South Derbyshire District Council

Elected Member Data Protection Handbook V1.1 [Draft]

September 2023

Contents

Version Control

Version	Description of version	Effective Date
1.1	Adoption	

Approvals

Approved by	Date
Data Protection Officer	
Leadership Team	

Associated Documents

Name
SDDC Member IT Protocol

About this guidance

This guidance has been developed for Elected Members. It serves as a useful reference to support Members in complying with the requirements of data protection legislation by providing practical advice, information and guidance on the collection, use and storage of personal data.

The advice and guidance contained in this document is primarily aimed at Members when representing the Council. However, the guidance may also be adopted by Members when collecting and using personal data for the purpose of casework (should they wish to do so).

It is entirely up to Members to decide whether or not this guidance is adequate in this regard and to adopt it for casework purposes. Whilst this guidance mirrors the key topics and themes covered in the formal Data Protection training that is provided to Members, it should be noted that the guidance is not intended to replace this training, nor the advice that is available from the Data Protection Officer.

Glossary of Terms:

The following terms appear regularly throughout this document. Their definitions are below:

Official Council duties or Council Business: 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.

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.

Information handling principles

Data protection legislation sets out good information handling principles that Members must follow. The key principles are summarised below and are covered in more detail within this guide:

1. Keeping 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. Specified 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 absolutely 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. Information Security

You must ensure that personal data is kept safe and secure.

7. Information Rights

You must ensure that people are made aware of their information rights and are able to exercise them.

1.0 How data protection applies to Members

This section aims to explain how data protection legislation applies to Members when collecting and using personal data when undertaking official Council duties, casework and when representing a political party.

The role of a Member

1) They will act as a member of the Council undertaking official council business, for example, as member of a committee or sub-committee. As defined in the Code of Conduct a "Councillor" means a member or co-opted member of a local authority or a directly elected mayor. A "co-opted member" is defined in the Localism Act 2011 Section 27(4) as "a person who is not a member of the authority but who
(a) is a member of any committee or sub-committee of the authority, or;
(b) is a member of, and represents the authority on, any joint committee or joint sub committee of the authority;

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. This policy only applies when the elected member acting in the capacity outlined in point one above.

Who is accountable for the personal data, and therefore what devices and communication channels to use, 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 will do this by providing Members with training, awareness, policies, procedures and guidance so that they know how to handle personal data properly and lawfully.

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 they process as they will determine the means and purpose of processing and must ensure that it is used in the right way. If the Member chooses to use ICT equipment provided by SDDC for their casework they remain the data controller for the lifecycle of the data, however the Council will also be a data controller for data stored on our network and as such will secure its network to prevent data loss. If data breach has occurred from a data loss relating to SDDC networks the Council will report the incident to the ICO

It is assumed by the Council that Elected Members undertaking casework are responsible for knowing and abiding by the data protection principles.

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.

Segregation of Duties & Personal Data
Data protection legislation requires that you have a very clear specified purpose for collecting and using personal data.
Once collected for a specific purpose, personal data cannot generally be used for any other purpose unless:

- the new purpose is compatible with the original,

OR

- you get the consent of the individual to use their data for another purpose,

OR

- you are required to use the information in another way by law (e.g. reporting a safeguarding concern).

For Members, the purpose for processing the personal data is linked directly to the role they are undertaking. For example, when representing a constituent, any personal data collected and used is for the specific purpose of dealing with the enquiry or complaint, and must not be used for any other purpose, e.g. political campaigning.

It is therefore important that Members segregate any personal data held for different purposes and roles.

2.0 Keeping People Informed

This section explains what information a Data Controller (DC) must provide to individuals when you collect their personal data.

What data protection law requires
Data Protection law requires that Data Controller's 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 collecting personal data from an individual it's important to provide 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?
The law sets out what information must be provided to individuals when you collect their personal data. At a minimum, and as a starting point you must always tell them:

- 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 DC's 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?
Data protection law does not specify how privacy information should be provided to individuals. Good practice is to use a blended approach using a number of communication methods and techniques.

