# Data Security: Keeping data safe

## Storing and handling information relating to a disability

All communications carrying sensitive personal information about a student should be marked confidential and the information given limited to what is necessary to support the student effectively.

The University guidance on data protection and information security should be followed and staff should actively follow the methods set out in the University's online information security awareness training. Some tops tips:

- Have a 'clear desk' policy (for example lock away unattended documents);
- Dispose of any papers using University issued confidential waste bins or shredders;
- Always lock your screen when you step away from your desk;
- All those with whom information is shared should be reminded of their duty to treat the information confidentially and keep the data secure.
- Avoid the use of email for sharing sensitive personal data. Secure SharePoint sites provide a good alternative and guidance on setting this up can be found on the University's IT website.
- If you do use email, follow these guidelines:

Email:

- Mark all email containing sensitive personal information as 'Confidential'.
- Password protect documents containing personal data, and provide the password separately.
- Always double-check your recipients,
- Always double-check your attachments and any forwarded text before pressing 'send'. Avoid forwarding text where possible to ensure that all information is given on a 'need to know' basis.
- Double-check your recipients, specifically making sure you've selected the correct individual where there could be individuals with the same name at the University,
- Consider setting up a delay on sending emails in Outlook – this allows you time to modify or delete the message if you realise after pressing 'send' that the email was drafted incorrectly (instructions on how to set-up the delay in Outlook).

There is more information about email management on the University's compliance website.

## Data retention

Data relating to support for disabled students should be retained for 6 years after the end of the student's time at University. See the University's student record retention policy.

## Further information

University information security website

University Policy on Data Protection

University Policy on Information Security

For students: Use of student personal data

How the University implements the General Data Protection Regulation (GDPR)

Six key principles of data privacy