Data Protection: a Quick Guide for University Staff

If you handle any information about identifiable people, whether they are applicants, students, other staff, alumni, research participants, visitors or anyone else, you need to be aware that you are dealing with personal data. You must look after all personal data carefully. You must be especially careful with more sensitive information about people, for example concerning their health, sexuality or ethnicity. This Quick Guide is designed to help. Detailed policies, guidance, training and resources are available from the University's data protection overview page.

PRINCIPLES AND RIGHTS

Personal data must only be used for the purposes it was provided for, as described at the time of collection. It must be relevant, accurate, treated confidentially/securely, and only retained for as long as it is needed (follow your Institution's timeframes for the disposal or removal of old records). A good rule of thumb is to consider whether someone would be surprised about how you are using their personal data (check the University's core privacy notices to see what they have been told).

Be aware of people's rights: people have a right to know what happens to their personal data and to see copies of it, including emails. They can ask for inaccuracies to be corrected and they can object to how their personal data is being handled, even asking for it to be deleted. Although many of these rights are not automatic, people do not have to follow standard channels when exercising them. Any formal requests you receive should be passed to the Information Compliance Office.

SHARING, RISKS AND BREACHES

If you need to share personal data with another organisation (except for a College or Cambridge in America), even if that organisation just stores personal data for you, you first need to be sure that all of the risks have been considered. A written agreement in the correct form may be required. If you are unsure about what to do, speak to your Departmental Administrator or other relevant contact. This is particularly important if the organisation is outside of the European Economic Area.

If you are starting a new project or initiative involving personal data, make sure you consider data protection issues early on.

If you think there has been a leak ("breach") of personal data, make sure you report it as soon as possible, including details of the personal data involved and how widely it may have spread. The University has to report serious breaches to the Information Commissioner's Office (the regulator) within 72 hours of discovery.

TIPS FOR HANDLING PERSONAL DATA IN THE OFFICE OR LAB

- **Your office.** If personal data is on your desk or shelves, consider locking your room when you leave it, especially if you are in a publicly accessible building.
- **Your computer.** Use a strong password, change it when needed and don't share it with others. Lock your PC when you leave it unattended and log out and the end of the day. Orient your screen so it can't be viewed by others. Never let others use your computer accounts. Allow IT staff to keep your machine backed-up and updated with the latest security and operating patches. Use passwords/access permissions to protect files and folders on shared drives storing sensitive data. Beware of unsafe websites.
- **Your papers.** Store files and documents about people in locked drawers and cupboards. Know where documents are kept and who has access to them. Ensure confidential waste is shredded or stored securely for collection.

TIPS FOR HANDLING EMAILS AND PHONE CALLS INVOLVING PERSONAL DATA

- **Emails.** Don't copy emails about people wider than you need to. Check email addresses before you send out personal data. Consider sending personal data in a password-protected attachment rather than the body of the email. If you are sending an email to a group of people, especially if it contains anything sensitive, think about using "bcc" so you don't share their addresses. Don't keep emails about people that you or the University no longer need. Be careful when opening emails and attachments from unknown or suspicious sources.
- **Phone calls.** Don't give out personal data about others unless you have verified the caller's identity and you're sure they have a right to have it. Generally, don't supply others' contact details or other personal data to unknown enquirers: take the caller's number and offer to pass messages/queries on. Pass requests from the police and other law enforcement agencies to the Information Compliance Office.

TIPS FOR HANDLING PERSONAL DATA ON THE MOVE	TIPS FOR WRITING ABOUT PEOPLE AND FOR ACADEMIC RESEARCH
• **Your mobile devices.** Use a strong password, change it when needed and don't share it with others. Use virtual private networks or secure remote access where possible. Set your devices to lock automatically when not in use. Keep them updated and backed-up. Store them securely. Dispose of old devices carefully. • **Portable storage.** Avoid using USB sticks to store personal data; if you need to, consider encryption or similar protections against inappropriate access. • **Travelling abroad.** Consider seeking advice before you travel abroad with mobile devices, and always do so if you are travelling to countries with significant cyber risks.	• **Comments about other people.** Keep comments – whether official or unofficial – fair, appropriate, accurate and justifiable. Always assume that the comment might eventually reach the person it is about. • **Academic research.** There are significant variations to the standard data protection provisions for different types of academic research. Consult the guidance.
REMEMBER: You want personal information about yourself to be handled carefully. Always treat other people's information in the same way.	