University of BRISTOL

General Data Protection Regulation (GDPR) – What do you need to do to comply?

	Action	Action description	Further information
1.	**Review old electronic and paper files**	Does your Division/School continue to have a valid reason for keeping files that contain personal or sensitive information?	A Records Management and Retention Policy has been produced. This is accompanied by a Records Retention Schedule that provides more specific guidance around retention periods for different types of information. For instance, whilst we'll hold a core electronic record for students and staff indefinitely, many associated or local records should not be kept any longer than 6 years from the date of graduation, departure or end of employment.
2.	**Complete the Training**	All staff with access to the MyReview system need to complete the two mandatory training modules covering data protection and information security. A further module has been produced for staff without access to MyReview, which can be accessed from this page.	Non-completion will be followed up via line managers.
3.	**Data Breaches**	Be aware of the procedure for reporting data breaches or security concerns. If you have experienced a data breach (or suspect that you may have), and/or have any security concerns then you should contact the Information Security Team and/or the Secretary's Office **immediately**.	GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data". In the case of more serious data breaches, there is a duty to notify the ICO and affected individuals of the breach within 72 hours of the organisation becoming aware of it.
4.	**Privacy notices and consent**	The University has top level privacy notices in place for staff , students, parents and guardians and research participants. If, however, you need help with reviewing or drafting local level privacy notices or help with consent collection, then place consult with the Secretary's Office.	GDPR enforces stricter rules around the way personal or sensitive data can be collected and used. This means that consent needs to be freely given, and data subjects (individuals) need to be given more specific details around the purpose and legal basis behind the collection and use of their personal data.

	Action	Action description	Further information
5.	**Data Protection Impact Assessments**	Be aware of Data Protection Impact Assessments (DPIAs)**.** A DPIA must be completed at the outset of any project, or change to an existing system or process, that involves the collection or handling of personal information. It is an important way of demonstrating compliance with GDPR.	DPIAs are built into project and new service procedures but may also be needed for initiatives not captured in this way, including research.
6.	**Subject Access Requests**	Be aware of subject access requests. If you receive any requests from individuals asking for access to their personal data, then please send these requests on to the Secretary's Office as quickly as possible. Individuals wishing to have access to personal data held by the University should complete a subject access request form.	Also be aware of request from individuals for their personal data to be erased and amended, as the University may also need to comply with these. Consult the Secretary's Office if you are unsure.
7.	**Contracts**	Be aware of any contracts or agreements relating to your area that involve the processing or sharing of personal data. If you are entering in to any new agreements or contracts then please consult with the Secretary's Office and, if relevant, Procurement, to gain advice and to get the appropriate templates. Existing contracts may also need revising.	This will include data processing agreements, where the University uses a third party to process personal data on its behalf (for example, using a service provider to send out communications using contact details we have provided); and data sharing agreements, where data is shared with, or obtained from, another "data controller" for agreed mutual purposes (for example, research data providers will often require such an agreement).
8.	**Marketing**	Be aware of changes around communications and marketing activities. Information promoting University events or opportunities for students could constitute direct marketing and therefore it is important that the University is aware of the definitions and regulations when sending any communications.	GDPR tightens the regulations around direct marketing. The ICO's definition of direct marketing includes "messages trying to sell goods or services and those promoting an organisation or its values or beliefs".