Data protection top tips

Time is of the essence

As soon as you notice that personal data has been lost, stolen or made available to the wrong people, report it to networks@rsc.org with as much information as possible, even if you're not completely sure there's a reason to be concerned. We have 72 hours to report breaches. Refer to our GDPR guildelines for our member networks to learn more.

Look after the data you have access to

Before we are able to provide you with data, you will need to complete our 'Data compliance form'. Keep files containing personal data in a secure place. Lock your PC (Windows key+L) and don't leave lapto Lock yock yock yock yock G m

Consider whether you have the right to process an individual's personal data

There are six lawful bases for processing an individual's personal data:

Consent:
the individual has given clear, consent for us to use their data for this specific purpose

Contract:
processing is necessary to fulfil the terms of our contract with this individual

Legitimate interests:
It is in our legitimate interests to process the data, providing this doesn't override the interests of the individual

**Only use data for the purpose it was collected in the first place.**

Don't use data for different purposes without checking with the Networks team.

Personal data records should be kept accurate and up to date.

Consider setting up a scheduled process to keep the personal data you request up-to-date. Think about the reason for which the data was collected, and the lawful basis for doing so. This will help you decide whether the data should be updated, anonymised or even deleted, when you review it. If you would like to contact all members within your network, talk to the Networks Team about how this can be done in a GDPR compliant way.
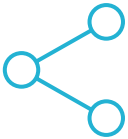
If you are thinking of sharing personal data outside of your committee, ask yourself:

"Do I have permission to share this data? Is the recipient GDPR compliant? Have I signed the RSC's data processing agreement this year? Should I password-protect the data?"

If you do have to share personal data, limit the risk by sharing links to shared files or password-protecting attachments. Remember, always send passwords separately.

If you need to send personal data outside the RSC, consult with our Networks team to create or amend a contract with the third party so it provides the right level of safeguarding for any data we share with them.

Keep it or delete it

Ask yourself: "Do I need this data?"; "Can I minimise/anonymise the personal data?"; "Would I be able to justify keeping this data if the ICO asked about it?"

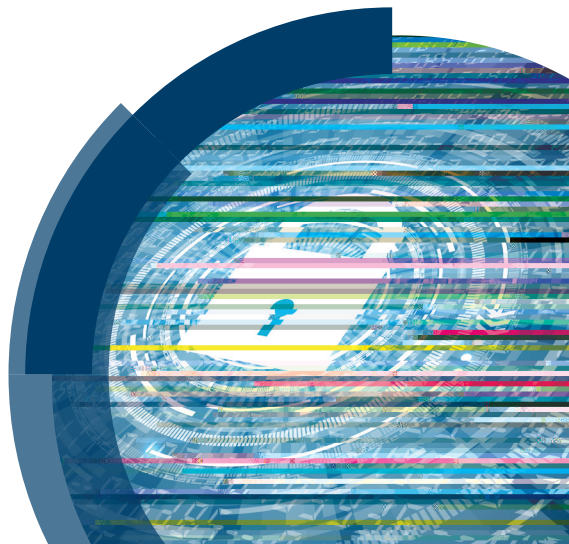Refer to our Data Retention flowchart to help you decide.

If you no longer need it, shred any documentation that contains personal data or place it in secure confidential waste bins - don't put it in recycling. If it's a digital file, delete it and make sure it's deleted from your recycle bin too.

Get GDPR-savvy

It's your responsibility to familiarise yourself with the GDPR. Our 'GDPR guidelines for our member networks' contains more information. It can be found at **rsc.org/formsdoc_men s**. Also check out the ICO's 'Guide to the General Data Protection Regulation 'GDPR' at ico.org.uk. Remember, if you have any questions, you can always contact the Networks team, who will support you.

Need help deciding what to do with personal data? Flip this card to see our data retention flowchart

Refer o he 'GDPR g idelines for o member ne orks' on o in rane for more informa ion

START

Is there a

YES   NO

YES | NO | YES

                NO   YES

                                NO

                                        YES

END