Smart Working & Security

1 INTRODUCTION

Whilst the University expects its employees and staff to comply with this policy, it does not confer contractual rights or form part of any contract of employment and may be amended by the University or replaced at any time following appropriate consultation and negotiation with recognised trade unions. Breach of this policy may be addressed via the University's Disciplinary Policy and Procedure and Code of Conduct.

This policy will be reviewed by the IT Resources and Human Resources department on a 3-year basis or amended in response to changes in future legislation and/or case law.

2 OWNERSHIP

The IT Services and Human Resources department owns and manages this policy on behalf of The University of Northampton.

3 ORGANISATIONAL SCOPE

This Remote Working & Hot Desk policy is a corporate policy and applies to all employees (and workers, as applicable) of The University of Northampton including any wholly owned subsidiaries, unless an alternative policy exists, subject to any qualifying conditions.

4 POLICY STATEMENT

The purpose of this policy is to define best practices for secure remote working onto the University of Northampton (UoN) network and associated systems via a web browser or a University approved VPN client.
This will be achieved by granting secure access via a series of industry approved security protocols thus, reducing the potential threat inherent in using a non-secure means of remote access.

5 DEFINITIONS

Users
All parties who have been granted access to the University's IT Resources. This includes students, all workers and employees of the University including those within wholly owned subsidiaries, contractors, agency workers, consultants, suppliers, customers and business partners.

Authentication
A process that ensures and confirms a user's identity.

VPN
A virtual private network (VPN) is a technology that creates a safe and encrypted connection, over a less secure network, such as the internet. VPN technology allows employees to securely access business applications and other resources. To ensure safety, data travels through secure tunnels and VPN users must use authentication methods, such as passwords, to gain access.

Encryption
Encryption is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.

Wi-Fi
A wireless networking technology that allows computers, smartphones or other devices to communicate over a wireless signal within an area.

Anti-virus
Software designed to detect and remove viruses from a computer.

BYOD
The practice of allowing employees of an organisation to use their own computers, smart phones or other devices for work purposes.

6 KEY PRINCIPLES

Users of mobile computing equipment should be provided with carry cases as necessary to reduce the risk of damage, theft or loss.

Any sensitive or confidential hardcopy documents must be securely stored when not in your immediate possession. If no secure storage is available, then they must not be removed from University premises, and ideally not printed out in the first instance.

When accessing the University's systems or data from remote locations all users must comply with the following requirements:

6.1 Connecting to the University network

- Citrix will be used as the primary method for remote access to front end systems.
- Requests for VPN access should be made directly with the IT Service Desk.
- Remote access into the University of Northampton's network will be logged.
- It is the responsibility of employees with VPN privileges and the sponsors of the third party professionals to ensure that unauthorized users are not allowed access to The University of Northampton's internal networks.
- By using Citrix access technology on personal devices (BYOD), users must understand that their machines are an extension of the University of Northampton's network, and as such are subject to the same rules and regulations that apply to University owned equipment, including the Bring Your Own Device Policy.
- All computers connected to the University of Northampton internal networks via VPN or any other technology must ensure that the appropriate security protection is in place (patching, anti-virus updates etc.), and that they follow the Acceptable Use Policy.

6.2 Public spaces

When accessing University systems while in a public space you should note the following:

- Public hot spots are not to be trusted even if they state that they are secure. Any access to University systems must only be via the University's secure VPN.
- If connecting to University systems, sit with your back to a wall to prevent shoulder surfers viewing University data and/or noting your authentication credentials.
- Consider the use of privacy screen filters if you spend a significant amount of time working in public spaces.
- Do not place any sensitive or confidential paperwork in public view. Ideally such material should only exist in softcopy form except while in a secure University location.
- Do not leave your laptop or smartphone unattended.
- Damaged, lost or stolen equipment must be reported to IT immediately.
- Do not use internet café provided devices to access University systems as the contents of the screen can be copied, and your logon credentials can be recorded.
- Do not discuss sensitive or confidential subjects within earshot of members of the public.

6.3 Home or Hotel room

- Hotel wireless should always be considered insecure. Only access University systems via the University's own secure VPN.
- If a cross-cut shredder is available then this can be used to dispose of confidential or sensitive documents, however you must witness the shredding of the documents yourself and not leave them with hotel staff to do when convenient.
- The user is accountable and responsible for their IT account (username and passwords) and how it is used. The user must ensure they take reasonable steps to ensure their IT account does not get compromised or used by somebody else. For example: using shared devices (home equipment) when the system may inadvertently stay logged in between users.

6.4 Hot Desks

When using a University of Northampton hot desk, you should note the following:

- Do not leave confidential or sensitive hardcopy on the desk when you are not in attendance
- Do not discuss confidential or sensitive subjects within earshot of teams whose access to this information is inappropriate
- Lock your screen when leaving your desk.

6.5 Education and awareness

Users shall be provided with instructions with regards to using mobile equipment securely:

- Protection of laptop
- Use of encryption to protect business information
- Backups of information
- Users are required to report any loss, damage or theft of computing equipment, as soon as possible, directly to IT Services.

7 PROCEDURE

7.1 Security protection

To ensure computers connecting to the UoN internal networks are appropriately secure:

UoN IT Device:

1) Ensure the laptop is turned on regularly and connected to a secure WiFi. This will allow updates and anti-virus scanning to be performed regularly.
2) Make sure you shut down your laptop each day.

Personal Device (BYOD):

1) Ensure your laptop is turned on regularly and connected to a secure WiFi. This will allow updates and anti-virus scanning to be performed regularly.
2) Download and/or purchase credible antivirus software to keep your personal device secure.

3) Make sure you shut down your laptop after each use.

8 ASSOCIATED DOCUMENTS

Acceptable Use Policy

9 EQUALITY IMPACT ASSESSMENT

An Equality Impact Assessment has been completed with this policy.

10 VERSION CONTROL

Version Control	1.0	**Approval record**	
Author:	IT Services	Approval:	TU Liaison – 18/09/2018 UMT – 09/10/2018 Boar – 11/12/2018
Date written:	August 2018		
Current status:	Live		

Record of Amendments			
Date	Version number	Details of Change	Approval