The following outlines how privacy information is/should be provided to individuals when you are representing the Council or undertaking casework.

2.1 Official Council duties

Who is responsible for providing individuals with privacy information?
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, via its Members and Officers use their personal data when providing them with services.

How does the Council provide individuals with privacy information?
The following outlines the key 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 consists of a series of webpages that provides individuals with information on the following topics:

- How we use your personal information – An Overview
- Introductory page about the way the Council uses personal data and the ways in which we protect people's privacy.
- How we use your personal information – frequently asked questions
- Answers to commonly asked questions about the Council's use of personal data.
- Your information rights
- Provides information on an individual's information rights and how they may be exercised.
- Concerns or complaints about the way the Council is handling your personal information Provides information on how an individual can raise a concern or make a complaint about the way the Council is handling their personal data.

Service Privacy Notice
Each Service has developed a more detailed privacy notice to compliment 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.

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 website for more detailed information.

2.1 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 law to provide privacy information to constituents.

3.0 Casework - Authority to Act

This section provides guidance on whether a Member needs authority from an individual to represent them or to discuss their concern with an organisation.

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, some Members may prefer to have something in writing, particularly in situations where the query or concern is of a sensitive nature. That way there can be no doubt that the constituent has requested your assistance in resolving their concern.

For indirect enquiries, do I need the consent of the individual who the enquiry is about before I take on the casework?

Example: An indirect enquiry is usually referred to as an enquiry received from a third party on behalf of an individual. For example - a daughter acting on behalf of her frail elderly mother contacts you for support regarding her mother's benefit claim.

In the above example, you would need confirmation from the mother that she is happy for the daughter to act on her behalf. This could be achieved through a simple phone call to the mother.

If the mother is incapable of confirming this, for example, if she suffers with dementia and does not have capacity, you should request proof from the daughter that she has authority to act on her mother's behalf (e.g. proof of power of attorney, confirmation that her mother's finances are in her name (bank statement), etc.). This authority should not be assumed even if the individual is known to you.

Do I need to provide proof of authority to act when requesting information from an organisation?

When undertaking casework you may be required to contact organisations to assist you in resolving the enquiry or concern. These organisations may include (but are not limited to) services within the Council, Local Health Board, GP Practice, Job Centre, Department for Work and Pensions, etc.

Often, as part of that organisation's data protection procedures, especially where a Member is not known to the organisation, the organisation may ask you to provide proof that you have authority (sometimes referred to as consent) to act on the constituent's behalf. In addition, the organisation may ask you to confirm your identify as an Member.

This request for authority / proof should not be perceived as a barrier or the organisation being obtrusive, but good practice that ensures personal data is not discussed or disclosed to someone acting under a false pretence.

4.0 Data Quality

This section covers what is commonly referred to as the 'data quality' principles. It includes good practice, hints and tips relating to data minimisation, keeping personal data accurate and up-to-date and retention.

Data minimisation

Data protection law requires that:

a) You collect enough personal data to sufficiently fulfil the purpose for which the personal data is being processed;

b) The personal data is relevant to the purpose for which it is being collected; and

c) It is limited to what is necessary in relation to that purpose.

Here are some hints and tips to help you comply with this requirement when undertaking casework:

- Ensure you have a clear reason for collecting and holding the personal data and can justify this if challenged.
- 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.
- Look for alternatives – do you need someone's date of birth or is their age enough?
- If you've collected personal data that you didn't actually need, delete it.

Accurate & Up-to-date

- You must take reasonable steps to ensure the accuracy of the personal data that you collect and record.
- You should consider whether the personal data you collect and record needs to be kept up-to-date.
- If you discover that the personal data is incorrect or misleading, you must take reasonable steps to correct or erase the personal data as soon as possible.

Here are some hints and tips to help you comply with this requirement when undertaking casework:

- When a constituent makes contact with you, get into the habit of checking 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.

- Watch out for typing errors, especially when entering house and telephone numbers and email addresses!

- 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
A Data Controller 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.

