Selwyn College Cambridge

Handling personal data at Selwyn

PRINCIPLES Personal data must only be used for the purposes it was provided for, relevant, accurate, treated confidentially, securely stored and only retained for as long as it is needed. A good rule of thumb is to consider whether someone would be surprised about how you are using their personal data. Check privacy notices on the College website to see what they have been told.

RETENTION Familiarise yourself with the parts of the Record Retention Schedule (on the College website) which apply to your role and ensure that records are destroyed or archived according to the timeframes provided.

RIGHTS People have a right to know what happens to their personal data and to see information about them, including emails. They can ask for inaccuracies to be corrected; they can object to how their personal data is being handled, even ask 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 Bursar.

SHARING Stop and think before you share personal data with other members of staff, Fellows and students. Do they actually need the data? Is the sharing necessary and proportionate? What is the minimum data you can share to achieve the aim? Could the data be anonymised? What safeguards can you put in place to minimise the risks?

If you handle any information about people, whether they are students, fellows, staff, visitors or contractors, remember you are dealing with personal data. You must protect all personal data and be especially careful with special category data concerning people's health, sexuality, race, politics or religious beliefs.

If you do need to share personal data with another organisation (except for the University, another Cambridge college or Cambridge in America), even if that organisation just stores personal data for the College, you must ensure all of the risks have been considered. A written Data Sharing Agreement may be required. If you are unsure about what to do, speak to your Head of Department or the Compliance Officer.

RISKS Before you process new or complex personal data, or if you are planning to significantly change the way you process data, ensure that data protection safeguards are considered. Contact the Compliance Officer to assess the risks; they may need to be recorded in Data Protection Impact Assessment.

BREACHES Data breaches can happen in a number of ways:

- Sending personal data in an email to an incorrect recipient.
- Leaving documents on a desk, photocopier, or PC screen where it can be seen by others.
- Lost or stolen computing devices (laptops, tablets, memory sticks).
- Accidently deleting or amending personal data without permission.
- Being unable to access the data due to a lost or forgotten password.
- Circulating spreadsheets containing personal or special category data.

THE CLOCK IS TICKING… If you think there has been a leak ("breach") of personal data, report the breach to the College Data Protection Lead (CDPL) (the Bursar), or the Compliance Officer in the absence of the Bursar **as soon as possible**. The CDPL will record the breach and report it to the College's Statutory Data Protection Officer, at the Office of Intercollegiate Services. Serious data breaches must be reported to the Information Commissioner's Office **within 72 hours** of discovery.

BEST PRACTICE

- Adopt a Clear Desk Policy.
- Store files and documents about people in locked drawers and cupboards.
- Know where documents are kept and who has access to them.
- Place personal data in locked drawers when leaving your workstation, especially if you share your office with others.
- Orient your PC screen so it can't be viewed by others.
- Use strong passwords, change them frequently and never share them.
- Use passwords/access permissions to protect sensitive data stored in files and folders on shared drives.
- Always shred confidential waste or stored it securely for collection.
- Never copy emails about people wider than you need to.
- Check email addresses before you send out personal data. Disable autofill in your email settings; it could prevent an email from being sent to the wrong person.
- Transfer personal data via email as a password-protected attachment and send a note of the password in a separate email, text or phone call.
- If sending an email to a group of people, especially if it contains special category data, use "bcc" so you don't share their addresses. Before sending personal data to external companies, send a test email to the address and await confirmation that it is the intended recipient before sending the file.
- Don't keep emails about people that you no longer need. Be careful when opening emails and attachments from unknown or suspicious sources; contact helpdesk@sel.cam.ac.uk for advice.

REMEMBER: You wouldn't want personal information about yourself to be shared with just anyone. Always treat other people's information with care.