By answering this question you will understand how to share information safely and securely.

**We are all responsible**

You are responsible for looking after any information that you have access to. This includes how you share this information with colleagues and other organisations.

If you are responsible for a system (application) or a set of information (asset), it is your responsibility to ensure that the information you manage is shared appropriately, and in line with the service or project it is connected to.

For example, the London Borough of Hackney may seek to join up a local service with the NHS to better support residents. Before any information was shared with the NHS to get the initiative underway, it would be the asset/application owner’s responsibility to ensure a Privacy Impact Assessment (PIA) was completed. This would enable the asset/application owner to consider and address any privacy risks to resident’s personal information and to get advice from the Data Protection Officer.

**Sharing is often necessary**

Restricting information within the Council can sometimes be as risky as sharing it more widely. For example, this may lead to people collecting the same information twice, or information being stored in multiple places.

Likewise, there will be times when you need to share information with separate organisations, for example, to help with safeguarding. In cases like this, you are still responsible for the information being shared and will need to make sure appropriate controls are in place.

If in doubt, speak to the Information Management team for help.

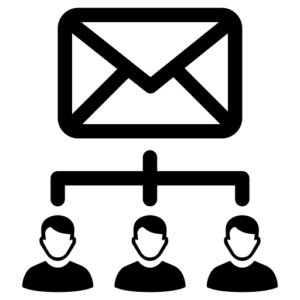
The examples below refer to sharing information in email, on the phone or in the post. However, the same principles apply to Whatsapp, texts, fax or even conversations or screens in open plan offices.

**Sharing with colleagues**

The most likely method of sharing information at work is via email, the phone or post. Here are some common mistakes that lead to information being inappropriately shared:

1. emails or letters being sent to the wrong person.
2. personal information being left on an answerphone, with no certainty of who will listen to that message.
3. long email chains with a growing list of recipients, who can all see the information shared earlier in the chain.
4. sending information to or from team inboxes, when that information does not need to be seen by the whole team.
5. information being left on a printer or copier.
6. including full names and other personal information in correspondence when initials or some form of omission might be more appropriate.
7. sending additional copies of documents that have already been shared, rather than referencing or sending a link to the master version.

If you are sharing information with colleagues or other departments, it's important the information is not used for a different purpose than was originally intended when it was collected. This is ‘purpose creep’: information used for a different goal than it was originally intended.



Think! Who really needs to see this email, and do they need to see all the information in the chain?

**Managing your colleague's access to information**

You should also take responsibility for checking that only those in your team have access to the information they need.

For example, there should not be anyone in your team who has access to your inbox or answerphone ‘just in case’. Where there’s a genuine need for you to access someone else’s inbox, or a shared inbox, you should ask IT for delegated access.

Do not share passwords.

Likewise, you should only copy emails to other members of the team if it is necessary for them to see that information. It is not appropriate to copy others in simply as a courtesy or because we want them to know we are working on a particular project or case.

**Sharing information securely**

You must always consider whether you are using the most appropriate channel for sharing information.

USB sticks or memory cards are not a secure way to store or share information. There is too great a risk that they will be lost or stolen.

Shared documents and correspondence must be stored in the Council’s filing systems such as Google Drive (with appropriate permissions). This is safer than emailing multiple versions of documents between two or more people.

Make it clear to your colleague that the information you are sharing is confidential. If you don’t want them to share the information more widely, state this clearly, on the document or in the email.

#### **Adding a classification marker to information**

Think about whether the information needs a classification marker.

There are two types of classification marker used at the Council: OFFICIAL and OFFICIAL-SENSITIVE.

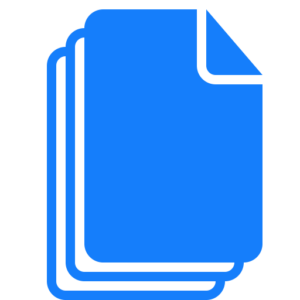
Any email, document or other record produced as part of your work for the Council is automatically classified as Official. You don’t need to put the word Official on the record, however.

Some types of information may need to be classified as OFFICIAL-SENSITIVE.

Examples include:

* very sensitive personal information (including information about vulnerable or at-risk people) where loss or disclosure could lead to significant harm or distress.
* large volume data (eg bulk sets of care or financial records).
* information about criminal investigations and legal proceedings that could compromise public protection or enforcement activities, or prejudice court cases.
* the most sensitive corporate information (eg organisational restructuring or negotiations, and major security or business continuity issues).
* policy development and advice to Council members on contentious and very sensitive issues.
* commercially or market sensitive information that might be damaging to the Council or to a commercial partner if improperly accessed.

If you are responsible for information that is OFFICIAL-SENSITIVE then you must make sure it is clearly marked with this classification.



All Council information is automatically OFFICIAL. You must decide if information you are responsible for needs to be marked OFFICIAL SENSITIVE

**Protect the information**

Use password protection for databases and documents where possible, or signed-for postal delivery if the information is in hard copy.

Email encryption and services such as Egress, help to keep email safe.

If the information has to be made available to a wider audience, or made public, then you must redact any personal information, or any other content that does not need to be shared more widely.

**Techniques to protect personal information for asset and application owners**

We must always use the smallest amount of personal data that will still allow us to achieve our goal. There are three useful techniques to consider when you need to share a document but want to avoid giving out the personal information they contain. These techniques can make it impossible or impractical to connect the personal information to an identifiable person.

#### **1. Redaction**

The process in which personal information has been erased from a document.

#### **2. Anonymisation**

The process of turning personal information into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

#### **3. Pseudonymisation**

Processing of personal information in such a way that it can no longer be attributed to an individual, without the use of additional information.

Anonymisation and pseudonymisation must be implemented in a way that does not enable anyone with extra information to identify the individual.

**An example of knowing when to redact**

The Council have been asked to publish a report as part of a response to a Freedom of Information request. The original report contains a large number of resident contact details.

In order to publish the report, the responsible department must remove the personal information.

This can be done by leaving the data in the document and using redaction software to remove the personal information. This should be a full removal that cannot be reversed, rather than simply highlighting in black.

This could also be done by deleting the data from the copy of the report. Care must be taken to make sure that it is fully removed and not possible to recover. If it is a spreadsheet it should be shared as a CSV to ensure that there is no hidden data.

**Subject Access Requests**

You may receive a Subject Access Request (SAR). It is important to understand what this is and who to refer it to.

Subject access is a common right and is most often used by people who want to see a copy of the information the Council holds about them. A member of the public can also request information about the reasoning behind any automated, computer-generated decisions.

SARs are managed centrally at the Council by the Information Management team. They may ask for assistance from you to locate the information and understand the context.

**Leavers policy**

When a member of staff leaves the Council, it is the responsibility of their manager to fill out a Leavers Form and follow guidelines on staff who are leaving. This is to ensure that access to Council systems is revoked and all devices returned.

If your staff member is moving to another part of the Council, you must fill out an e-mover form. This ensures they do not have access to any personal data they no longer need in their new role. Their new line manager will ensure that they have access to the systems they need.

**Tasks**

Basic

**Your experience of information being shared inappropriately**

Describe an example of when you have seen information shared inappropriately.

Was it in email, on the phone, or somewhere else?

What went wrong and why?

Intermediate

**Understanding how to share information in appropriate ways**

Describe two ways that you can ensure information is shared appropriately.

Advanced

**Knowing when a Subject Access Request might affect your work**

Give an example of the type of personal information you are responsible for, that may be subject to a Subject Access Request from a member of the public.