If a Member uses an SDDC email account and laptop to conduct casework they are able to request any pertinent data when leaving office. If no such request is made, the Council shall delete emails and files in line with its protocol.

5.0 Communicating with individuals.

This section highlights the main risks associated with sending personal, sensitive or confidential information by email, letter, fax or social media messages. Members should select the most appropriate method of communication taking into consideration the volume and sensitivity of the information being communicated.

5.1 Communication via Email

When undertaking official Council duties, Members must use their Council email account, i.e. <name>@southderbyshire.gov.uk for all communications.

When undertaking casework, it is strongly recommended that Members use their Council email account to communicate with constituents.

Members may send the Council content from their personal addresses in relation to their casework, however personal email addresses cannot be used when undertaking official Council duties and as the data controller they must ensure the appropriate level of security and procedure is in place.

If a Member uses personal email accounts to conduct casework they are the sole data controller and will be responsible for reporting any data incidents to the ICO. If a Member uses their @southderbyshire.gov.uk email account the Council will at that point become an independent data controller with responsibility to keep data collected by the Member safe on the Council's network.

Any use of the Council's email system, whether a Member is using it for official Council duties or for casework use, must be used in line with terms set out in the Member ICT Policy.

Are Council emails secure?

Internal emails:
Emails sent internally within the Council <name>@ southderbyshire.gov.uk email account to another <name>@southderbyshire.gov.uk are secure. This means that the email is unlikely to be intercepted as the email never leaves the Council's network.

Emails to other public bodies:

Emails to and from a <name>@ southderbyshire.gov.uk email account, other Local Authorities and key partner organisations such as Central Government, the LGA, Police Authorities, DWP, are considered secure as the messages are encrypted in transit. This means, if the email is intercepted it's unlikely that the content of the email can be read by others because it is encrypted.

External emails:

Emails sent from a <name>@ southderbyshire.gov.uk email account to an external recipient (e.g. Gmail, Hotmail or private business accounts, etc.) cannot be guaranteed as being secure (as standard), as it depends on the security measures that have been implemented by the email provider of the recipient.

When sending emails where interception could compromise the freedoms of recipients or data subjects an additional level of security can be added to the email via outlook by clicking on the 'Sensitivity' button in a new message and selecting 'Official -Sensitive'. Note, this will change how the email is received and will require the recipient to take an extra step in order to read the message.

Are private / free email accounts secure?
Emails sent to and from private/free email accounts such as Gmail, Hotmail, etc. cannot be guaranteed as secure as it depends on the security measures that have been implemented by the email provider.

Before signing up to a private/free email account it is advisable to check the provider's terms and conditions and read their privacy notice to find out:

- What level of security they offer.
- In which country your emails will be stored.
- Whether they scan the content of your emails and if so why.
- Whether they use your information for any other purpose other than to manage your account.

In addition, before utilising a private/free email account to communicate personal data, Members should consider the following and form a view on the adequacy and appropriateness of using email to facilitate the enquiry:

- The nature of the enquiry.
- The sensitivity of the information.
- The number of individuals the information relates to.
- The potential impact on the individuals should the email be intercepted and the information
- contained within the email becomes known to others etc.

Sending personal information by email?

Email
In addition to the 'technical' risks mentioned above (i.e. email being intercepted whilst in transit) and the risk of a phishing attack, the biggest risks associated with using email for communicating personal, sensitive or confidential information are:

- The email could be sent to the wrong email address.
- Recipients could be copied in by mistake.
- The wrong attachment could be sent with the email.

How can I reduce those risks?

- Double check that you have the right email address.
- Double check that you have typed in the email address correctly. Ensure that you have included all letters, numbers and symbols.
- When selecting the recipient from the Council's global address list or the auto-populate list, ensure that you have selected the right person and be aware of users with the same/similar names.
- Check that you have not 'copied in' anyone by mistake.

Multiple Recipients:

- If using a distribution list, make sure that the members are up-to-date. Remember – local distribution lists are managed by you, not ICT. Updates to corporate distribution lists are made when a service manager or the Leadership Team compile a request for the list to be amended.

