MOBILE AND REMOTE WORKING POLICY AND GUIDANCE

Department	Information Services Department		
Author	Legal Advisor		
Authorised By:	VCB		
Implementation By:	All Staff		
Policy Reference:	POIT1718010		
Policy Replaced:	None		
Version No:	1	**Approval Committee:**	VCB
Date approved:	23.07.18	**Minute no:**	17.146.02
Status:	Approved	**Implementation Date:**	August 2018
Period of approval:	3 years	**Review Date:**	Aug 21
I have carried out an equality impact assessment screening to help safeguard against discrimination and promote equality.			
I have considered the impact of the Policy/Strategy/Procedure *(delete as appropriate)* on the Welsh language and Welsh language provision within the University.			

Introduction

Mobile working and remote access extends the transit and storage of information outside of the University infrastructure, typically over the internet. This brings great benefit to the University in terms of its ability to meet its strategic objectives, especially in enterprise, partnerships, marketing and student recruitment but also exposes it to new risks that must be managed effectively.

The purpose of this Policy is to outline the risks associated with remote working and remote access to systems, and describe the responsibilities of 'users' and asset owners, including enabling remote access for third parties or service providers.

Scope

This Policy applies to all University members and all third parties accessing University systems and information remotely.

This policy covers all University information and systems being accessed electronically from remote locations, or via mobile devises or tablets

For the purposes of this Policy, the terms ‘mobile’ and ‘remote’ are used interchangeably and should be taken to cover any scenario where University related business is carried out away from the University campus or the campus network.

Risks

Loss or theft of the device: Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as University campus locations

Being overlooked: Some users may work in public open spaces, such as on trains, planes and other public transport where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials including passwords.

Loss of credentials: If user credentials (such as username or password) are stored with a device used for remote working or remote access and it is lost or stolen, the perpetrator could use those credentials to compromise services or information stored on (or accessible from) that device.

Unauthorised access to remote gateways: Credentials that are stolen via other means (such as phishing) may be used by attackers to gain unauthorised access to interfaces that are exposed to the Internet, such as email or student systems. This can potentially compromise any information stored within those systems

Policy

Information Asset Owners and managers should ensure that processes are in place to authorise remote access and mobile working within their area of responsibility.

Where third parties have been permitted to access University systems remotely, Asset Owners should ensure that appropriate contracts are in place to cover such access, and that said contracts are regularly reviewed to ensure compliance with this and other information security policies

University staff members working on a mobile device or on a remote basis should ensure that they are authorised to do so, and that access is in accordance with this policy.

In order to assure the confidentiality and integrity of University systems and information, only approved technologies may be used for remote access and mobile working

The University reserves the right to restrict remote and mobile working if information risks are not being managed in accordance with this, and other Information Governance policies.

Mobile and Remote Working

i. Working remotely - away from the University and/or from Home

All the University’s policies on data protection www.glyndwr.ac.uk/dataprotection apply when a member of staff takes work containing personal information away from the campus or to their home.

The University's Data Protection Officer has issued a brief summary of the additional rules applying when working from home or taking any personal data from the campus:

- Staff must obtain permission from their line manager/Information Asset Owner to take work containing personal data away from the campus, whether that be for external business requirements or to work from home. The data protection principles must be maintained at all times and special care should be taken when transporting personal data e.g. no leaving in your car, when shopping or eating out on your way home.
- At times there may be a need to transport personal data that is not owned by the University but is related to a research project undertaken by University staff. At such times the data protection principles of the University must be maintained at all times.
- Personal data must never be kept on laptops or portable storage (such as USB drives) unless the device or the file has been encrypted appropriate software security systems dependent on the devices being used, for example 'bitlocker' for Microsoft Office systems..
- If personal data is lost or accidentally disclosed to third parties, this must be reported to the Data Protection Officer on dpo@glyndwr.ac.uk and the form completed on Reporting a Breach which can be found on the Information Governance website www.glyndwr.ac.uk/dataprotection immediately so that remedial action can be taken.
- Further information, including the forms to report a breach data protection incidents is available at www.glyndwr.ac.uk/dataprotection

ii. Using mobile devices

Many University staff have laptops (either work or own), which are of course convenient to use whilst travelling, however, special measures should always be taken to protect both the individual and the University's security when working remotely. To conform with University policy the following basic principles should be followed:

- encrypt the laptop
- encrypt any removable data devices such as 'bitlocker' for Microsoft systems
- protect your passwords
- take extra care about the physical security of the laptop
- make sure that copies of all important files on the laptop are backed up onto a supported University network file store

For the purpose of ensuring appropriate security and anti-virus protection, University purchased and maintained IT equipment is the preferred means of operating on-campus and remotely. However, by using your own devices you need to be aware that:

- full value may not be received on insurance claims if lost or stolen.
- Anti-virus software may not up to date and appropriate for the University's security purposes.
- IT Support and Services would not be able to prioritise personal equipment when maintaining, servicing and/or repairing.

The University takes no responsibility for you using your own devices.

iii. Health & Safety and Welfare when working from home

The University has a duty to protect the health, safety and welfare of their employees and this includes those who regularly work from home. Home Workers are defined as those people who regularly work at home because of formally agreed arrangements with their managers or are contracted to work at home.

