RHONDDA CYNON TAF

INFORMATION MANAGEMENT

GUIDANCE

Elected Member
Data Protection Handbook

V1.1 DRAFT – November 2021

DIOGELU DATA PROTECTION

MAE EICH DATA O BWYS YOUR DATA MATTERS

Contents

About this guidance

This guidance has been develop at the request of 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 specialist advice that is available from the Information Management team. Members should continue to consult the Information Management team directly should they have a specific query or concern that is not covered in this guidance.

The document signposts to a number of supporting Council policies, procedures and guidance. Whilst these documents are primarily aimed at officers, their content and good practice applies equally to Members when handling personal information and may be adopted by Members.

Definitions

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.

- **Device:** Any ICT device that may be used by a Member including a laptop, tablet, office PC, mobile phone, etc.

Good 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.

Section 1:

How data protection applies to Members

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 the Member

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.

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.

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.

Hints & Tips

You should not use personal data obtained in one line of business for another.

Organise your records - keep documents separate for the different roles that you undertake.

Clearly label files, folders, records and documents so you know in what capacity you obtained the personal data and for what purpose it should be used.

Remember this applies to electronic records, paper records and emails.

Section 2:

Keeping People Informed

Keeping people informed

This section explains what information you must provide to individuals when you collect their personal data. Its covers the responsibilities of the Council when Members process personal data when representing the Council, and the responsibilities of Members when undertaking casework.

What data protection law requires

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?

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 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?

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.

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.

Keeping people informed - What do I need to do when representing the Council?

- **Familiarise yourself with the privacy information contained on the Council's website.**

- **Be aware that if you chair a committee where the public are present and are able to participate in the meeting, an Officer will read a short privacy statement at the start of the meeting so that the public are aware of how their personal data will be captured, recorded and used during and following the meeting. This is especially important where the meeting is being recorded.**

- **In the unlikely event that an individual contacts you directly with an enquiry about the way the Council or you as a Member (when undertaking official council duties) uses their personal data, you should signpost them to the Council's website for further information or advise them to contact the Information Management Team (contact information is provided in Section 11 of this guide).**

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.

How should I provide constituents with privacy information?

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

- ❖ **Face-to-face or on the phone**

  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.

  To support you in this area a suggested script is contained within the Guidance for Elected Members on the requirement to provide privacy information to constituents when undertaking casework (page 6).

- ❖ **Councillor Privacy Notice**

  As agreed by Members at the Democratic Services Committee, each Member has a Councillor Privacy Notice published on the Council's website under their individual Member webpage.

  The privacy notice is equivalent to the Council's 'service' privacy notice and explains to constituents in detail how you may use their personal data when undertaking casework on their behalf.

- ❖ **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. At the request of Members, we have created a poster template that you may wish to display in surgery waiting areas or meeting rooms, etc.

  The poster is also available in Appendix II of the guidance or copies can be obtained via Members' Services.

Keeping people Informed when undertaking casework
Hints & Tips

- **Familiarise yourself with the content of your privacy notice (your Member webpage on the Councils website).**

- **Signpost constituents to your privacy notice when required.**

- **When communicating with constituents, whether in person, over the telephone or by email get into the habit of confirming how you will use their personal data.**

- **If holding a surgery, etc. consider displaying a privacy poster to demonstrate to constituents that you take data protection and their privacy seriously.**

- **Familiarise yourself with the Guidance for Elected Members on the requirement to provide privacy information to constituents when undertaking casework.**

Section 3:

Casework - Authority to Act

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.

At the request of Members, an 'Authority to Act' form has been developed. The form may be used by Members should they wish to obtain written confirmation from a constituent to act on their behalf. The form can be accessed here. Members are free to make changes to the form to suit their individual requirements.

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.

If in doubt as to what is considered sufficient proof, or if you have any concerns regarding this please feel free to contact the Information Management team for advice.

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

Sometimes. 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.

Casework – Authority to Act
Hints & Tips

- **Use the Authority to Act form if you prefer to have something in writing from a constituent confirming that they are happy for you to represent them.**

- **For indirect enquiries, always confirm with the individual (who the enquiry is about) that they are happy for a representative (e.g. a family member) to act on their behalf.**

Section 4:

Data Quality

(Minimisation, Accuracy & Retention)

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:

Hints & Tips:

- **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:

Hints & Tips:

- **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

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 Democratic Services 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

In relation to casework, it was agreed by Members that records would be kept for no longer than 3 years from the date the matter was brought to a close. This is reflected in each Member's privacy notice. However records should be regularly reviewed and weeded to ensure that only essential information is kept for that period of time.

