# Data Protection and Security for Undergraduate and Postgraduate Taught (Master and PsychD) Students Projects

Students who use personal data as part of a research project to fulfil educational requirements need to follow this guidance provided by the University's Information Compliance Unit. Supervisors of students are responsible for ensuring that students follow this guidance.

This includes the collection of names and email addresses, even if they are only collected to recruit participants.

**What is data protection?**

The General Data Protection Regulation and the Data Protection Act 2018 protect the rights of individuals when you process personal data about them. Processing can be anything that you do with data, including collecting it, holding it, analysing it, merging it with other data you hold or destroying it.

The definition of personal data is complex. The legislation defines it as "information that can be used to either directly or indirectly identify a living individual". It is easiest to assume that all information about a living, identifiable individual is personal data. This includes opinions made by or about an individual, and also includes names and email addresses.

**Why should you care?**

When you carry out a project as part of an educational requirement you are processing personal data on behalf of the University of Surrey. This means you need to comply with the **University Data Protection Policy** .

In most cases, both you and your supervisor must ensure the use of personal data is in accordance with these requirements.

**How do you do that?**

There are **ten main steps** that you must take ensure that you comply with data protection requirements:

1) Before you start a research project, you must carefully consider what personal data you need to collect for your project.
   - You must discuss the project and the data you intend to collect with your supervisor to agree the smallest amount of data that is needed to meet the aims of your project.

2) If you are using data relating to human participants, you must complete the University's self-assessment for governance and ethics (SAGE).
   - As part of this self-assessment you will be asked to declare the use of personal data. You must declare this, even if you are collecting very small amounts of personal data.

3) Once you have decided on the purposes of your research you must ensure these are declared on SAGE. You must only use the personal data you collect to meet these declared purposes.

   - Any personal data collected must not be accessed, shared, copied or otherwise processed in any way other than in line with the purpose of the project.
   - You must not collect or keep data that isn't necessary for your research.  If possible, remove names and other identifying information.

4) You must give a clear explanation of what you are going to do with the data to the people who are participating in your research.

5) Ensure that all personal data, including opinions, is recorded accurately.

6) Try and respond to requests from a participant to update or delete data about them that you have collected.
   - If you are not able to destroy or update data when requested, then record this alongside other project information.

7) Try not to transfer personal data outside the European Economic Area (EEA).  This includes accessing it or making it available outside the EEA.
   - If you become aware of a need to transfer personal data outside the EEA, then you must ensure it meets required safeguards for international transfers of personal data.  Contact the RIGO team or the data protection team for advice on this if needed.

8) Contact the RIGO team or email databreach@surrey.ac.uk as soon as you realise that there has been a breach of security, or that personal data has been accessed or shared with anyone who should not normally have access to it.
   - If data is shared with or accessed by unauthorized people or organisations then we will have to investigate.  Please help us by telling us anything that can help with this investigation when we ask you.

9) Don't disclose any personal data to anyone except to the individual whose data it is.
   - If you are asked for personal data, either by a third-party organization or an individual then contact the RIGO team without delay.
   - We may have to respond to requests for information from individuals whose data is being processed.  Please help us by sharing with us any information we ask for to respond to these requests.

10) Once you have completed your studies you must securely destroy all personal data.
   - This includes shredding any paper or hard copies of data.
   - If your research is continuing, you can transfer the relevant personal data to your supervisor.

**Security of data**

When you are processing personal data, or any other data that would be considered to be confidential, you must follow these security steps.  This helps to ensure that the confidentiality, integrity and availability of data is maintained.

1. Use your University email account for any correspondence with participants or when you are sending/receiving personal data related to the research project.

  - You must never use your personal email account for this.

2. Do not use public computers for research activities.  This includes communicating with participants such as sending emails

3. You can use personal device(s) to carry out research activities, as long as the following security measures are met:
   - Use of a firewall to secure connections to the Internet, especially where publicly-accessible Wi-Fi networks are being used.
   - Up to date anti-virus protection allowing regular and as-needed scans of the system.
   - All devices should be protected by a suitably strong password.
   - Use of up to date software and device operating systems.
   - Devices on which data is being stored are kept physically secure.

4. Avoid using removable storage devices (external hard drives, USB sticks etc).
   - If you can't avoid using them, you must ensure the device is encrypted, and that any documents you create or access on it are password-protected.

5. Limit the work you do in public areas.
6. Lock any devices containing information and data relating to your project when you aren't using them.
7. Try not to make additional copies of information - printing, saving duplicates, etc.
8. Avoid using any cloud storage facilities, apart from those provided by the University IT department.
   - If you use University cloud storage, then make sure you don't access data outside of the EEA.
   - If you are asked to use alternative cloud storage, contact IT Services to check if it is approved for use.

If you require any help or clarification of the above points please do not hesitate to contact RIGO (rigo@surrey.ac.uk) or the Information Compliance Unit (dataprotection@surrey.ac.uk).