General Data Protection Regulation (GDPR) briefing for managers – what you need to do

The General Data Protection Regulation (GDPR) comes into effect from 25 May 2018 and will govern how we collect, process and retain personal information in future.

'Personal information' is any information from which an individual can be identified, either directly (such as by name) or indirectly (such as from an ID number). Much of the personal information we hold relates to employees, students and research subjects. But we also hold a great deal of information about individuals who engage with us in other ways, such as contractors and people who attend events. The personal information we hold covers a wide spectrum, from relatively routine (such as contact details) to highly sensitive (such as bank and health details).

Find out how 'personal information' is defined here and in the glossary here.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act, so on the whole your current approach to compliance will remain valid. The most significant implications for the university relate to centrally-owned processes and policies, which the Information Governance Group has been reviewing and updating over the past 18 months.

Read Queen Mary's Data Protection Policy here.
Read the Information Commissioner's guide to the GDPR here.

The introduction of the GDPR also prompts us all to review our practices and to assure ourselves and others that we are processing personal information fairly and lawfully.

There are five action points for each school, institute, department and centre to consider:

1. Establish a complete picture of the information you hold

Make sure you know about all the personal information being collected and used in your area. This includes electronic and paper records, whether they are shared, or kept only by individuals. One of the best ways to demonstrate compliance with the GDPR is to keep a record of the information you hold and to review it on a regular basis. Individuals have the right to access the personal information we hold about them, so it is also important that you can quickly and easily find their information when asked.

You only need to keep a record of the information for which you are responsible. If you work in a school or institute, for example, you are not responsible for personal information held in the student records system (SITS). But you are responsible for any copies of the information you keep, such as in spreadsheets, student files or your own student records system, as well as any personal information you collect yourselves.

2. Be clear about why you are using information

Individuals have the right to know what personal information you hold about them and how you use it. You also need to be able to explain the lawful basis on which you are processing their information. Much of the information collected on staff, students and contractors, for example, is necessary for the performance of their contract with the university. You may need an individual's explicit consent to collect information lawfully for other purposes. For academic research, consent is required for ethical purposes.

We publish Privacy Notices to explain how the university collects, processes and shares personal information. Each Privacy Notice is aimed at a specific group of people, such as staff, students and visitors to our website.

Read the Privacy Notices for staff and students here.

Make sure that everything you are doing with personal information is already covered by one of the Privacy Notices. Are you collecting additional types of information, or sharing information with anyone else outside the university? Are you using information in ways that people might not expect, such as by combining or matching it with other information? Contact the Records and Information Compliance Manager straight away if you are doing anything that is not covered.

If you are creating or using mailing lists of people outside the university make sure the form you use to collect contact details explains the purpose of the mailing list and makes it clear that the individual is giving their consent to be contacted. You must not contact members of the mailing list for any other purpose without first obtaining their consent. It is also good practice to include information on how people can remove themselves from the list in future mailings.

3. Be clear about how long you are keeping information

Individuals have the right to know how long you will keep their personal information. You should also be able to respond to requests to update their information as long as you have it on file. The guiding principle is to delete, destroy or redact any personal information you no longer need. This limits the risk that information will fall into the wrong hands and reduces the burden on physical and electronic storage.

We publish a Records Retention Schedule to explain how long the university keeps personal and other information. This takes into account the university’s needs, as well as regulatory and statutory requirements. Make sure you comply with the Records Retention Schedule. It is also worth thinking about whether you can delete or destroy redundant copies of information that is formally stored elsewhere, such as in a central records or filing system. Contact the Records and Information Compliance Manager straight away if you are doing anything that is not covered.

4. Keep information safe and secure

You must protect the personal information you hold. Ensure that paper records and electronic storage devices are physically secured, such as in locked cabinets and offices. Electronic information must also be password protected and access controls kept up to date. Paper and electronic filing systems should be partitioned so that the most sensitive information is only accessible to people who strictly need it.

Contact the IT Helpdesk if you want to review the list of people who can access your file shares and if you want to change how the folders are organised. IT Services can also advise on more specific questions about the security of electronic information.

The Records and Information Compliance Manager can provide details of suppliers that have been approved by the university to destroy paper records securely. IT Services can also advise on how to go about destroying electronic devices that hold personal data.

5. Ensure that people are aware of their responsibilities

It is important for everyone who is using personal data to understand their responsibilities. For many people working at the university it will be sufficient to read guidance that can be found on the intranet. We offer training events for people in roles that have greater responsibility for personal and sensitive information. As a manager you have a responsibility to ensure that people working in your area have an appropriate level of awareness and training for their roles.

Read guidance on email, shared drives and more here.
Consult our policies and procedures on information security and other things here.
Book training via the online booking system here.

A footnote on research

The principles of the GDPR are embedded in the ethical approval process for research involving human participants. For example, the information sheet for participants performs an equivalent function to the Privacy Notice and Records Retention Schedule. It must set out clearly what personal information is being collected, how this will be used and protected, the legal basis for processing, how long the information will be kept, and what happens to it when a participant withdraws from the study. The information sheet must also provide a route for participants to raise questions or objections about how you are using their personal information. The consent form must require participants to tick a box saying that they consent to their personal information being processed in the way described in the information sheet.

The Research Group in IT Services provides support to researchers on protecting personal data, including to the high standards that apply to clinical trials.

Read about the ethical approval process here.