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.

**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.

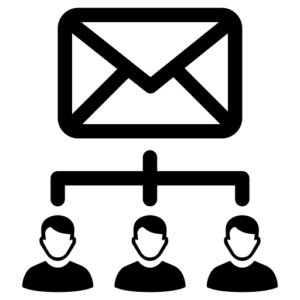
If in doubt, speak to the Information Management team for help.

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 overheard 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.



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 must take responsibility for checking that only those in your team have access to the information is only provided where it is needed.

In the same way that you are responsible for deciding when you no longer need to access information, and removing your access rights, 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 Hackney filing systems such as Google Drive. This is safer than emailing multiple versions of documents between 2 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.

Think about whether the information needs a classification marker.

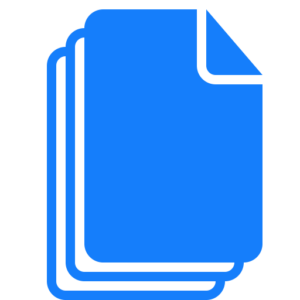
There are 2 types of classification marker used at Hackney Council: OFFICIAL and OFFICIAL-SENSITIVE.

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 must 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.

**Tasks**

Basic

**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

**Describe 2 ways that you can ensure information is shared appropriately**

Advanced

**Upload an example of a Word document in which you have redacted some information using the guide above.**

Note: please don’t share any personal information here, even if you have redacted it. You should either use a dummy document, or some information that is in the public domain