

UNIVERSITY OF  
Southampton

# Data Protection and Coronavirus

Barbara Halliday

Legal and Governance Services

20 March 2020

# Data on the move

- Office based data protection measures need to continue to operate well when data leaves the workplace
- Information Commissioner (ICO) has levied £1 million in fines for breaches in this area alone
- ICO is taking pragmatic approach to coronavirus challenge BUT data protection does not stop when data leaves work

# Protect data – by technical and organisational means and you!

- Office based data protection measures need to continue to operate well when data leaves the workplace
- Information Commissioner (ICO) has levied £1 million in fines for breaches in this area alone
- ICO is taking pragmatic approach to coronavirus challenge BUT data protection does not stop when data leaves work

# Possible outcomes of loss

- Distress caused to individual by loss of sensitive data
- Identity theft
- Fraud caused by loss of individual's financial data
- Fine or enforcement notice to University from Information Commissioner

# How to keep data safe – top tips 1

- Minimise removal of physical data from work
- During transportation ensure it is secure – e.g. locked in a briefcase
- Do not leave it unattended
- Remember to take it with you!
- Keep paper files secure and shred securely when no longer needed

## How to keep data safe – top tips 2

- If your computer is provided by the University no access to it should be given to other members of your household
- If the computer is yours, restrict access and password protect access to University systems and data
- Don't share your password and if you have shared it, change it immediately
- Encrypt and/or password-protect information
- Think carefully about what data to download and whether to download it – do you need it and how much do you need?
- Delete data that is no longer required

## How to keep data safe – top tips 3

- Use automatic screen locking – after 10 minutes of inactivity
- Use disk encryption
- Avoid public wi-fi hotspots
- Don't leave personal devices unattended in public spaces
- Activate remote wipe



## How to keep data safe – top tips 4

- Do not use 3<sup>rd</sup> party cloud storage services like Dropbox, Google Drive, Box.com or OneDrive (using a personal login) for the storage of University files.
- Do not use USB memory sticks or hard drives for storing University files.
- **To access your files from your personal device(s), use Microsoft OneDrive for Business or other Office 365 applications, using your University login.**

## How to keep data safe – top tips 5

- Report accidental loss, destruction or damage to data using the University's breach reporting form  
<https://www.southampton.ac.uk/about/governance/freedom-of-information.page>
- If you need assistance or have any questions:  
Contact [infogov@soton.ac.uk](mailto:infogov@soton.ac.uk) OR [service@service.soton.ac.uk](mailto:service@service.soton.ac.uk)