

You're responsible, so beware!



Everyone is responsible for protecting personal data. Find out what steps you should be taking.

Personal data can be stored digitally or physically. Ensure that you are processing, sharing and storing personal data safely and in line with the College's standards.

Protecting personal data is everyone's responsibility, not just an ICT or compliance issue.

For further advice on responsible data handling or help with any aspect of General Data Protection Regulation, please see the website or contact Data Protection Officer, Robert Scott:
robert.scott@imperial.ac.uk

www.imperial.ac.uk/data-aware

Imperial College
London

BE PERSONAL DATA AWARE



Your guide to responsible data handling

Always handle it with care



Treat other people's personal data as you would wish your own data to be treated.

Make sure the right physical and technical measures are in place to protect it. It is everyone's responsibility to ensure that any personal data provided to the College is not misused.

Make yourself aware of the relevant guidance, codes of practice and policies. If you are unsure of how this affects your role, please get in touch with the team.

Think twice before you share



Only share personal data when it is appropriate to do so.

Take measures to protect any data you share, especially if you are sending data outside the College. Consult our guidance on how to share data securely.

Before you send or share any data, check that you have the correct measures in place. This could be a Data Sharing Agreement, Data Processing Agreement, other contractual measures, as well as secure transfer. Template agreements are available on the website.

Only process when it's fair



You need to have a valid lawful basis in order to process personal data, and the subjects of the data should be aware of what you are doing with it.

Check whether your processing is covered by one of the College's privacy notices. Whenever personal data is directly collected, the individual must be informed about the collection and use of their data.

If you receive personal data from a third party, you must contact the individuals with information about how their data will be used within one month except for in very limited circumstances. Check the current College Privacy Notices, and if these do not cover your data processing, a new notice will be required.

Should that data still be there?



Only keep personal data for as long as you need it, then destroy it safely and securely.

You can check whether it is time to dispose of personal data – and other types of data – by referring to the College's Retention Schedule.

Legally we cannot keep data longer than we need it. You should ensure a suitable retention approach is applied and adhered to. For more guidance, contact the Archives and Corporate Records Unit.

Human error is not rare



Many data breaches – leaking or losing data – happen accidentally.

If you think a breach may have occurred, report it immediately using the notification of security breach form.

Consult the College's data breach plan and do not keep a potential breach to yourself. By reporting the breach, steps can immediately be taken to manage the situation. The College may have to report the incident to the regulator within 72 hours from the time a breach is identified, so recognising and reporting such events is crucial.