Information Security Remote working Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins

Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	03/04/2017
V 0.2	Andrew Clarke	PWG Technical amendments and exceptions	06/04/2017
V 0.3	Andrew Clarke	Policy renamed from Teleworking to Information Security Remote working – approved CISA	21/04/2017
V 1.0	Andrew Clarke	Approved Information Subcommittee	27/04/2017
V 1.1	Andrew Clarke	Appendix A – International Travel	06/03/2019
	Andrew Clarke	Annual review	09/04/2019
	Andrew Clarke	Annual review	06/05/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 27 Apr 2017
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 27 Apr 2017
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering Teleworking and Mobile Device Remote Access.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Systems Manager	Is responsible for maintaining and managing systems policies on IT systems and infrastructure and ensuring that remote teleworking complies with this policy.
Network Manager	Is responsible for maintaining and managing network policies on network systems and ensuring that remote teleworking complies with this policy.
Head of Development and Application Services	Is responsible for maintaining and managing password policies on application and web systems and ensuring that remote teleworking complies with this policy.
Cyber & Information Security Manager	Is responsible for maintaining Remote Access policy best practice and ensuring compliance with legislative and regulatory requirements.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A6 – Organisation of information security
ISO 27001:2013 Conformance Control	Information Classification Objective A.6.2.1 Mobile Device Policy A.6.2.2 Teleworking & Remote working security

1.4 Scope

The scope of this policy applies to:

- Brunel University employees, contractors, vendors and agents with a Brunel University-owned or personally owned computer or workstation used to connect to the Brunel University network from a remote location;
- Information system resources, including data networks, LAN servers and PC (stand-alone or network-enabled) located on Brunel University London and non-Brunel University London locations, where these systems are under the jurisdiction and/or ownership of Brunel University London, and any personal computers and/or servers authorised to access Brunel University London's data networks;
- Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.
- Remote access connections used to do work on behalf of Brunel University London, including reading, sending email and viewing intranet web resources from all types of equipment.

1.5 References

- CESG Good Practice Guide (GPG) 10 - Remote Working v2.2
- Brunel University London Virtual Private Network (VPN) Policy
- Brunel University London Acceptable Use Policy
- Mobile Computing Policy

1.6 Policy Objectives

The objectives of this policy with regard to the protection of information system resources against unauthorised access from remote locations are to:

- Minimise the threat of accidental, unauthorised or inappropriate access to either electronic or paper-based information owned by Brunel University London or temporarily entrusted to it and to limit damage including the loss of sensitive or University confidential data, intellectual property, damage to public image, damage to critical Brunel University internal systems;
- Minimise Brunel University London's network exposure, which may result in a compromise of network integrity, availability and confidentiality of information system resources;
- Minimise reputation exposure, which may result in loss, disclosure or corruption of sensitive information and breach of confidentiality; and

- Define standards for connecting to Brunel University's network from any host. These standards are designed to minimise the potential exposure to Brunel University from damages, which may result from unauthorised use of Brunel University resources.

1.7 Policy Overview

Brunel University London information system resources are important business assets that are vulnerable to access by unauthorised individuals or unauthorised remote electronic processes. Sufficient precautions are required to prevent and detect unwanted access from unauthorised users in remote locations. Users should be made aware of the dangers of unauthorised remote access, and managers should, where appropriate, introduce special controls to detect or prevent such access

1.8 Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an ongoing basis by Brunel University London. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from Brunel University London intranet (IB) or other relevant communication media on an ongoing basis and accept the terms and conditions contained therein.

2.0 Teleworking Policy

2.1 Policy Summary

The purpose of this policy is to protect the confidentiality, integrity and availability of Brunel University London's information by controlling remote access to University Information Services (IS) systems by Brunel University London's personnel, temporary staff, contractors, students and service providers utilising Brunel University London's information system and to define standards for connecting to Brunel University London's network.

Brunel University London's IS resources are assets important to Brunel University London's business and stakeholders and its dependency on these assets demands that appropriate levels of Information Security be instituted and maintained. It is Brunel University London's policy that appropriate remote access control measures are implemented to protect its IS resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such IS resources.

