INFORMATION GOVERNANCE:

A Guide for Elected Members

April 2022

Supporting New Members.

CARDIFF
CAERDYDD

Contents

ABOUT THIS GUIDANCE

It serves as a useful reference to support Members in complying with the requirements of data protection and access to information legislation by providing practical advice, information and guidance on the collection, use and storage of personal data. The following terms appear regularly throughout this document. Their definitions are below:

• **Official Council duties**: The work undertaken by a Member when representing the Council, for example attending or chairing a committee.

• **Casework**: The work undertaken by a Member when representing a constituent. This may include a direct query, complaint, service request, community issue, etc. (as described in the Local Government Association – Handling Casework Councillor Workbook).

• **Data protection legislation**: Refers to current data protection legislation within the UK.

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

• **Processing**: In relation to personal data, this can be any activity involving (but not limited to) the collection, use, storage, sharing, and disposal, etc. of the personal data.

• **Personal Data"** shall take the meaning given in the Data Protection Legislation

• **FOI**: Freedom of Information Act 2000

• **EIR**: Environmental Information Regulations 2004

DATA PROTECTION PRINCIPLES

Data protection legislation sets out good information handling principles that Members must follow. The key principles are summarised below with further information on how to comply with these set out within this guidance.

1 **Keep people informed**	**You must be open, honest and transparent with people about the way you use their personal data and provide them with appropriate privacy information.**

2. Specific Purpose	**You must collect and use personal data for a specified purpose and stick to that purpose.**

3. Minimisation	**You must only collect the personal data that it necessary in relation to the purpose.**

4. Accuracy	**You must take reasonable steps to ensure that personal data is correct and kept up-to date where required**

5. Retention	**You must not keep personal data for is longer than is needed in relation to the purpose.**

6. Data Security	**You must ensure that personal data is kept safe and secure**

7. Information Rights	**People have rights over their own personal information. You must ensure that people whose information you are processing are made aware of their information rights and are able to exercise them.**

HOW DATA PROTECTION APPLIES TO MEMBERS'

Elected Members typically have three key roles:

1) They will act as a member of the Council, for example, as a Cabinet Member or a member of a Committee.

2) They will represent the residents of their ward, for example, when undertaking casework.

3) They will represent a political party, particularly at election time.

Members will process personal data for different purposes depending on which of the above roles they are undertaking.

Who is accountable for the personal data when undertaking these roles?

Official Council duties

When a Member collects, uses and stores personal data when undertaking official Council duties such as attending a Committee, the Council is the Data Controller and is accountable for ensuring that the data processed by the Member is used in the right way. The Council may do this by providing Members with training, awareness, policies, procedures, and guidance so that they know how to handle personal data properly and lawfully.

To ensure compliance with our data protection obligations, you must follow the Council's policies and procedures when acting in this role.

Undertaking Casework

When a Member collects, uses and stores personal data when undertaking casework, the Member is the Data Controller.

The Member is accountable for the data it processes and must ensure that it is used in the right way.

Representing a Political Party

When representing a political party, for example when campaigning at election time, the political party is the Data Controller and is accountable for ensuring that the data processed by the Member is used in the right way. The Political Party may do this by providing its members with appropriate training, awareness, policies, procedures and guidance

MEMBER NOTIFICATION

The Data Protection Act requires Data Controllers to notify or register with the Information Commissioners Office (ICO). A Data Controller is the person or organisation that determines the manner in which personal data is processed, such as what is collected, what is done with it, how it is stored and when it is deleted or disposed of.

The Council registers with the ICO as an organisation and work done by Members in their role as a Member of the Council is covered by that registration. Members are individually responsible for personal data they manage in their role of ward representative and the ICO requires councillors to register as separate Data Controllers.

This is a completely separate notification to any Council wide or political party notification. Whilst many authorities require Members to undertake their own individual registrations with the ICO, Cardiff Council undertakes a Members' annual notification to the ICO on their behalf.

KEEPING PEOPLE INFORMED

Data Protection law requires that you are open and honest with people about the use of their personal data. This is especially important in situations where the individual has a clear choice about whether they wish to enter into a relationship with you (for example, where a constituent is considering asking you to represent them on a particular matter) or the use of their data may be unexpected.

