DURHAM SU REMOTE WORKING DEVICE USE POLICY

1. INTRODUCTION

1.1. Durham SU recognizes 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 BYOD working.

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

1.3. All staff can request to be provided with a home working device by Durham SU if they are required to work remotely and will usually be provided with a Durham University laptop in these instances. Exceptions to this may be where a different device ie a tablet or phone, is required for the work to be done. Some staff may be required to work from a Durham University laptop rather than BYOD because their roles require additional system security or functionality. As when working in the office, Durham SU must take reasonable steps to ensure Durham University’s requirements for use of their IT services are met by staff.

1.4. This policy sets out the minimum requirements for remote working systems and BYOD. Individual business areas may need specific, additional, higher requirements met.

2. INFORMATION SECURITY AND IT POLICIES

2.1. All relevant Durham SU policies still apply when using your own device. In particular, staff should ensure they are familiar with our Data Protection and Information Security Policy.

2.2. When using a Durham University device, such as a laptop, Durham SU staff must comply with Durham University’s policies and requirements for use.

2.3. When using a Durham SU provided device which is not a Durham University Device (for example a tablet or mobile phone), then all Durham SU policies still apply, at the manager of the business area for which the device is primarily used is responsible for ensuring the devices physical security and its security features are enabled.

2.4. Staff may often use Durham University platforms and software to ‘remote access’ their work computers or to access other Durham University services, and in many cases this is required. However, they should be aware that when doing so they must follow the relevant Durham University policies, in particular, the Staff IT regulations.

3. RESPONSIBILITIES OF STAFF

4. Staff who use their own device (BYOD) for Durham SU work must ensure that it and the information it contains is appropriately protected. They must take responsibility for their own device and how they use it by doing the following.

    4.1. Familiarise themselves with their device and its security features so that they can ensure the safety of Durham SU information (as well as their own information)

    4.2. Invoke the relevant security features of the device

    4.3. Maintain the device themselves ensuring it is regularly patched and upgraded

    4.4. If other members of your household use your device, ensure they cannot access Durham SU information, for example, with an additional account passcode. (Our preference is for you not to share the device with others.)

5. Staff using BYOD ***or*** working remotely from a Durham University or Durham SU device must take all reasonable steps to:

    5.1. Prevent theft and loss of data

    5.2. Keep information confidential where appropriate

    5.3. Maintain the integrity of data and information

    5.4. Take responsibility for any software they download onto the device

    5.5. Staff should do this by:

        5.5.1. Setting up passwords, passcodes, passkeys or biometric equivalents, and enabling multi-factor authentication. These must be of sufficient length and complexity for the particular type of device

        5.5.2. Setting up remote wipe facilities if available and implement a remote wipe if they lose the device

        5.5.3. Setting devices to lock automatically when the device is inactive for more than a few minutes

        5.5.4. Whenever possible, use remote access facilities to access information on University systems. Log out and disconnect at the end of each session

        5.5.5. When using Wi-Fi outside of Durham University, controlling the device's connections by disabling automatic connection to open, unsecured Wi-Fi networks and make risk-conscious decisions in line with staff guidance before connecting. Disable services such as Bluetooth and wireless when not in use

        5.5.6. Downloading and maintain appropriate anti-virus software to their device

        5.5.7. Taking appropriate physical security measures. Not leaving device unattended.

        5.5.8. Encrypt documents or devices as necessary, such as USB devices or external hard-drives

        5.5.9. Not hold any information that is sensitive, personal, confidential or of commercial value on personally owned devices. Instead, staff should use their device to make use of the many services that the University offers allowing access to information on University servers and platforms, or SU platforms securely over the internet. If staff are unsure what information is 'confidential' they should speak to their line manager.

5.5.10. Where it is essential that information belonging to Durham SU 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

5.5.11. Ensure that relevant information is copied back onto University or Durham SU systems and manage any potential data integrity issues with existing information

5.5.12. Report the loss of any device containing University data (including email) to the Durham SU's Data Protection Officer

5.5.13. Be aware of any Data Protection issues and ensure personal data is handled appropriately

5.5.14. Report any security breach immediately to the Data Protection Officer, and for Durham University devices or services, to Durham University's Computing and Information Service

5.5.15. Ensure that no Durham SU 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.

6. MONITORING AND ACCESS

6.1. Durham SU will not routinely monitor personal devices. However, it does reserve the right to:

6.1.1. Prevent access a particular device from accessing Durham SU or University platforms or services, either from the wired or wireless networks or both.

6.1.2. Prevent access to a particular system

6.1.3. Take all necessary and appropriate steps to retrieve information owned by the Durham SU, which includes work related information held on a personal device. This may happen when a formal process such as a Data Subject Access Request, complaint or any other formal process requires it, or when it is deemed necessary for any other reason.

7. DATA PROTECTION AND BYOD

7.1. Durham must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 1998 and adhere to the General Data Protection Regulations. 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.

7.2. Durham SU, 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 significant fines for the charity. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the Durham SU's facilities being withdrawn. For more information see the Durham SU's Data Protection webpages.

8. REMOTE WORKING AND SAFEGUARDING

8.1. Durham SU has a responsibility to safeguard children and people at risk of harm who are in the Students' Union or in contact with its staff and student volunteers, and it recognizes the risks presented by online activity. As such, everyone has a duty to be vigilant reduce the risk of online spaces for vulnerable parties, and report any behavior online which would indicate a risk to vulnerable parties. For example, not requiring staff or students to share their background in video calls, reporting instances where you believe photos of video calls may have been captured, particularly of children or people at risk of harm etc. For further guidance on safeguarding, refer to Durham SU's safeguarding policy.

9. POLICIES AND REGULATIONS

9.1. Durham SU Data Protection and Information Security Policy
9.2. Durham SU Safeguarding Policy
9.3. Durham University IT Regulations

10. DOCUMENT INFORMATION

10.1. Compliance with the policies and guidance laid down in this document will be monitored via the SU's Senior Leadership Team, together with reviews by the Performance and Delivery Committee, within the annual Data Protection Report to this Committee. The Data Protection Officer is responsible for the monitoring, revision, version tracking and updating of this document on a three yearly basis or sooner if the need arises.

Author	Date Drafted	Approved By	Date Approved	Date for review
Georgina Lambert	26/11/2021			December 2023