2.2 Policy Requirements

- It is the responsibility of Brunel University London's employees, contractors, students and temporary staff with remote access privileges to Brunel University London's network to ensure that their remote access connection is given the same consideration as their on-site connection to Brunel University London;
- General access to the Internet for recreational use by immediate household members through the Brunel University Network on personal computers is permitted for employees (although not recommended). The Brunel University employee is responsible to ensure the family members do not violate any Brunel University policies, do not perform illegal activities, and do not use the access for outside business interests. The Brunel University employee bears responsibility for the consequences should the access be misused;
- IT equipment provided to the employee to support working from home is for the exclusive use of that employee alone;
- The only permitted remote access method for non-Brunel University London computers is via the Connect Portal VPN;
- Managed mobile devices [running the SLM Windows build and registered with SCCM] and Community [Brunel owned and unmanaged] mobile devices e.g. Laptops, Blackberry's, smartphones, iPhones and iPads are supported by Brunel University London for remote connectivity;
- Users are permitted to connect their personal mobile devices to Brunel University London email system. However, the IS Service Desk will only provide support for this method of connection on a goodwill basis. Furthermore, it is the

responsibility of the user to ensure that their personal mobile device is protected by a password. If that device is lost or stolen then it is the responsibility of the user to advise their mobile provider and arrange for the device to be removed from the service. If the IS Service Desk believes that access to Brunel University London email systems is occurring without adequate security provisions, this facility will be withdrawn immediately and a request for the mobile device to be wiped will be issued;

- At no time should any Brunel University employee provide their login or email password to anyone, not even family members.
- Brunel University employees and contractors with remote access privileges must ensure that their Brunel University-owned or personal computer or workstation, which is remotely connected to Brunel University's corporate network, is not connected to any other network at the same time, with the exception of home or personal networks that are under the complete control of the user.
- Brunel University employees and contractors with remote access privileges to Brunel University's corporate network must not use non-Brunel University email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Brunel University business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the Brunel University network must meet minimum authentication requirements of CHAP. [Ref. Appendix A – Definitions]
- Reconfiguration of a home user's equipment for the purpose of split-tunnelling or dual homing is not permitted at any time.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Non-standard hardware configurations must be approved by Information Systems and Cyber & Information Security must pre-approve security configurations for access to hardware.
- All hosts that are connected to Brunel University internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Remote Access Support Policy Agreement.
- Personal equipment that is used to connect to Brunel University's networks must meet the requirements of Brunel University-owned equipment for remote access.
- Organisations or individuals who wish to implement non-standard Remote Access solutions to the Brunel University production network must obtain prior approval from Remote Access Services and InfoSec.

2.3 Documentation and Data

- All University Confidential documentation being used at a remote location must be securely stored and not displayed in a manner which allows its content to be viewed by unauthorised persons.
- University Confidential data and documents belonging to Brunel University London must not be stored on personal equipment unless permission from the Line Manager has been obtained. Any data stored on personal equipment must be encrypted, using advice obtained from the Cyber & Information Security Team for Windows, LInux and Android devices.

2.4 Working Remotely

- Employees wishing to work from their own equipment should ensure that their hardware and software configuration complies with Brunel University London's minimum requirements. It is the responsibility of the user to ensure their equipment is patched accordingly. The IS Service Desk will advise the user only on suggested actions but they will not action any changes to non-Brunel University London equipment.
- Brunel University London will retain ownership of community devices and equipment.
- The employee must take good care of the equipment and ensure that it be used in accordance with Brunel University London's full range of policies.
- When working in a public area, for instance on a train, the employee must take all reasonable steps to ensure that Brunel University London's information remains confidential and secure. The employee must ensure that any documents/laptop screens are, as much as possible, not readily visible to members of the public.

2.4.5 Trusted and Untrusted Access

Access to Brunel University of London services may be denied, withdrawn or require further steps (such as providing multiple factors of authentication – see MFA Policy) based on a number of conditions including (but not limited to) who you are, the device you are using, your location, the date/time and what you are attempting to do.