When you collect personal data from an individual, it's important that you provide them with an explanation as to how their data will be used and for what purpose. By providing this information, individuals will know from the outset how their personal data will be used and the likely implications for them. This is likely to prevent complaints or concerns being received from individuals about the way you are using their personal data.

What information must I provide to individuals?

As a starting point you must always tell people:

- Who you are
- Why you need their information
- What you are going to do with it
- Who it will be shared with.

The information that you provide to individuals about the way their personal data will be used is often referred to as ‘privacy information’. In written form it is referred to as a ‘privacy notice’.

How and when should I provide privacy information to individuals?

Best practice is to use a blended approach using a number of communication methods and techniques.

In relation to the personal data you may process when undertaking official Council duties, it is the responsibility of the Council to ensure that citizens, service users, customers and visitors are informed about how the Council will use their data.

How does the Council provide individuals with privacy information?

The following outlines the main ways in which the Council provides privacy information to individuals. This is in addition to any verbal privacy information that officers may provide to individual when they make contact directly with the Council.

Main Privacy Notice

The main Privacy Notice is published on the Council's website under the Data Protection section. The notice provides individuals with all key information on:

- How we use their personal information
- Individual's information rights and how they may be exercised.
- How an individual can raise a concern or make a complaint about the way the Council is handling their personal data

The privacy notice is available via: Cardiff Council Privacy Notice

Service Privacy Notices

Some Services have developed a more detailed privacy notice to complement the main privacy notice. Service Privacy Notices are also published on the Council's website. They include specific information about what personal data each service collects, where the data comes from, who the data is shared with and how long it is kept for.

Cardiff Council Service Bespoke Privacy Notices

Forms and Applications

Forms and applications used to capture personal data from citizens, residents and applicants contain a short privacy statement that explains to individuals how the personal data requested on the form will be used by the Council. The statement also signposts individuals to the Council's Privacy Notice/s on its website for more detailed information.

When undertaking casework who is responsible for providing privacy information to constituents?

When undertaking casework, the Member (as the Data Controller) has a direct responsibility under data protection to provide information to constituents.

How should I provide constituents with privacy information?

You may provide privacy information to constituents in a number of ways:

- Face-to-face
- on the phone and
- via a Privacy Notice

When liaising with constituents in person or on the telephone, it is good practice to summarise during the call what information you've recorded about them and what you intend to do with that information, e.g. who you intend to share it with. In most cases this will be obvious, but for the avoidance of doubt it doesn't harm to clarify things. Constituents should also be referred to the Councillor's Privacy Notice (see below).

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:
https://www.cardiff.gov.uk/ENG/Home/New_Disclaimer/service-specific-privacy-notices/privacy-notice-for-ward-councillor-and-consent-form/Pages/default.aspx

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 following email footer:

'Any personal information you give me will be treated as confidential, but may be shared with others if necessary to enable me to assist with your enquiry – if you have any concerns about this or would like further details please see the Privacy Notice for Ward Councillor and Consent Form (cardiff.gov.uk)

Bydd unrhyw wybodaeth bersonol a roddwch i mi yn cael ei thrin yn gyfrinachol, ond gellir ei rhannu gydag eraill os oes angen i'm galluogi i gynorthwyo gyda'ch ymholiad – os oes gennych unrhyw bryderon am hyn neu os hoffech gael rhagor o fanylion, gweler yr Hysbysiad Preifatrwydd ar gyfer Cynghorwyr Ward a Ffurflen Ganiatâd'

Poster/signage

Good practice is to display notices in public areas so people can see that you are taking privacy seriously, and they know how to contact you in the event of a query or concern about the way you are using their personal data.

Do I need written authority from a constituent to represent them?

Data protection law does not require a Member to have written authority from a constituent to represent them. However, you should seek written consent if practically possible, to confirm your constituent's instructions and consent. That way there can be no doubt that the constituent has requested your assistance in resolving their concern.

