Data Protection Policy Summary

The University's Data Protection Policy explains how the University meets its obligations under the Data Protection Act (DPA) and what your responsibilities are as a member of staff.

So Did You Know?

- There is a centralised University procedure for responding to requests to access personal information made under the DPA.

But Did You Also Know?

- The University only has 40 calendar days, from the date a request is received, to provide access to personal information;
- Information in any work-related record, including email, could potentially be released in response to a request;
- 'Processing' is a collective term and includes obtaining, recording, storing, using, sharing, disclosing, transferring and destroying personal data. All staff who process personal data as part of their duties must ensure that they are complying with the eight data protection principles;
- The Information Commissioner's Office (ICO) has the power to take regulatory actions to enforce compliance with the DPA which include enforcement notices, audit, monetary penalties (up to a maximum of £500,000) and criminal prosecution.

So Do You Know?

- What to do with a request for personal information if you receive one;
- What the eight data protection principles are;
- What to do if there is a security breach (a breach could arise from a theft, a deliberate attack on University systems, unauthorised use of personal data, accidental loss or equipment failure) involving personal data held in your area;
- Who to ask if you're not sure.

And Could You?

- Locate any information you hold if it is requested;
- Provide that information quickly.

To find out more read the University of Lincoln's Data Protection Policy available on the Portal at http://secretariat.blogs.lincoln.ac.uk/information-compliance/data-protection.