reported immediately to Democratic Services who can seek advice and guidance from the Information Governance team.

Respond – Familiarise yourself with Access to information legislation and know how to respond. Further information on the deadlines can be found in the **Information Governance Members Guide.**