You should also seek written consent from your constituent in the following cases:

(a) If there is any doubt about what the constituent wants you to do or what you will do with their information;

(b) Where the request is about someone else (a third party), you should seek consent from the third party, if practicable, or seek advice;

(c) For safeguarding cases, or cases involving any other type of exceptionally sensitive personal information, where the Council (or other agencies) will require evidence that you are acting on behalf of the constituent and that the constituent has consented to disclosure of that information to you.

The Council has produced a consent form which Members can use to obtain written consent. This can be found via: https://www.cardiff.gov.uk/ENG/Home/New_Disclaimer/Documents/Ward%20Councillor%20Consent%20Form.pdf

DATA MINIMISATION & DATA ACCURACY

Minimisation

You should ensure you have a clear reason for collecting and holding the personal data and can justify this if challenged. Some tips include:

- Collect and hold no more data than you need – always the minimum amount.
- Don't collect or hold personal data "just in case" it might be needed.
- Consider each enquiry on a case-by-case basis and carefully decide what personal data you need to resolve that particular enquiry.
- If you've collected personal data that you didn't actually need, delete it.

Additional care should be taken if you need to collect Special Category data such as race, health or political information

Accuracy

When a constituent makes contact with you, it would be good practice to check that any contact information you hold for them is current, accurate and up-to-date.

- When collecting personal data, take care recording the data and confirm/repeat the information back to the individual to ensure that you have recorded it correctly.
- Where personal data changes, update your records promptly and double check the information that you have entered.
- If receiving personal data via a third party, take reasonable steps to verify the accuracy of the data where required. Don't assume it's always right!
- Correct incorrect information promptly.

Retention of Information

You must not hold personal data for longer than is needed in relation to the purpose for which it was collected. You must also be able to justify the length of time you are keeping personal data for.

Official Council duties

The vast majority of personal data held by Members in relation to their official Council duties are likely to be copies of master records held by the Council and/or that are published on the Council's website, for example copies of committee agendas, reports and minutes, etc. These copies may therefore be routinely disposed of after they have served their purpose.

Casework

Following closure of a case, the case papers may be kept until the end of an Elected Councillor's term of office or 3 years, unless you are asked to do otherwise or are otherwise required by law.

Casework is often revisited to provide the best service and representation for constituents, from whom Elected Councillors may continue to receive correspondence. Therefore, it is reasonable for an elected representative to hold personal data for this length of time.

Handover of Casework

If a Member's period of office ends before resolving a constituent's request, you may wish to transfer the case file to another ward councillor. However, before transferring any case file, the constituent should be informed and given the opportunity to ask you not to do so; and if the case file includes any Special Category or Criminal Convictions Data, you should seek written consent from the constituent (or any third party who the information is about) before transferring the file. You should keep a written record of any case files transferred, with confirmation from the Member to whom files have been transferred.

DATA SECURITY & COMPLAINTS

Cardiff Council is legally required under the Data Protection Act 2018 to ensure the security and confidentiality of the information it processes on behalf of its clients and employees.

Whilst using Council supplied devices Members must adhere to all IT Security and Information Governance policies and procedures and queries should be raise with Members Services.

Data Loss incidents

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.

Typical data security incidents are categorised by the Council as follows:

A **Data Loss** is when personal data of our customers or employees has been disclosed or destroyed in error through system failures or neglect in procedures for storing, transmitting, and processing data.

An **Asset Loss** occurs when Council IT equipment such as laptops, mobile phones, or tablets have either been lost or stolen. This leaves the data on the device(s) vulnerable to attack.

An **email error** is when an email containing personal or sensitive data is sent internally to the wrong recipient in error. An external recipient would be considered a Data Loss incident.

Data Protection Complaints

Any complaints in relation to data protection matters in respect of members, including where data may have been breached by a member, should be reported immediately to Democratic Services for advice.

The reporting requirements will differ depending on the role in which the member was acting at the relevant time. Where a complaint relates to a member's ward or political work, the member will need to seek advice from their political group or the ICO.'

In respect of any complaint against a Member in relation to your personal obligations under the Data Protection Act you should seek advice from your political group or the ICO.

