GDPR – Handling Staff Personal Data

These guidelines have been compiled to help you comply with your role in handling staff personal data. The General Data Protection Regulations which come into force on 25 May 2018 are stricter than the Data Protection Act 1998 and the penalties are significant if we breach the regulations.

The guidelines apply to everyone but are most relevant to staff working in HR, plus administrators and managers who regularly view or deal with staff personal data.

For the purposes of the GDPR, the University is a Data Controller for all the following categories of staff, who are defined in the regulations as a 'data subject':

- All job applicants
- All University employees on any form of salaried contract
- People who work for the University on a casual or claims basis
- Visitors or Contractors who require access to University systems and / or an ID card
- Former staff who are members of a University pension scheme

Personal data is anything which relates to and identifies a living individual. Examples are name, current address, payroll number, photo, gender, age.

Sensitive personal data is subject to another level of control in GDPR and is information about religious or other beliefs, political opinions, trade union membership, offences, sexual orientation, health.

GDPR has three changes which all organisations must comply with:

- A requirement for greater transparency about personal data is processed. This will result in, for example, more use of Privacy Notices
- All data breaches must be reported to the Information Commissioner's Office in 72 hours
- A Data Subject Access Request must be completed within 30 calendar days and there is no charge. However, extensions are permitted if the request is difficult to comply with within these timescales.

All colleagues have a responsibility in enabling the University to comply with these timescales.

	Do	Don't
The Basics	• Be clear on why you are holding the personal data – is it for statutory purposes, necessary for the performance of the employment contract, for a legitimate business reason, vital for the protection of life or necessary to perform a public duty (the six reasons permitted in GDPR)? • Ensure the personal data is stored securely and only appropriate colleagues can view and / or process in accordance with the Information Categories and Controls Policy • Regularly review the personal data that you are holding and, where necessary, destroy it in accordance with the University's Retention Schedule • Review your emails regularly - it is good practice to delete emails older than 2 years which contain personal data unless you have a legitimate reason to retain the information for longer (refer to first bullet). If you want to retain the email, convert to a PDF document in a secure workspace with an appropriate filename including a destruction date for your future reference • Ensure personal data is accurate, relevant and not excessive in relation to your needs • Where possible keep hard copy personal data locked away and your desk clear • Ask yourself the question – would I be comfortable with responding to a Data Subject Access Request (DSAR) with this personal data? If the answer is 'no', get rid of it immediately (although not if the information has already been requested as part of a DSAR)	• Keep any personal data if you don't have a legitimate reason to do so • Keep personal data for longer than is necessary and beyond the Retention Schedule • Store personal data in an open access area, either physical or electronic • Retain a document to use as a template without removing the personal data first • Use personal data held for one purpose for a different purpose without the written consent from the data subject. An example would be a completed job application form being used in a training event with personal data visible or sharing a CV with someone else because you think the applicant might be suitable for another position without the consent of the data subject • Write anything in an email or letter about a colleague that you wouldn't be comfortable saying or sharing with them directly

Reporting a breach	• Report immediately any accidental or deliberate release of personal information to your Data Co-ordinator or line manager and dp@lboro.ac.uk	• Attempt to cover up or ignore a data breach – this may have serious consequences for you and the University. Often, a breach is likely to be the result of a system failure or a gap in knowledge and training provision. The University is more concerned with taking corrective action rather than allocating blame to individuals.
	Do	**Don't**
Getting rid of personal data	• Establish a procedure to ensure you have Use the office confidential waste bags or the office shredder to dispose of any document containing any personal data • Regularly empty your Deleted Items, Junk Email and Recycle Bin – electronic personal data needs to be 'put beyond use' • Refuse requests from family or friends for information about an employee, unless prior written permission has been received from the individual OR the release of the personal data is vital for the protection of life	• Archive personal data instead of destroying it - information that is archived, is subject to the same data protection regulations as 'live' information. Only HR can archive staff personal data in accordance with their procedures • Erase or alter data after you have received a Data Subject Access Request – you must comply with a DSAR from the University Data Protection Officer within the required timescale
Sending and sharing	• Be clear on who you can share personal information with and the purpose of sharing. Check with your HR contact if you are not sure. • Please be very aware of sensitive personal information being shared over email and retain the information for only as long as you need it • Where possible avoid sharing personal data outside of University corporate systems or premises. If you must do this, use encrypted removable media eg an encrypted USB pen drive. • Ensure that you have a contract (data processing agreement) in place when sharing personal data with a third party. Further advice on setting up a new or amending an existing contract can be obtained from Procurement.	• Share sensitive personal information with a third party without understanding the basis for releasing the data OR obtaining the staff member's consent • Open email attachments from an unknown source • Disclose any sensitive personal data over the telephone unless it is vital for the protection of life • Disclose any personal data (including giving references) about an individual to an external organisation without first checking that the individual consents to such disclosure, or, in the case of the police contacting the HR Director first

	• Send personal data (even if encrypted) via a secure remote access ie use your Lboro email not your personal email	
Passwords	• Use a strong password (see the IT advice) • Prevent others seeing you enter passwords or viewing sensitive personal information	• Share your passwords with anyone else or write them down • Save passwords in web browsers if offered to do so
	Do	**Don't**
Security	• Log in using the secure University networks • Log-off / lock your computer or device when leaving it unattended • Avoid using your own device (computer, mobile phone) to view employee personal data	• Log on to public Wi-Fi whilst working with employee personal data • Store or download business data onto your personal devices unless first authorised by your manager
Processing & saving data	• Process and save personal data in accordance with your role – seek clarity from your line manager if you are unsure about this • Save the personal data in accordance with your department's access arrangements, so the relevant colleagues can continue to access it if you are not in work	• Save personal data outside of University corporate systems • Process personal data outside of agreed procedures
Working on-site	• Be aware of data security in relation to a visitor in your place of work • Adopt a clear desk policy where practicable, particularly in relation to personal data • Minimise your paper records; electronic data held, for example, in a secure workspace is always recommended	• Leave sensitive information unattended; lock it away in lockable drawers or log off or lock your work station • Position screens where they can be read from outside the room. Invest in a privacy filter for your screen if you are concerned about others viewing your screen. • Assume that your main security threat is external

	• Always use University corporate systems for data storage as there will be contracts in place to protect the University if data is lost. It also prevents data from being shared or stored outside of the EEA	
Working off-site	• Access data remotely instead of taking it off-site using approved secure systems • Sign out completely from any services you have used • Take information offsite only when you are authorised to do so. • Ensure personal information is protected offsite.	• Work in public spaces where other people could view or overhear personal data • Download personal data to your personal device unless essential; if you do, delete the data when you have finished your work