University of BRISTOL

TOP 10 DATA SECURITY TIPS

- Know what constitutes restricted UoB data
- Process restricted data on secure UoB computers only and do not store restricted data on non-UoB equipment
- Encrypt restricted data to transport it and fully disk encrypt your laptop/ netbook
- Share restricted data only with those with the right and need to view it

POSITIVE WORKING environment

TOP 10 DATA SECURITY TIPS

- ☑ Do not make copies of restricted data
- ☑ Lock away unsecured restricted data and lock your door if leaving your room unattended
- ☑ Never share or disclose your UoB password or use it for non-UoB services
- ☑ For UoB business use your UoB email account and a UoB recommended secure email client
- ☑ Securely erase data before disposing of hardware and storage
- ☑ If in doubt about data, ask advice from the Information Rights Officer based in the University Secretary's Office

Data security is not optional

www.bris.ac.uk/infosec