INFORMATION RIGHTS – PUBLIC ACCESS TO INFORMATION HELD BY THE COUNCIL AND OR ELECTED MEMBERS

Members of the public have statutory rights to access information under:

• UK General Data Protection Regulation and Data Protection Act 2018 which regulates the processing of personal information and gives individuals rights over their own personal information

• The Environmental Information Regulations 2004 which provides access to environmental information held by (or on behalf of) public authorities

• The Freedom of Information Act 2000 which provides access to other information held by (or on behalf of) public authorities

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.

This section of the guidance sets out the requirements of the authority and Members' role and responsibilities in access to information requests.

Freedom of Information and Environmental Information Regulations

The Freedom of Information Act and Environmental Information Regulations cover all recorded information held by, or on behalf of, the Council, regardless of the format it is recorded in or how long it has been held.

The main principle of the legislation is that people have a right to know about the activities of the Council. Individuals do not have to provide a reason for requesting information, all requests are treated equally and the identity of the applicant is irrelevant when deciding if information can be released.

Information must be disclosed unless it falls within one of the exemptions set out in the legislation.

Information held by Members

Information held by Members may be regarded as being held 'on behalf of' the Council and therefore open to public access under FOIA and EIR.

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 or 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.

Examples of what **is** open to disclosure under FOIA / EIR:

- Information provided by a Member to a Council officer
- Information held by Cabinet Members in relation to their Cabinet role (discharging the executive functions of the authority)
- Information held by a Member in relation to their role as representative of the Council on an outside body
- Information held by a Member in relation to discharging a specific role on behalf of the authority, for example, as the Chair of a Committee

Members should also note that any information sent by a Member to another public authority, which is subject to FOI/EIR, may need to be disclosed by that public authority.

Examples of what is **not** covered by FOIA / EIR:

- Members' ward correspondence (with residents or third parties on behalf of residents)
- Correspondence between Councillors
- Party political information
- Information held by the Council solely on behalf of a Member (or another person) and not for any Council purposes,

unless it also falls within one of the categories of information which is open to disclosure, as listed above, for example, if it is sent to a Council officer.

Data Protection Individual Rights Requests for information

Members, as registered Data Controllers under the Data Protection Act (DPA), are personally responsible for complying with their statutory duties under the DPA.

The DPA gives individuals specific rights over their own personal information – called Individual Rights Requests. There are 8 rights altogether but the three most common are the right to Access (Subject Access Request (SAR)), Erasure and Rectification.

This means that members of the public may request a copy of any personal information about themselves held by an Elected Member, or its deletion or correction, subject to the exemptions available under the DPA.

Members are personally responsible for responding to Individual Rights Requests for information held by them in relation to casework, even if the information is held on Council ICT systems.

If the personal information requested is *held by the Council* (not the Member), then the applicant should be advised to forward their request on to the Council's Information Governance Team either by submitting the request via the online form or to individualrights@cardiff.gov.uk. Verbal requests can be submitted via C2C

Detailed guidance on Individual Rights Requests is available from the Information Commissioners Office www.ico.org.uk and advice can be sought through Democratic Services and the Information Governance Team.

What you need to do if you receive a request for information under FOI/EIR?

In your role as an Elected Member of the Council, you may receive a request for information by letter, email or verbally. If you receive a request for information, you must act on it promptly.

- If the request expressly refers to the Freedom of Information Act (FOIA, or EIR), you should explain to the requester that Members are not personally subject to FOI/EIR and advise the applicant to refer the request on to the Council's Information Governance Team by submitting the request via the online form or to FOI@cardiff.gov.uk. Requests must be in writing to be valid.

- If the information requested relates to ward (constituency) or political matters, you should deal with the request as a routine ward / political matter. The FOIA / EIR public rights to access information do not apply to such information. You should, however, be mindful of your duties under the Data Protection Act.

- If the information requested relates to Council business and does not expressly refer to FOIA or EIR, you should consider whether it is appropriate for you to respond personally or whether it would be more appropriate to refer it to a relevant Council officer for response (with the consent of the person concerned). Members' Services can advise you on this, if necessary.

If you are in any doubt or require any guidance you should contact the Information Governance Team for advice immediately via foi@cardiff.gov.uk

Please note that it is a criminal offence to deliberately erase, conceal, alter, deface or prevent information from being disclosed.

