By answering this question you will understand how to:

* keep information safe.
* report a breach.

**We are all responsible**

You are responsible for making sure that all information you hold is kept secure.

It is important to understand:

* what makes a secure password.
* when it is appropriate to use a password.
* why we should use different passwords for locking down different information.
* how to safely share this information with other colleagues.

As part of your responsibilities for keeping information safe, you must think about where it is stored and about the devices you use to access it.

Devices include work laptops or phones, as well as personal devices: your own phone, tablet or home computer.

**Passwords**

A strong password is the key to keeping information safe.

Do:

* Use a strong complex password that includes: numbers, uppercase letters and lowercase letters and at least 8 characters
* Keep your fob or google authenticator safe
* Decline any prompts to ‘Remember Passwords’

Do not:

* Share your password with anyone
* Write your password down
* Use the same password for corporate systems as you do for personal ones
* Use easily guessed passwords (e.g. pet names)
* Use shared or public computers unless they are protected by an individual account that is used to access the computer with a password that only you have access to

For additional information, please visit here: [keep information and ICT equipment safe](http://intranet.hackney.gov.uk/article/3441/Keep-information-and-ICT-equipment-safe)

**Taking care of information in the workplace**

In the office it is important that everyone stores information in a logical and routine way. This helps:

* keep it in order.
* makes it easier to find.
* helps ensure you don’t keep information for longer than is necessary.
* make the information available to the right people at the right time.

For example if you have information saved on laptops, phones as well as hard copies of files in a desk drawer then collating it together may take some time.

This scattered approach to keeping information can also risk a breach of information.

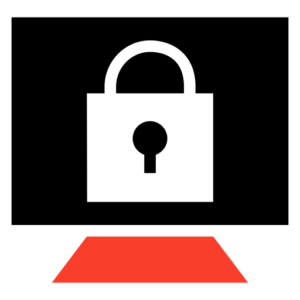
Files that have vague labelling or are stored in different ways are more likely to be shared mistakenly as email attachments or in hard copy.

Storing information on any device, whether that device belongs to the Council or is your own, is not recommended. Ensure you are filing information in the correct folders online, or archive the information appropriately. Please review the [intranet guidance](http://intranet.hackney.gov.uk/article/3441/Keep-information-and-ICT-equipment-safe) if you would like more information.

One of the easiest things to do to help take more care of information is simply to print less and encourage colleagues to do the same.

Assuming you’ve taken care of filing, you still need to pay attention to what’s going on around you in the office. Ensure that you:

* lock your screen when you leave your desk, even if you only plan to be gone for a few minutes.
* don’t tolerate tailgaters when entering your building (people following you closely through security barriers or locked doors).
* keep a clear desk and be aware of what is always on your screen for others to see. Sometimes it may be necessary to work on a document in a different location where you are not overlooked.
* be cautious about clicking on links sent to you in emails, particularly if the website you are led to asks for login details. Even if you recognise the name of the sender, it may be advisable to call them and check that they have sent that email, before you click the link.



Always lock your screen when leaving your desk

**Taking care of information on the road**

The main difference between keeping information safe on the road, compared to in the office, is that there’s even greater need to make sure your mobile devices are secure and up-to-date.

IT will deliver automatic security updates to your work phone and laptop, but you must ensure these updates are not ignored. Likewise, it is also your responsibility to keep your personal device updated and secure.

You can help keep information on mobile devices safe by only taking them with you, when you need them. The rest of the time, keep phones and laptops locked somewhere close-by, but safe: a locked car boot if your job involves driving, a desk drawer or a secure compartment of a bag.

Stay alert to who can see the information on your screen if you are working in a public place and don’t leave it unattended.

If you lose a work-issued phone or laptop, or a personal device through which you access work information, then you must inform IT immediately.

**Reporting an information breach**

A breach occurs any time information is lost, stolen or shared with the wrong person or people.

A breach might include:

* emailing a resident’s file to the wrong department.
* sending private information to the wrong email address.
* realising that a database or contact list cannot be found.
* lost IT equipment.

For example, the London Borough of Hackney might receive a number of complaints about the same issue, from individual residents. If you were to respond to all the residents in the same email, putting their email addresses in the To field, so they could identify each other, that would be a breach of information. In this example, you should send separate emails to each resident, or put all their addresses in the BCC field.

If you discover a breach, or you are not sure if the incident actually counts as a breach, you must report it immediately, even if you don’t have all the details. You can report a breach using the 'security incident or data breach' link on the intranet.

Failing to report a breach quickly at the Council can count against you, as misconduct.

It is the Council's duty to report a breach within 72 hours. The Council may also be penalised by the Information Commissioner’s Office. If the breach is considered to be over a certain threshold of severity, we also have to inform the people affected by the breach.

**Privacy by Design**

Privacy by Design means thinking about privacy and data protection from the outset, when designing a new process, or piece of technology.

For example, the Council may decide to redesign the process on their website for members of the public to report fly tipping. The team responsible for the website design and content would need to ensure they had considered how personal information was to be collected and protected at the outset of the redesign process.

You need to ensure that you consider privacy at the initial design stages and throughout the development process of any new products, processes or services that involve processing personal information. A Privacy Impact Assessment (PIA), also known as a Data Protection Impact Assessment, is a tool that must be used for projects meeting a certain threshold.

Even if your project doesn’t meet the threshold to require a PIA, you should still build privacy and security into the design and implementation.

You will also need to think about any services you deliver with a third party. You will need to complete a PIA if they are moving their platform or otherwise changing the way they process the information.

Contact dataprotection@hackney.gov.uk if you need any advice about this.

**Tasks**

Basic

**Create a strong password**

Give an example of a strong password using one of the methods described above.

Intermediate

**Take more care of information every day**

Describe two examples in your daily routine where you can take better care of information.

Advanced

**Incorporate privacy by design**

Name a process or development in your department that would need to incorporate a privacy by design approach.