Hints & Tips:

- **Review the personal data that you hold regularly whether it's held in electronic or paper format.**

- **Delete personal data that does not need to be kept for the full 3 years or at all. As a rule, this usually applies to information that is duplicated, unimportant or with no significant value. Examples may include:**

  - **Working copies or drafts leading to a final item of correspondence.**

  - **Follow-up emails, etc. that add no value or bearing on the outcome of the enquiry or any decision made etc.**

  - **Requests for everyday information.**

  - **Correspondence where you have been 'copied in' for information only.**

  - **Information that is duplicated e.g. a printed copy of a letter that is also held in electronic format.**

  - **Remember to securely dispose of any information using a cross cut shredder or via confidential waste (see Section 8 for further information).**

Section 5:

Communicating with individuals

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.

By Email

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

When undertaking casework, Members may use their Council email account to communicate with constituents should you wish to do so. Such use would be considered 'personal use' of the Council's email system.

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

Are Council emails 'secure'?

Internal emails:

Emails sent internally within the Council (from an <name>@rctcbc.gov.uk email account to an <name>@rctcbc.gov.uk.) are considered '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 an <name>@rctcbc.gov.uk email account and other local authorities in Wales and key partner organisations such as Welsh Government, WLGA, South Wales Police, South Wales Fire & Rescue Service, Cwm Taf Morgannwg University Health Board 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 an <name>@rctcbc.gov.uk email account to an external recipient (e.g. Gmail, Hotmail or private business accounts, etc.) cannot be guaranteed as being secure, as it depends on the security measures that have been implemented by the email provider of the recipient.

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.

Should a member have a specific query or concern regarding the use of email for communicating personal information they may contact the Information Management team.

Should a Member decide to use their personal email account for casework it is recommended that the Member:

- Has a dedicated email account for casework.
- Does not used a shared (e.g. family) email account as any personal or confidential information contained within email communications to and from constituents may be seen by family members.
- Creates a strong password for the email account.
- Does not share their email password with others including family members.
- Ensures that they fully signed-out of their email account when not in use, especially if the device is used by others.

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 (covered in Section 6), 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?

Email Address:

- 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 - distribution lists are managed by you, not ICT.
- 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@rctcbc.gov.uk, be mindful that the email may be seen by any recipient who has access to that mailbox. If in doubt, check who has access before sending the email.

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!

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/or the Information Management Team 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).

ℹ Procedure for dealing with emails that have been sent in error.

By 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?

Name & Address:

- 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.

Envelope & Content:

- 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

Postal Method:

- 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.
- For further information on delivery options please contact the Business support Unit on XXXXXX

Confirm Receipt:

- 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.

By fax

What are the risks?

- The fax number could be misdialled.
- Delivery is not guaranteed.
- If the fax is sent to the wrong number it can be difficult to identity who the fax has gone to.
- Fax machines are often in shared office spaces (e.g. reception). The fax could therefore be seen or collected by others.

How can I reduce the risks?

The use of facsimiles for transmitting personal information is not advisable. Should you have no alternative other than to use fax, the following guidance should be followed:

Fax Number:

- Use a tested pre-programmed fax number wherever possible.
- If this is not possible double check that you have the right fax number and be careful when dialling.

Content:

- Double check that the correct information is being faxed.
- Check all pages front and back.

Contact the receipt ahead:

- Telephone the recipient ahead to let them know that the fax is being sent. Ask them to wait for the fax by the fax machine and acknowledge safe receipt.

Fax cover sheet:

- Always use a fax cover sheet.
- Ensure the fax cover sheet is fully completed and addressed to an individual rather than a company or department.
- Ensure you state the number of pages included in the fax on the cover sheet.

Fax confirmation sheet

- Check the fax confirmation sheet to ensure that:
  - The fax has been successfully transmitted;
  - All pages have been successfully transmitted; and
  - The document has been transmitted to the correct fax number.
- Make sure that you take all copies of any documents that you fax away with you - some faxes will automatically print a copy of what you have sent after they have finished sending the document.

By 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

Any use of social media by a Member when undertaking official Council duties must be in keeping with terms of use set out in the Council's Social Media Policy.

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

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

Some Councillors choose to have separate social media profiles for personal use and a Facebook page for their Councillor use. 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.

Private messaging:

As with personal email accounts, messages sent and received via social media messaging services such as Facebook messenger, WhatsApp etc. cannot be guaranteed as secure as it depends on the security measures that have been implemented by social media platform provider. Before utilising a private social media messaging service to communicate with constituents, you should consider the following and form a view on the adequacy and appropriateness of using social media 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 message be intercepted and the information contained within it become known to others etc.

Members should also be mindful that all social media messages is relation to casework, whether in an open forum or through a private message can be disclosed under subject access rights (see Section 10). If using social media to communicate with individuals, Members should consider how they would provide such information in response to a request.

Section 6:

Cyber Security

Cyber Security

Cyber threats and attacks are one of the biggest risks the Council now faces. Whilst the Council takes proactive measures to reduce the likelihood of an attack happening, inevitably, with scams becoming more and more sophisticated, it's important that Members are aware of the dangers and know how to protect themselves.

This section of the guide focusses on one of the biggest known cyber risks the Council and its User face today - 'Phishing' email attacks. The advice in this section may equally to Members in their home life as it does in their work life.

Phishing Emails

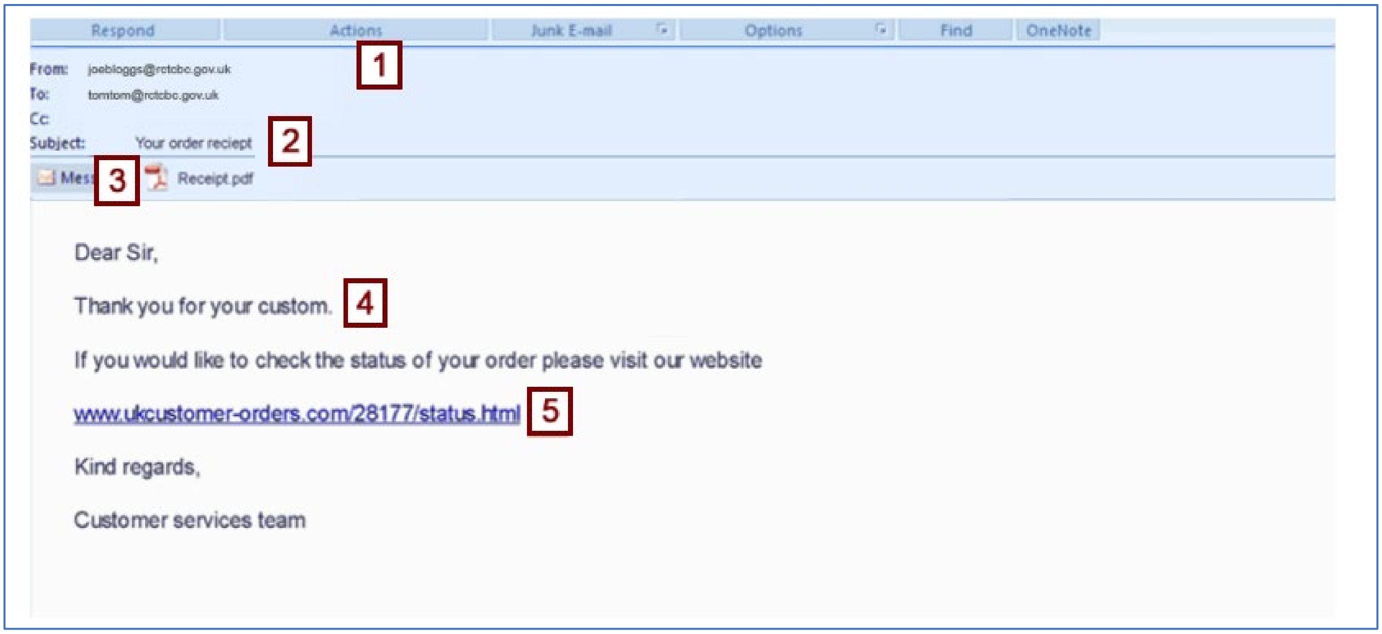
What is Phishing?