- When sending an email to multiple recipients who are not known to each other, use the 'Blind Carbon Copy (BCC)' function to protect the confidentiality of the recipients email addresses.
- When sending personal, sensitive or confidential information to a 'generic' inbox, such as customerservices@southderbyshire.gov.uk, be mindful that the email may be seen by any recipient who has access to that mailbox.

Attachments:

- Be careful when inserting attachments – ensure you have attached the right document(s).
- Once attached to the email, open the attachment and double check it is the right document before you send.

And finally, be careful and take your time when composing the email. Double check everything before you press send. Remember that most emails will be disclosable under Freedom of Information requests so content must be appropriate.

What if I send an email containing personal or confidential information to the wrong person?
Email errors involving personal information are one of the most common causes of personal data breaches. Despite anyone's best efforts, mistakes will happen and when they do it's important that you deal with the error promptly. The following steps should be taken in the event of an email containing personal of confidential information being sent to the wrong person:

1) Immediately recall the message in Outlook.

2) If you can, obtain the contact number of the recipient. Contact them to request that the email be deleted. Ask them to confirm by email that this has been done, and also as then to confirm that the email content has not been forwarded or disclosed to anyone else.

3) Notify the Council's Monitoring Officer and Data Protection Officer of the error.

4) Keep copies of any relevant correspondence to show you have taken all relevant steps to recover the email (this may be needed for any Information Management investigation that may be required).

5.2 Communication via Letter

What are the risks?

- The wrong address and/or recipient could be written on the envelope.
- The wrong information could be included in the envelope.
- The letter could be lost in transit - delivery and receipt of the letter can't be guaranteed in all cases.
- Information could be delivered to wrong address even if the right address is on the envelope.
- Information in paper from is not protected if lost, stolen or seen by
- others.

How can I reduce the risks?

- Double check that you have the correct address
- Ensure the address is correct on the envelope and clearly stated.
- Always include a postcode.
- Always address the letter to a named individual.
- When sending to a company, where possible mark the envelope for the attention of a named individual and their department.
- Ensure the envelope is fit for purpose and can withstand transit. Use tamper proof envelopes where required or seal the information in a double envelope.
- Ensure a return address and contact name is marked on both the outer and inner envelope so that it can be returned to you by the mail service in the event of non-delivery.
- Double check that correct information is enclosed.
- Ensure the information enclosed is also addressed
- Select the most appropriate postal method for the letter based on the sensitivity and volume of the information being sent, e.g. special delivery if you require full tracking and proof of delivery, etc.
- It is good practice to let the receipt know when and how you are sending the information then and to ask them to confirm receipt.

5.3 Communicating via Social Media

Social media is an increasingly popular means of communication that allows people greater freedom and choice in how they communicate both socially and for business purposes. For many it is now the preferred way of finding out what's going on in the local area or contacting a business or organisation.

Using social media when undertaking Council duties will be co-ordinated via the Communication team and Elected Members should not represent the Council using social media in this capacity.

Personal social media accounts and messaging services such as Facebook, Messenger, WhatsApp, etc. must not be used to conduct official Council Business.

Using Social Media for casework
As the Data Controller Members are free to decide whether they wish to use social media as a platform to communicate with constituents when undertaking casework. Should a Member wish to use social media it is recommended that the following guidance is observed:

Open groups/forums/chatrooms:

- Never communicate with constituents on personal matters in a public forum etc.
- Should a constituent contact you via an open forum regarding a personal matter you should advise them to contact you directly via a more appropriate private communication channel (e.g. email, telephone, in person, etc.)

Separating personal from professional
This separation of personal and professional will provide you with greater privacy and may provide you with greater engagement, allowing your local residents to engage with you as a Councillor without the need to become your 'friend'. It also will allow you to undertake casework without using your personal social media account.

You can make use of stringent privacy settings if you do not want your personal social media account to be accessed by the press or public. However, it's important to note that even the strictest privacy settings are no guarantee for posts or actions to remain private.