It is the responsibility of the line manager to ensure that appropriate risk assessments are carried out for home workers. Any equipment provided to an employee to use at home remains the responsibility of the University. This might include laptops, power packs/ re-chargers, etc. The domestic electrical supply is the responsibility of the employee as is any equipment owned by them. Approval to work at home, even occasionally, must be given by the employee's line manager in order for them to be covered by the University's insurance.

Working from home and the use of IT will be the same as if you were working within the workplace, and therefore can be assessed as suitable and reviewed by the homeworker. Regular or prolonged use of IT equipment and office furniture should be subject to a Display Screen Assessment (DSE). This can be done by the homeworker using the guidance http://www.hse.gov.uk/pubns/ck1.pdf

The employee should ensure that the home work environment, is to an appropriate work and ergonomic standard. A simple checklist covering such items as the work environment must be completed prior to the agreement to work from home on a regular or prolonged period of time and the employee needs to review annually and submit the form as outlined in Appendix 1 to their line manager. The line manager should keep copies, and act upon any matters of concern, including suspending any working from home until those concerns are addressed.

First Aid: Any home worker must ensure that there are adequate first aid supplies available.

iv. Other relevant policies

Health and Safety http://www.hse.gov.uk/pUbns/priced/l26.pdf

Staff Acceptable Use Policy and Janet Acceptable Use Policy:

https://glynfo.glyndwr.ac.uk/course/view.php?id=114%22%20target%3D%22_blank%22

Data Security Policy for Portable Electronic Devices and Data Storage and Data Protection and Data Disposal Policy

www.glyndwr.ac.uk/en/information-governance/policies/

Guidance on Working Remotely

1. Working while travelling (in transit)

Take care about which WiFi networks you connect to. When connecting to The Internet, make sure that it is password protected to indicate a secure network.

Safer networks - The safer networks are:

- Eduroam (If available to you, this should be your first choice network to attach to)
- your own **private** home network if password protected
- wireless networks run by an institution or company you are visiting

Less-safe (or insecure) networks - Insecure networks are often:

- those found in cafes, bars, and in the street
- public networks that do not require a password to access
- public networks that require your email address, or other personal details to allow you to join

2. Protect against loss or theft of Information, or your devices

When you are travelling, or in a very public place, there is a heightened risk of the following:

- that your computer or device is stolen or lost, or left behind
- that someone may see sensitive information you are working on
- someone may overhear you if you are talking about anything sensitive
- someone may see your PIN or password, or, if determined, they may even have filmed you, or filmed your reflection in a window.

3. Ten Basic Security Rules

i. Never reveal or share passwords. Do not write them down unless absolutely necessary.
ii. Lock your computer or completely log off whenever you leave your workstation; do not rely on the automatic screen lock.
iii. Never store personal information on your local drives or desktop, use network storage instead.
iv. Turn off file and printer sharing on your computer, if applicable
v. Consider if emails containing personal data should be encrypted, content depending.
vi. Encrypt all sensitive data held on USB drives, CDs or laptops.
vii. Immediately report lost or stolen items like laptops, mobiles, USB drives and ID cards through the appropriate channels (see above).
viii. Verify the security of online payment systems you use.
ix. Limit print outs to information that is not sensitive. Dispose of printouts by using the confidential waste bins, shredding the documents does not make them unreadable.
x. Secure your computer by configuring it to automatically check for software updates - especially up to date antivirus software.

No further advice is offered other than to urge you to be aware of these, and to take measures to reduce the risk. Hide your PIN or password while typing it. Do not talk loudly about sensitive issues. Do not leave sensitive documents in plain view. Do not leave your laptop bag or personal belongings on the floor or back of a chair whilst in a café or restaurant or leave them in your car whilst shopping or eating out.

APPENDIX 1

Homeworking self-assessment checklist

This form should be completed initially by the homeworker and returned to the line manager. Any matters of concern should be resolved before home working commences. The responses should be reviewed annually, and at any time if significant changes occur

	Yes	No	N/A
1**.General**			
Have you read and understood the University guidance on remote working?			
2. Fire			
Is the work area tidy?			
If not can you tidy it now?			
Are your exit routes of your home clear?			
Do you have smoke alarms fitted and tested?			
Are waste materials regularly disposed of to avoid accumulation of combustibles?			
3. Electrical Equipment			
Is the means of switching off equipment readily available?			
Is there adequate space around the equipment for access and cooling?			
Are the flexible leads in good condition (free from cuts, fraying and damage etc.)?			
Is the socket outlet in good condition (e.g. not cracked or damaged or showing any signs of overheating etc.)?			
Does the equipment switch on and off properly?			
Are cables securely fixed in all plugs?			
Are the correct value fuses fitted?			
4. DSE			
Have you carried out a DSE workstation assessment			
5. Home Security			
Is your home wifi secure to enable you to work securely at home?			
Do you have secure area for sensitive work, if in paper form?			

To be completed by home worker/line manager as appropriate

List any matters of concern which needs attention before homeworking starts:

Home Worker's name:	Date:
Home Worker's signature:	

The matters of concern raised above have been addressed and home working is agreed.
Line Manager's (name):
Line Manager's signature:
Date: