RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

HOW TO GUIDE –
TRANSFERRING PERSONAL INFORMATION

Version: 3

Document Information	
Version:	3
Status:	FINAL
Date:	2nd December 2025

Contents

How to Guide: Transferring Personal Information

1. Introduction

During our working day, we routinely transfer personal and confidential information as part of our roles. This may involve sharing information internally, for example by sending details to a colleague or another department, or externally when corresponding with citizens, customers, clients, service users, or partner organisations.

When transferring personal or confidential information, by email, phone, post, or other means, mistakes can happen. Communication errors are a leading cause of data protection and confidentiality breaches in the UK. This guidance explains the risks and offers practical steps to reduce them, helping you share information safely and appropriately to protect individuals and the Council.

This guidance applies to all Council employees, agency staff, trainees, individuals on work placements, contractors, elected members, and anyone working for or on behalf of the Council (whether temporary or permanent) who handle Council information. It covers all methods of transferring information, whether internal or external, and whether the information is in electronic, paper, or any other format.

2. What is Personal and Confidential Information?

We use a wide range of information about our citizens and service users to deliver Council services. This information is likely to include personal details such as names, addresses, contact information, and other data that can identify someone. Personal information can be held in many formats, including paper files, electronic records, photographs, and audio recordings.

Confidential information also includes any data that is not intended for public disclosure. This might be commercially sensitive information, internal Council documents, financial records, draft reports, or details about Council operations, staff, or service users. Even if it does not identify an individual, confidential information still requires careful handling due to its sensitive nature.

3. Why is it Important to Safeguard This Information?

Safeguarding personal and confidential information is essential for several reasons:

- **Legal:** The Council is required by law (including the UK General Data Protection Regulation and the Data Protection Act 2018) to protect personal data and ensure it is handled securely.
- **Ethical:** Citizens, service users, and colleagues trust us to handle their information with care and respect.
- **Reputational:** Data breaches can damage the Council's reputation and erode public confidence in our services.
- **Financial:** Serious breaches can result in significant fines and costs for the Council.

4. Common Risks When Transferring Information

Transferring information, whether by email, post, secure portal, or in person, always carries some risk. The level and type of risk depend on the method you use, the sensitivity of the information, and how carefully you follow good practice.

Some methods, like email or post, are quick and convenient but can easily result in mistakes if details aren't checked thoroughly. Others, like secure portals, are designed to reduce risk but still require careful use.

Typical risks include:

- **Sending information to the wrong person** (for example, by email, post, or handing over in person without confirming identity)
- **Using insecure methods to transfer sensitive data** (such as unapproved websites, standard email for confidential documents, or fax)
- **Sharing more information than is necessary** (for example, including unnecessary personal details or entire files when only part is needed)
- **Failing to verify the identity of the recipient** (especially over the phone or in person)

Being aware of these risks and following the guidance in this document will help you choose the safest method and avoid common pitfalls.

How to Guide: Transferring Personal Information

1. Deciding the Best Way to Transfer Information

Before you transfer personal or confidential information, it's important to pause and consider the best way to do it. In some cases, you will need to make a decision yourself, based on the circumstances and the sensitivity of the information. In other cases, there may be a specific service protocol or procedure that you are required to follow for transferring certain types of information, always check if there is a relevant protocol in place for your service area.

The method you choose should balance the need for efficiency with the need for security. Here are some key things to think about:

- **How sensitive is the information?**
  The more sensitive the information (for example, health details, financial data, or confidential Council business), the more secure the transfer method should be.

- **How quickly does it need to get there?**
  Sometimes speed is important, but security should never be overlooked. If a secure method takes a little longer, it's usually worth the wait.

- **Who are you sending it to?**
  Are they a colleague, a partner organisation, or a member of the public? Are you sure they're the right person and entitled to receive the information?

- **How much information are you sharing?**
  The more you send, the greater the risk if something goes wrong. Large volumes or bulk transfers may need extra safeguards.

- **What could go wrong?**
  Think about the risks, could the information be lost, sent to the wrong person, or accessed by someone who shouldn't see it? Communication errors, such as sending information to the wrong recipient or using an insecure method, are among the most common causes of data breaches.

Always choose the most secure method that's practical for your situation.
If you're ever unsure, check with your line manager or the Information Management team before you send anything.

2. Transferring Information by Email

Email is widely used for sharing information, but it's also one of the most common sources of data breaches. Taking a few extra moments to check details before you send can prevent mistakes and protect both individuals and the Council.

1. Checking Recipient Email Addresses

- **Always check that contact details for service users, citizens, clients, or partners are current and correct.** Don't rely on old records or previous emails, people's contact details can change frequently.

- **Take extra care when manually typing an email address.** Even a single missing letter or digit can result in your message going to the wrong person.

- **Be cautious when selecting recipients from the global address list.** Many people have similar or identical names. Always check job titles, departments, or other details to make sure you've chosen the right person.

- **Double-check the recipient's email address, especially if using auto complete.** It's easy to select the wrong contact by mistake.

2. Attachments

- **Be careful when selecting the file to attach.** Make sure you are choosing the correct document for the intended recipient.

- **Review the content of the document in its entirety before sending. Confirm that you are only sharing the information that is necessary.** For spreadsheets, check for hidden rows, columns, or sheets that may contain sensitive or irrelevant data, and remove them if not needed.

- **Label attachments clearly and appropriately.** Avoid generic file names like "document1.pdf." Use descriptive names that make it clear what the document is.

- **Once attached, open the file from your email draft to double-check it's the correct and final version.** This helps prevent mistakes, such as sending the wrong file or an out-of-date version.

- **Limit the amount of personal or confidential information in the body of the email.** Use an attachment for sensitive content whenever possible.

- **If sending sensitive information, consider adding an extra layer of protection by password-protecting the attachment, especially for external emails.** This is good practice for particularly sensitive or high-risk information. Send the password separately (for example, in a follow-up email or by phone).

3. Bulk Emails, Protecting Email Addresses, and Using BCC

- **Never use standard email to send bulk messages to large groups of service users, citizens, or external contacts.**
  For example, this includes sending newsletters, marketing updates, or important announcements to all customers, citizens, or service users. As a rule of thumb, if you need to contact 75 or more recipients, do not use conventional email. Bulk communications increase the risk of data breaches, such as exposing recipients' email addresses or sending information to the wrong people.

- **If you need to send a bulk email, contact the Digital Improvement Office first.** They can advise on suitable, secure solutions for bulk communications that protect personal information and comply with Council policies.

- **When emailing multiple recipients who should not see each other's email addresses (for example, service users or external contacts), always use the BCC (blind carbon copy) field.** This helps protect privacy and prevents accidental disclosure of contact details.

- **If you're unsure whether to use BCC or need advice on bulk communications, check with your line manager.**

4. After Sending

- **Where possible, request a delivery and read receipt** so you know the email has arrived and been opened.

- **Monitor for any bounce-back or undeliverable messages** and follow up as needed to ensure the information reaches the intended recipient.

- **If you realise you've made a mistake** (for example, sent information to the wrong person or attached the wrong file), report it immediately following Council procedures. Acting quickly can help limit any potential harm.

3. Transferring Information by Letter – In Person or by Post

Sending information by letter or post is sometimes necessary, but it carries its own risks, such as loss, theft, or delivery to the wrong address. Taking care at each step can help keep information safe.

1. Preparing the Information

- **Check the address is current and correct.** Don't rely on old records, confirm the recipient's address, especially for service users, citizens, or external partners.

- **For citizens or service users:** Use their full name (not just initials) and complete address, including the postcode. Clearly mark the envelope for the intended recipient, especially when sending confidential or sensitive information.

- **For partner agencies or organisations:** Include the full name of the company or organisation. If the letter is for a specific person, add their full name and job title. Double-check where to send the letter, as the intended recipient may be based at a different location from the main postal address. Clearly mark the envelope for the intended recipient to ensure it reaches them directly or is routed to the correct place for receipt.

- **Double-check the contents before sealing.** Make sure you are sending the correct documents and only what is necessary.

- **If sending sensitive or confidential information, use a double envelope**. Place the documents in an inner envelope marked "Private and Confidential," then seal that inside an outer envelope. This extra step helps protect the information if the outer envelope is damaged or opened in transit and ensures that only the intended recipient sees the sensitive contents.

- **Include a return address on the envelope.** This allows undelivered mail to be returned safely to the Council.

2. Sending the Information by Post

- **Choose a secure delivery method if needed.** For particularly sensitive or high-risk information, consider using a tracked delivery service or a trusted courier service so you can monitor and confirm receipt.

- **Ensure the envelope is robust enough to withstand transit.** Use an envelope that is strong and secure enough to protect the contents from damage or accidental opening during delivery, especially for sensitive or confidential information.

- **Be mindful of where outgoing mail trays are located.** Mail trays should not be placed on reception counters or in public areas where someone could remove or tamper with the mail. Always ensure that outgoing post is kept in a secure area until it is collected for delivery.

- **Keep a record of what was sent, to whom, and when.** This can be helpful for tracking, audit purposes, or in the event of an incident.

- **Request confirmation of receipt where required** for important or sensitive documents and/or check mail tracking.

- **Monitor for undelivered or returned mail.** If a letter is returned or you become aware it hasn't arrived, follow up promptly and report any potential data loss or breach according to Council procedures.

3. Delivering the Information in Person

- **Go straight to the location where possible and secure the document in transit.**

- **Where possible, hand the letter directly to the intended recipient.** This is the most secure way to ensure the information reaches the right person.

- **If you need to post the letter through a letterbox and there is no answer, only do so if you are confident, it is the correct address.** Double-check the address details before posting, especially for sensitive or confidential information, to avoid accidental disclosure.

Bulk Mailings

Where you need to send information to a large number of individuals (for example, all service users, citizens, or customers), it is strongly recommended that you use the Council's Print/Mail services. This approach is not only more secure but also supports efficiency and cost savings.

When using the Print/Mail service, make sure you specify how documents must be handled and protected, especially if they contain personal or confidential information. For more information or to arrange a bulk mailing, contact the Business Support Unit.

4. Transferring Information by Telephone

Sharing personal or confidential information by phone can be quick and convenient, but it carries risks, especially if you cannot be sure who you are speaking to. Always take steps to confirm identity and protect information.

1. Outbound Calls (When You Are Calling)

- **Confirm you are speaking to the correct person before sharing any personal or confidential information.**
  This is important because someone else could answer the phone (for example, a family member, colleague, or receptionist), or you may have misdialled and reached the wrong number.
  - Ask the person to confirm key details (such as their full name, address, or reference number).
  - If you reach someone else, do not disclose any information, simply leave your name, department, and a request for the intended recipient to call you back.

  Do not leave personal or confidential information in voicemail messages. Only leave your name, department, and a callback request. This is especially important for landlines, where messages could be accessed by others in the household or workplace.

- **Make sure your conversation cannot be overheard.** Avoid discussing sensitive information in open offices or public areas.

2. Incoming Calls (When You Receive a Call)

- **Always verify the identity of the caller before sharing any personal or confidential information.**
  - For service users, citizens, or clients, ask for details only they should know (such as full name, address, date of birth, or a reference number).
  - For partner organisations or agencies, ask for their full name, job title, and organisation. If you don’t know them, take their main switchboard number and call them back to confirm their identity.

- **If someone is calling on behalf of another person, check that you have appropriate consent or authority to discuss the matter or share information with them.** Never assume permission, always confirm before proceeding.

- **Never share information if you are unsure about the caller’s identity.** Politely explain that you need to verify their details before proceeding.

5. Transferring Information via Secure Portals or Web Uploads

The Council increasingly uses secure online systems, sometimes called “secure portals” or “web uploads”, to share personal or confidential information. These are special websites or platforms designed to keep information safe when it’s shared between Council staff and partner organisations. For example, you might use a secure portal to send documents to another public body, upload files for a contracted service provider, or share information with a partner agency.

When sharing information with citizens or service users, some Council services use Egress, a secure email and file transfer system, for regular sharing of sensitive or confidential information. Access to Egress is provided where there is a business need. If your service requires this, your Line Manager should contact the ICT Service Desk to find out more.

While these systems are often safer than email or post, it’s still important to follow good practice to make sure information only goes to the right people and stays protected.

Good Practice for Secure Portals and Web Uploads

- **Use only Council-approved secure portals or systems.** Never upload personal or confidential information to unapproved websites or platforms. Sometimes, you may receive a link from a partner organisation or agency requesting information to be uploaded and providing a web link. **Never upload information unless you are absolutely sure the upload mechanism is approved by the Council and the request is genuine.** If you have any doubts about the legitimacy of the request or the security of the portal, verify with your Line Manager, the Information Management team, or ICT before proceeding.

- **Check the website or portal is secure.** Look for “https://” in the address and any Council or partner organisation branding.

- **Verify the recipient’s access.** Make sure only authorised individuals can access the information you are uploading or sharing.

- **Follow any specific instructions for uploading or sharing files.** Some systems require you to set permissions or notify the recipient separately.

- **Double-check the information before uploading.** Ensure you are sharing the correct files and only the information that is necessary.

- **Keep a record of what was uploaded, to whom, and when.** This can help with tracking and audit purposes.

If you are unsure about the security of a portal or have any concerns, contact the Information Management team or ICT for advice before proceeding.

6. Transferring Information by Fax

Fax is no longer permitted for transferring personal or confidential information within the Council. This is because fax machines present significant risks to information security. Faxes can easily be misdialled, resulting in sensitive documents being sent to the wrong recipient. Additionally, fax machines are often shared or located in public or communal areas, meaning that documents can be accessed by unauthorised individuals or even left unattended. There is also no reliable way to confirm who receives or collects the faxed information, and fax does not provide adequate security or audit trails for sensitive data.

If you are ever asked to send personal or confidential information by fax, do not proceed. Instead, use one of the approved secure methods outlined in this guidance, or contact the Information Management team for advice.

7. Incident Reporting: If Mistakes Happen

Despite everyone's best efforts, mistakes can sometimes happen when transferring personal or confidential information. If you think information has been lost, sent to the wrong person, accessed by someone who shouldn't see it, or if you have any concerns about a possible data breach, it's important to act quickly. Prompt reporting allows the Council to investigate, support those affected, and take action to prevent further issues. It also helps us meet our legal obligations under data protection law.

What to do:

- **Employees, agency staff, trainees, individuals on work placements, and anyone working for or on behalf of the Council** (whether temporary or permanent) must report any potential, suspected, or actual information security incident or event immediately to:
  - ➢ Their Line Manager, and
  - ➢ The ICT Service Desk

  - **Elected Members** must report any potential, suspected, or actual information security incident or event immediately to the Council's Monitoring Officer, who will then notify the ICT Service Desk on their behalf.

If you are ever unsure whether something is an incident, it's always better to report it and ask for advice.

Version Control

Version No	Valid from	Valid to	Changes Made
1.0	30.06.2016	06.10.2016	Reformatted into procedure guide.
2.0	07.10.2016	01.12.2025	Amended to guidance.
3.0	02.12.2025		Full review to bring in line with current working practice and good practice