6.0 Data Breaches

This section outlines what responsibilities a Data Controller has in relation to personal data breaches and what to do in the event of a breach.

What is a personal data breach?
A personal data breach is an incident that affects the confidentiality, integrity and / or availability of personal data.

It is not possible to detail every single incident that may result in a breach, but instances would typically include:

- The theft or loss of personal data or devices that hold such data.

- Inappropriate disclosure of personal data (e.g. an email being sent to the wrong recipient, wrong information in a letter).

- Unlawful access to personal data (e.g. an officer accessing a service user's record with no legitimate business reason for doing so).

- A computer virus that affects Council data.

What does the law require in the event of a personal data breach?
The controller must investigate any breach of personal data and keep a record of that breach.
Where there has been a serious breach, the controller may also be required to inform the Information Commissioner's Office, and in some instances the individual whose personal data has been affected. This must be done within 72 hours of becoming aware the breach.

The data controller must also keep a record of any personal data breach regardless of whether the ICO and/or individual is informed.

Should you encounter a potential, suspected or actual breach of personal data you must report the matter immediately to the Council's Data Protection Officer or any other senior manager in their absence (dataprotectionofficer@southderbyshire.gov.uk) It is recommended that this be done by telephone rather than an email to ensure that the matter is dealt with promptly.

When reporting, you should provide as much information as possible so that the Data Protection Officer can assess the severity of the breach and make an informed decision on whether the matter is to be reported to the ICO and the individual who is affected by the breach. This should include:

- A description of the data breach

- The type and sensitivity of the information affected by the breach.

- Number of individuals affected.

- Whether the breach could put anyone at risk.

- Any action taken to recover/contain the situation.

7.0 Information Rights

Data protection legislation gives rights to individuals. There are several rights including the right to be informed, right of access, right to rectification, right to erasure.

This section focuses on the right of access which is one of the most commonly exercised rights. It explains how a request can be made and how it should be handled.
For details on the other rights please see the ICO's website or contact the Information Management team. Please note that the right to be informed has already been covered in Section 2 of the guide.

What is the right of access?
Individuals have the right to access the personal data that a Controller holds about them. Such a request is commonly referred to as a Subject Access Request (SAR). Individuals are not entitled to the information of anyone else under this right.

A SAR can be made in writing, e.g. mail, letter or through the completion of a SAR form. A SAR can also be made verbally, e.g. in person or over the telephone.
Once a request has been made and the identity of the requestor verified, the Controller has one month to provide the information.

7.1 Who is responsible for responding to a SAR?

It is the responsibility of the Council to respond to any SAR for personal data that is held by the Council. This includes any personal data that may held by a Member for the purpose of undertaking their official Council duties.

What should I do if I receive a SAR from an individual for their personal data?
Should a Member receive a SAR directly from an individual, the request must be forwarded (without delay) to the data protection officer by email (dataprotectionofficer@southderbyshire.gov.uk). Upon receipt of the SAR, the DPO will validate and acknowledge the request to the individual.

Should the scope of the request include information held by a Member (for the purpose of official Council duties), the Data Protection Officer and the Council's Monitoring Officer will work with the Member to identify the requested information and respond to the individual within the relevant timescale.

7.2 Subject Access Requests for personal information relating to casework

It is the responsibility of the Member to respond to any request received from an individual for personal information that is held by a Member in relation to casework.

How should a Member respond to a SAR?

The following suggests the key steps that may be taken by Members when responding to a request. Alternatively, the Member may wish to contact the Council's Data Protection Officer who will support the Member in responding to a SAR:

- Step 1 - Confirm the identity of the requestor, calculate the deadline for response and formally acknowledge the request.
- Step 2 – Locate the information, searching all electronic and paper records held. Collate the information covered by the request.
- Step 3 - Review the information, redacting any information relating to others.
- Step 4 – Decide how you will provide the information to the individual explaining anything that they may not understand (abbreviations, etc.).
- Step 5 – Review and double check the information ready for release.
- Step 6 – Provide the information to the individual. Keep a record of the information provided for any future enquiry.