How the Council deals with Requests for Information

The Council has approved procedures for dealing with all information requests.

Requests are classed as either:

- Ordinary Business Requests – which are dealt with by the relevant directorate without unnecessary delay or formality; OR
- FOIA / EIR Requests – if the applicant expressly refers to their statutory rights or if the Council is minded to withhold certain information under a statutory exemption available by law. All FOIA / EIR requests are managed by the Council's Information Governance Team, in accordance with approved procedures and strict legislative requirements.
- DPA Individual Rights Requests - The Council has a separate procedure for dealing with Individual Rights Requests in relation to personal information held by the Council.

When the Council receives an FOIA or EIR request, it is logged by the Information Governance Team and forwarded to officers within the relevant directorates, who conduct a search of their records and collate any relevant information, which is then considered for disclosure. If the relevant information includes information relating to Elected Members, officers will seek to consult the Members concerned about their views on disclosure.

If necessary, officers may also ask Members to search their own records to check whether they hold any relevant information on behalf of the Council. Support staff may be able to assist Members to search their records. Officers will again seek to consult the Members concerned about their views on disclosure of the information which relates to them.

Please note, however, that the Council is ultimately responsible for complying with its statutory duties under FOIA and EIR, so the Council must make its own decision on disclosure; and it may not always be possible to consult Members in advance due to the strict statutory timescales for responding to requests.

The Council will usually redact any personal information about third parties prior to disclosure. However, the names of Members and Senior Officers (above Operational Manager level) within any documentation which is to be disclosed are generally released in the interests of accountability and transparency.

MEMBERS' RIGHTS OF ACCESS TO INFORMATION AND DOCUMENTS

Members may ask any Council Service to provide them with information, explanation and advice so that they can carry out their role as councillors. This can range from a request for general information about some aspect of a Service's activities to a request for specific information on behalf of a constituent.

In addition to general information, explanation and advice Members may also seek access to specific documentation held by the Council, its Officers or Cabinet. These rights are set out in the Access to Information Rules in the Constitution (Rules 17 and 18) and provide that:

- Any Member can see documents which contain information relating to the public and private meetings of the Cabinet, meetings of the Council and its Committees, any decision to be taken by an individual member of the Cabinet and any key decision made by an Officer, except for certain categories of exempt and confidential information.

- All members of a Scrutiny Committee have a right to copies of documents which contain information relating to the public and private meetings of the Cabinet, any decision to be taken by an individual member of the Cabinet and any key decision made by an Officer. However, they are only entitled to a copy of a document containing exempt and confidential information where the information is relevant to an action or decision which the member is reviewing or scrutinising or which is relevant to any review contained in a work programme of the Committee or Sub-Committee.

- All Members have a right to inspect the accounts of the Council and of any of its Proper Officers under Section 228 of the Local Government Act 1972.

All Members have a common law right to inspect documents where this is necessary for a Member to perform his or her duties (referred to as a 'need to know'). Members also have the same general rights available to any person under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

Member FOI Requests

Members have the same rights as anyone to make a request under FOIA. However, as a release of information under FOIA is a release of information to the public at large, a request from a Member is treated the same as if it were from a member of the public. As Members may have access to more information than members of the public, you may find that using the Members Enquiry Service will usually be a more appropriate route than making an FOI request.

An FOI request will give you the same information as a member of the public would receive, as FOI responses are considered to be publicly available information. Occasionally there may be situations where Members wish to know how much information would be publicly available in respect of a particular issue and so may wish to make an FOI request.

Protocol for Members Requesting Access to Information

The Council has adopted a Protocol on Members' Rights of Access to Information and Documents (found within Part 5 of the Constitution), which aims to clarify what Members are entitled to see, and how to go about seeing it. Members and Officers must at all times follow the Members Rights of Access of Information and Documents Protocol.

FURTHER ADVICE & GUIDANCE

WLGA – GDPR Guidance for Members (June 2018)

ICO Advice for elected and prospective councillors

ICO Constituency casework of members of Parliament and the processing of sensitive data

ICO Disclosure of personal information by local authorities to councillors

ICO Guidance on political campaigning

ICO Guide to the GDPR