Phishing is a type of online scam where perpetrators send out fraudulent email messages that appear to come from a legitimate source. The email is designed to steal your data by tricking you into entering confidential information such as, account numbers, passwords, pin numbers or personal information such as your date of birth or national insurance number, etc. into a fake website by clicking on a link. The perpetrators are then likely to use this information to commit identity fraud or sell it on to a third party.

Top tips to spot a Phishing attack:

Identifying a phishing email has become a lot harder than it used to be as perpetrators have honed their skills and become more sophisticated in their attack methods. The phishing emails that we receive in our inbox are increasingly well written, personalised, contain the logos and language of brands we know and trust and are crafted in such a way that it is difficult to distinguish between an official email and a malicious email drafted by a scammer.

Whilst the Council has a number of ICT technical controls in place that block any suspected malicious e-mails reaching a Members inbox, it's important that Members are aware of the dangers and know how to protect themselves.



From: joebloggs@rctcbc.gov.uk
To: tomtom@rctcbc.gov.uk
Cc:
Subject: Your order reciept

Receipt.pdf

Dear Sir,

Thank you for your custom.

If you would like to check the status of your order please visit our website

www.ukcustomer-orders.com/28177/status.html

Kind regards,

Customer services team

1. Sender

- Do you know this person? Is this their usual email address? Were you expecting this email?
- Not recognising the sender isn't necessarily cause for concern but look carefully at the sender's name and email address – does it sound legitimate, or is it trying to mimic something you are familiar with?
- Double (left) click on the senders' name. Check the actual email address the email come from in the pop-up box.

2. Subject

- Does the email subject look unusual? Is it meaningful in relation to the message? Does it contain excessive punctuation, capital letters, etc.?
- Subject lines are often alarmist and use excessive punctuation, hoping to scare the recipient into an action without much thought. Conversely subject lines can also be left blank enticing the recipient to open the email to find out its content.

3. Attachments

- Do I recognise the attachment format (e.g. doc, pdf or jpeg)? Does the email mention the attachment? Are you expecting an attachment?

4. Content

- Be wary of emails that refer to you by a generic name, or in a way you find unusual, such as the first part of your email address, generic greetings such as ‘Dear member’ or ‘Dear user’
- Look out for spelling errors, bad grammar, poor word choice, impersonal and/or odd/disjointed written emails but bear in mind modern phishing looks a lot better than it used to.
- Be mindful of short, vague or odd-sounding messages and those with promises that sound too good to be true!
- Be wary of emails that ask you to carry out an action like clicking on a link, opening an attachment or replying to the email with personal information.

5. Links

- Check links closely as they can easily be disguised to take you to malicious websites.
- Hover your mouse over the top of the link to reveal the actual hyperlink address. If the address is different from the address displayed in the email, the message is probably fraudulent or malicious.
- Look out for slight alterations or misspelling such as a missing forward slash (/) or subtle changes like an additional or missing full stop (.) or letter.

6. Other things to look out for

- No matter how realistic and official an email might look, it’s always a bad sign if the sender requests personal information from you. A reputable company should never send an email asking for your account number, password, credit card number, or the answer to a security question.
- Be aware of emails that seem too good to be true – they usually are!
- Be aware of emails inviting you to donate to a worthy cause after a natural disaster or other tragedy. Go to the charity’s official website should you wish to make a donation.
- Check the time and date of the email – has it been sent during normal office hours (e.g. Mon-Fri, 9.00-5.00) or out of hours or at the weekend? If the email has been sent/received at an unusual time this could be cause for concern.
- Check the logo, it may be of a low quality if the sender has simply cut and pasted from a website.
- Be wary of common phrases and offers that are enticing you to take action ‘verify your account information’, ‘you have won a prize’, ‘your account has been frozen – take action now’.

How to protect yourself

- Familiarise yourself with our guidance for Staying safe when using email.
- Be alert!
- Never click on suspicious links.
- Never open suspicious attachments.
- If using a personal device (PC, laptop, tablet etc.) for conducting casework, ensure it has anti-virus installed.
- If using a personal email account for conducting casework check that the provider has web-filtering.
- Contact the ICT Service Desk if in doubt.

More detailed guidance: Staying safe when using email

Section 7:
Out and About
&
Working from Home

Out & About & Working from Home

When travelling and working with personal information outside of the normal office environment, information becomes more vulnerable and susceptible to loss, theft and compromise. Extra care must be taken to protect the confidentiality of personal information and measures taken to avoid unnecessary risks to that information and the people it is about.

