

Tips for keeping and using personal data

First of all, what is 'personal data'?

- Personal data is information about someone that can be used to identify them.
- Under GDPR, personal data is split into two categories:
 - 1) **personal information**, which could be gathered from another source.
For example, name, address, phone number, etc.
 - 2) **sensitive information**, which would have to have been given by the person themselves. For example, gender, sex, religious belief, medical history, etc.

When you are using or storing personal data, always:

- **Dispose of printed personal data or confidential information securely**, such as by shredding it.
- **Find somewhere you cannot be overheard** to hold meetings or telephone calls if you need to talk about personal data or confidential information.
- **Check whether people around you can see your computer screen.**
Can they see any personal data that they shouldn't?
- **Restrict other people's access to personal data.** Lock your computer screen and don't leave personal data or confidential information lying around on a desk or anywhere else insecure.
- **Keep your passwords private.** Never write them down or share them with anyone outside of your group.
- **Make sure that you know who you are sharing personal information with.**
Check that you are not selecting 'reply all' if you do not need to; check email threads for personal data or confidential information before forwarding on to anyone; and clearly label post that is 'private and confidential'.



- **Ask yourself, “Do they really need all this information?”** when forwarding emails with personal data or confidential information, including any attachments.
- **Use strong passwords** for all of the systems you use for work, and don't use the same password twice.
- **Use password protection** when emailing attachments that contain personal data or sensitive information.
- **Challenge group volunteers** if you have been sent personal information and you are not sure why. You should never have access to personal data without an explicit purpose. If this happens, ask why the personal data has been given to you. If there is not a valid reason, let them know that you think there has been a data breach and report it.

And never:

- **use an email distribution list to circulate personal data or sensitive information,** unless every person on the list needs the information.
- **share other people's personal data online.**

Finally, an easy rule to follow is:

- Handle all personal data as if it is your own – don't leave it where others might be able to see it.

