When creating information on behalf of the University, use the following categories to classify your content, before sharing.

**PUBLIC 🍄**
This information can be readily shared and made publicly available with no adverse consequences for any organisation or individual. Typical content might be:

- news and updates
- external website content
- most policy documents
- published research
- published accounts.

**RESTRICTED ACCESS 🗝**
This information can be shared with a limited audience, usually within the University. It could have financial or commercial value, personal data, or subject to intellectual property, trademark or other legal protection. Typical content might be:

- most professional correspondence
- individual student marks and feedback
- emails and documents containing limited personal data
- policy, procedure and planning documents with technical or commercially sensitive information
- non-confidential meeting agenda and minute
- pre-publication research data
- most financial data.

**CONFIDENTIAL 🗝**
This information has significant value for Oxford Brookes University, another organisation or individual. Wrongful disclosure could impact the reputation or standing of an organisation or an individual, the safety of an individual or could cause financial loss. Typical content might be:

- emails and documents containing large amounts (200+ records) of student personal data - grades, names and addresses
- HR records
- student wellbeing records
- emails and documents that include special category personal data of staff and students (race, ethnicity, religion, health, political beliefs, genetic or biometric data, trade union membership, criminal convictions and sexual orientation.)
- materials received from third-parties that are proactively marked as 'confidential'.

[www.brookes.ac.uk/it/information-management/iso-27001](http://www.brookes.ac.uk/it/information-management/iso-27001)