Information in paper format:

Personal information in paper format cannot be protected if lost, mislaid or stolen and is therefore potentially accessible by anyone who comes across it.

Top tips:

- Limit the amount of personal data you carry in paper format.
- Only take what's absolutely necessary.
- Never carry personal data on the off-chance you might need it, or look at it if you have the time - this is just creating extra risk for no real purpose.
- Don't leave paper records lying around for others to see, even when at home.
- Store paper records securely and out of sight when not in use.

Information Disposal:

Make sure you dispose of personal data in paper format securely – i.e. shred it using a cross cut shredder. If you do not have a shredder at home, make sure you utilise the office shredder or confidential waste bags. Never dispose of personal data in a recycling bag or public waste bin unless it has been shred.

Information in electronic format:

When undertaking Council business, wherever possible, personal data should be transported in electronic format using a **Council approved electronic encrypted device** such as a laptop, tablet or USB memory stick.

Telephone Conversations:

Ensure that confidential information is kept confidential:

- Avoid discussing anything sensitive where people might overhear.
- Pay attention to who is around you when on the telephone.

On-lookers:

- Make sure your device screen is not visible to others.
- Position your work in such a way so that others cannot see.

Housekeeping:

- Work tidily and with care.
- Ensure no information is on display.
- Check that you haven't left anything behind when you leave.
- Never leave your device or any source of sensitive information unguarded. It should always stay close to you.

Transporting information:

- Reasonable measures should be taken to safeguard personal data and equipment whilst in transit. These measures include reducing visibility to others and maintaining control of the data at all times.

- Electronic devices and paper records should be concealed and placed in a bag or briefcase, etc. For added security, the bag should be locked if possible.

- If you are visiting a number of places during the working day, you should carefully consider the risks associated with leaving the personal data your car (e.g. risk of theft/break in, etc.) against the risk of taking the personal data with you, for example into a constituent's home (e.g. risk of the documents being misplaced or left behind when you leave, etc.). If you decide to leave the personal data and/or your device in your car, you it should be securely locked in the boot of the vehicle.

- If travelling by public transport, personal data will become more vulnerable, and may be susceptible to opportunist crime, etc. You must ensure that the data remains in your possession at all times. Be aware of the risk of theft and ensure that nothing has been left behind when you leave.

Storing Information:

- When not in use, personal data and devices should be stored securely in your home out of sight of any visitors, etc.
- It is advisable to store information in paper format separate from your device.
- You must not leave your device or any information in your car overnight.

For more information see Protecting personal information outside the normal office environment.

Section 8:
General Security

Printing

Only print documents that contain personal, sensitive or confidential information when absolutely necessary.

When printing always:

- Attempt a test print when using a printer for the first time to make sure that it prints out in the place you are expecting it to.
- Collect documents promptly.

Should you come across any unclaimed printouts, ensure they are disposed of securely.

Information Disposal

Paper documents and records containing personal, confidential or commercially sensitive data be must shredded using a cross cut shredder, or disposed of in confidential waste. Such records must never be placed in a recycling bag or bin unless the information has been shredded.

All Council issued ICT devices must be disposed of securely via the ICT Service Desk.

For more information see Procedures for secure disposal of personal and commercially sensitive information.

Clear Desk

- Don’t leave paper records lying around; store them away when they’re not being used whether you are working from the office or at home.
- If you expect to be away from your workstation for a long period of time ensure all documents that contain personal data are securely stored.
- Work tidily and with care.
- Limit the amount of documents you print.
- Consider scanning paper documents that need to be kept.
- Securely dispose of information you no longer require.

Privacy when on the telephone

Always remember that a telephone conversation may be overheard by others, especially in an open-plan office, public area or when conducting business from home. You should avoid discussing private or confidential matters over the telephone when you are within earshot of anyone who does not need to know the information.

Voicemails & Messages

Leaving a voicemail for an individual or a telephone message with a family member or friend is a handy way of keeping someone updated on progress where you are unable to speak to them directly. But leaving a voicemail or message carries the risk of breaching an individual's confidentiality.

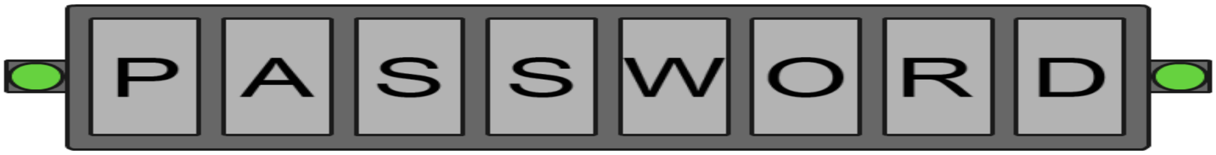
When leaving a voicemail or message for an individual with others you should:

- Check that you have permission from the individual to leave a voicemail and on what number it can be left (mobile phone, landline, etc.).
- Seek permission from the individual to leave messages with others. Do not assume permission, even if they have been involved in the enquiry.
- Be especially mindful of leaving a message on a landline as the message may be picked up by family members, etc.
- Ensure that you have the right telephone number and have dialled it correctly!
- Keep voicemails brief and to the point. Do not leave a detailed a message or any specific information concerning the nature of the enquiry, etc. especially if it's of a sensitive nature!

Email Calendars

Good business practice is to share email calendars with colleagues so they can easily check your whereabouts, availability and arrange meetings. However, email calendar entries such as meeting requests and appointments often contain personal or confidential information in the subject line or body. Remember to mark any such items as 'private'.

Passwords



Create strong passwords with a minimum standard of:

- ✓ At least **eleven** characters in length
- ✓ Contains characters from three of the following four categories
  - Uppercase characters (A through Z)
  - Lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %) (*Please note, '£' cannot be used*.)

Avoid weak passwords:

- ✗ Do not use your login (user ID) name in any form (as-is, reversed, capitalised, doubled etc.).
- ✗ Do not use your full, first, middle or last name in any form.
- ✗ Do not use your spouse's or child's name.
- ✗ Do not use personal information about yourself or family members that can easily be obtained about you. This includes generic information such as, vehicle license plate number, telephone number, birth date, the name of the street you live on, and so on.
- ✗ Do not use a password that contains all digits, or all the same letters.
- ✗ Do not use days of the week, months of the year, seasons of the year, sporting teams
- ✗ Do not use adjacent keys on the keyboard like "qwertyui".
- ✗ Do not use consecutive letters or numbers like "abcdefgh" or "123456789".
- ✗ Do not use a well-known abbreviation e.g. RCTCBC.
- ✗ Do not contain obvious substitutions e.g. '$' for 's', '@' for 'a', '1' for 'I' etc.
- ✗ Do not use the same password for all systems.

Protect passwords at all times:

- ✗ Never reveal your passwords to anyone.
- ✗ Never let anyone else access your account.
- ✗ Never write your passwords down or store them where they are open to theft.
- ✗ Never store your passwords in a computer system without encryption.
- ✗ Never use the 'remember password' function on a shared of public device.
- ✓ Beware of someone looking over your shoulder when entering your password.

For more information see Password Management Standard

Locking your device

An unattended device may provide an opportunity for unauthorised access.

Whether you are working in an office, at home or at a meeting, get in the habit of locking your device every time you leave it unattended. It only takes a couple of seconds and is one of the most effective ways of keeping the information stored on your device secure.

Control, **Alt** and **Delete** before you leave your seat!

USB & Removable Media

USBs (or pen drives as they are more common known) and removable media devices are a convenient way for Members to access personal and business information on the go. However, due to their portable nature these devices carry greater security risks than other ICT devices.

As they are small, users tend to carry them in their pockets, handbags or leave them lying around on their desks etc. As such they are often mislaid, lost or even stolen.

Top Tips:

- Should you wish the save information to a removable media device such as a USB you must ensure that the device is encrypted. Should you wish to purchase an encrypted USB please contact the Councils Monitoring Officer who will arrange this for you.
- Create strong password for the device and keep them safe and secure.
- Ensure the device is properly removed from you PC, laptop or tablet after you've finished using it.
- Store the device securely when not in use.
- It is not recommended that master copies of data are stored to USB's. USB's are not backed up and in the event the device becomes corrupted ICT will not be able to restore the data for you.
- If someone gives you a USB to view or uploaded information ensure that it's from a trusted source. USB's are susceptible to viruses and a seemingly harmless USB has the potential to trigger a cyber-attack. If in doubt as the individuals to provide you with the information via another source (e.g. email) or contact the ICT Service Desk who will download the data for you.

Section 9:
Personal data breaches

Personal data breaches

This section outlines what responsibilities the Council and Members (in relation to casework) have 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.

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

Personal data breaches when undertaking Official Council duties

What should I do if I encounter a personal breach?

Should you encounter a potential, suspected or actual breach of personal data you must report the matter immediately to the Council's Monitoring Officer, who will report the matter to the ICT Service Desk and the Information Management team on your behalf. 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 Information Management team 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.

Personal Data Breaches - What I need to know:

- Know how to recognise a personal data breach.
- Know how to report a personal data breach
- Familiarise yourself with the Procedures for reporting information security incidents and events.
- Unsure if something constitutes a personal data breach? Report it anyway just in case.
- In the event of a breach, support the Councils Morning Officer and Information Management team with their investigation and work with them to put things right and stop the same thing happening again.

Personal data breaches when undertaking casework

Who is responsible for undertaking the investigation?

If the personal data breach relates to casework, as Data Controller, it is the Member's responsibility to investigate the breach and where required to notify the ICO and/or the individual who has been affected by the breach.

How should a Member investigate a personal data breach?

The following suggests the key steps that may be taken by Members when investigating a breach. Alternatively, the Member may contact the Council's Monitoring Officer who, guided by the Information Management team, can either undertake the investigation on the Member's behalf or support the Member in undertaking the investigation themselves.

- **Step 1** – Establish key facts – what went wrong, nature and sensitivity of the information, who is affected, how they are affected, what are the risks?

- **Step 2** – Contain the situation.

- **Step 3** – Decide if the matter needs to be reported to the ICO.

- **Step 4** – Decide if the individual whose personal information has been compromised need to be informed.

- **Step 5** – Identity measures to stop or reduce the risk of the same thing happening again in the future.

- **Step 6** – Document the breach.

- **Step 7** – Ensure any recommendations / actions are implemented.

Section 10:

Information Rights

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.

Subject Access Requests for personal data held by the Council that relates to Members official Council duties

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 Information Management team by email (where possible). Upon receipt of the SAR, the Information Management team 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 Information Management team 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.

For more information see Procedure for handling requests from individuals for their personal information.

Subject Access Requests for personal information relating to casework

Who is responsible for responding to a SAR?

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 Monitoring Officer who, guided by the Information Management team, 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.

The following guidance has been published to support Council Officers in responding to Subject Access Requests. Whilst the guidance is aimed at Officers, it content may also be useful for members when responding to SAR's.

Procedure for SAR Co-ordinators on dealing with requests from individuals for their personal information.

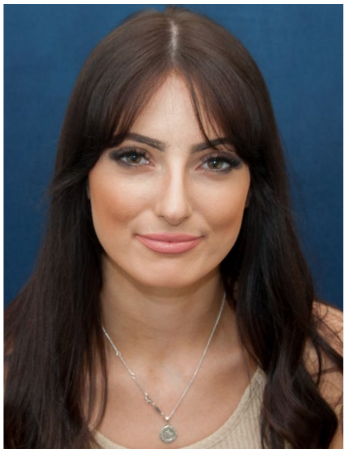
Section 11:

Help & Support

Help & Support

Should you require any information, support or guidance on any data protection matter please do not hesitate to contact a Member of the Information Management team.

Louise Evans
Data Protection & Improvement Officer
louise.evans@rctcbc.gov.uk



Jessica Colley
Deputy Data Protection Officer (Council)
jessica.colley@rctcbc.gov.uk

Sharon Langley
Deputy Data Protection Officer (Schools)
sharon.e.langley@rctcbc.gov.uk

Information Management

☎ 01443 562289

✉ Information.management@rctcbc.gov.uk

ℹ Inform > Support Services > Information Management

Useful links:

- 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 MP's correspondence
- ICO Disclosure of personal information by local authorities to councillors
- ICO Guidance on political campaigning
- ICO Guide to the GDPR.

Document Approvals

This document and subsequent revisions require the following approvals:

1. Overview & Democratic Services Committee (initial document only)
2. Democratic Services Committee

Version Control

Version No	Date Approved	Valid From Date	Valid To Date	Changes Made
1.0	TBC	TBC		Handbook launch.