Bring Your Own Device Policy

Version 1

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
1	4/6/18	Ali Mitchell	New template, Data Protection legislation updated in paragraph 5

Review Distribution

Name	Title
Rhiannon Platt	Information Governance Manager and Data Protection Officer
Ian Tilsed	Assistant Director Strategy and Architecture

Approval

Name	Position	Signature	Date
	Members of the IGSSG		June 2017

1. Introduction

1.1 The University of Exeter recognises the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at home, on campus or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. It is committed to supporting staff in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing University provided services on BYOD.

1.2 The use of such devices to create and process University information and data creates issues that need to be addressed, particularly in the area of information security.

1.3 The University must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.

2. Information Security Policies

2.1 All relevant University policies still apply to staff using BYOD. Staff should note, in particular, the University's Information Security related policies. Several of these are directly relevant to staff adopting BYOD.

- Regulations Relating to the Use of Information Technology Facilities
- Policy for Information Security on laptops and portable media
- Anti-Malware Policy
- Data Protection Policy

3. Staff Members Responsibilities

3.1 Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of University information (as well as their own information)
- Invoke the relevant security features
- Maintain the device themselves ensuring it is regularly patched and upgraded
- Ensure that the device is not used for any purpose that would be at odds with the University Regulations Relating to the Use of Information Technology Facilities
- While University IT staff will always endeavour to assist colleagues wherever possible, the University cannot take responsibility for supporting devices it does not provide.

3.2 Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data
- Keep information confidential where appropriate
- Maintain the integrity of data and information, including that on campus
- Take responsibility for any software they download onto their device

3.3 Staff using BYOD must:

- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device

- Set up remote wipe facilities if available and implement a remote wipe if they lose the device
- Encrypt documents or devices as necessary (see Policy for Information Security on laptops and portable media)
- Not hold any information that is sensitive, personal, confidential, or of commercial value on personally owned devices. Instead they should use their device to make use of the many services that the University offers allowing access to information on University services securely over the internet. More information on determining if information is 'confidential' is available on the website
- Where it is essential that information belonging to the University is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails
- Ensure that relevant information is copied back onto University systems and manage any potential data integrity issues with existing information
- Report the loss of any device containing University data (including email) to the IT Help desk
- Be aware of any Data Protection issues and ensure personal data is handled appropriately
- Report any security breach immediately to IT Helpdesk in accordance with the Information Security Policy (the Information Governance team will be informed where personal data is involved)
- Ensure that no University information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party

4 Monitoring and Access

4.1 The University will not routinely monitor personal devices. However it does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks or both
- Prevent access to a particular system
- Take all necessary and appropriate steps to retrieve information owned by the University

5 Data Protection and BYOD

5.1 The University must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 2018. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

5.2 The University, in line with guidance from the Information Commissioner's Office on BYOD recognises that there are inherent risks in using personal devices to hold personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data. A breach of the Data Protection Act can lead to the University facing significant fines. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the University's facilities being withdrawn, or even a criminal prosecution. For more information see the University's Data Protection webpages.

6. Information to Help Staff

6.1 The University has a policy of ensuring remote access to its systems and services wherever possible - Remote Access to University provided Academic Services. The University provides information for staff making use of remote access services:

http://www.exeter.ac.uk/staff/employment/leave/flexibleworking/staff/ps/homeworking/itguidance/. On campus BYOD will normally be limited to the Wi-Fi Network using eduroam. Additional information is provided to help with encryption: http://www.exeter.ac.uk/ig/infosec/encryptfiles/.