Examples include:

- *Denied: Jailbroken or rooted Apple iOS and Andoid mobile devices*
- *You: If you are a student / member of staff, the department you belong to, the type of job you do*
- *Device: If the device is managed by Brunel or is a BYOD (Bring Your Own Device e.g. untrusted), the operating system, the security conditions (e.g. antivirus, encryption, pin code etc)*
- *Location: If you are on the University secure network, on the campus visitor network, if you are in the UK, if you are in Europe etc*
- *Time/Date: If you are within business hours, is it the middle of the night etc*

2.5 General Rules & Principles of Virtual Private Networks (VPNs)

Approved Brunel University students, employees and authorised third parties (contractors, vendors, etc.) must utilise the benefits of the University provided VPN for remote access to University resources.

- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
- Dual (split) tunnelling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by Brunel University network group.
- All computers connected to Brunel University internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (BUL Connect Portal Security Requirements) this includes personal computers.
- VPN users will be automatically disconnected from Brunel University's network after thirty minutes of inactivity. The user must then logon again to reconnect to

the network. Pings or other artificial network processes are not to be used to keep the connection open.

- The VPN concentrator is limited to an absolute connection time of 24 hours per session.
- Users of computers that are not Brunel University-owned equipment must configure the equipment to comply with Brunel University's VPN and Network policies.
- Only the Brunel-Cisco-approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Brunel University's network, and as such are subject to the same rules and regulations that apply to Brunel University-owned equipment, i.e., their machines must be configured to comply with Brunel University's Security Policies.

2.6 Reporting Security Incidents

All security incidents, including actual or potential unauthorised access to Brunel University London's information systems via remote access, should be reported immediately to the Head of Security and Emergency Planning or Cyber & Information Security Manager.

2.7 Business Continuity

Business continuity plans may include provision for working from home or other remote locations in the event of Brunel University London's campus or other premises being unavailable for a significant period of time.

2.8 User Awareness

Users commencing remote working will be made aware by their Line Manager of this policy and all its provisions.

2.9 Disciplinary Process

Brunel University London reserves the right to audit compliance with this policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with Brunel University London's Rules and Disciplinary Code as amended from time to time.

4.0 Appendix A – International Travel

The University is increasingly reliant on fast, reliable access to a wealth of digital information, even while travelling, particularly in relation to academic research. The demand for remote instant access to the virtual office regardless of location or time of day via the use of portable electronic devices which can offer the traveller both communications services and secure access to University critical data is increasing exponentially.

Devices such smart phones, laptops and tablets can all be secured, but the person operating them, and indeed accessing data remotely, must be made aware of the associated risks they face whilst travelling on international business and to follow this policy and guidelines to mitigate the risk.

Staff and students who are travelling internationally on University business must be familiar with what measures they can take to limit the potential for threats to expose vulnerabilities and create risk, they also need to understand that the very measures designed to protect them, can also bring about unforeseen challenges when crossing international borders.

This advice can be found within the Travel Booking system that the University provides to arrange all travel and accommodation in relation to University business (Ian Allen Travel) or from Terry Vaas, Head of Security And Emergency Planning

For example, such is the risk of compromise in some high cyber risk countries that an expectation exists whereby any devices taken into the country will be accessed remotely and unencrypted data copied as a norm. This makes it essential that international travellers are fully briefed regarding ICT entry requirements into each country, particularly those assessed as high ICT risk (including Bahrain, China and Russia) and that they are provided with the necessary training to understand what mitigation measures should be implemented before travel. However, there are also instances where the measures deployed by border security agents in western countries have also placed sensitive corporate data at risk, and this is something which the traveller cannot control or mitigate against.

Recommendations:.

- Always take ‘clean’ equipment where possible. The University offers clean loan laptops for travel, loaded only with what is needed for that business trip. Any University Confidential information can then be accessed over the internet once arrived at the destination and deleted before returning.
- Follow University encryption guidelines - BUL-POL-10.1 - Cryptographic Policy. University research data can be subject to suspicion if academics and students undertake their research abroad.
- Ensure you are aware of the rules surrounding encryption, and the legality of entering a country with an encrypted device.
- Password protect all devices using strong complex password layers and ensure that both University and personal devices are protected, where possible, by a multi-factor authentication process.

- Disable remote connectivity such as Bluetooth, Wi-Fi, and file sharing when not in use, and always decline to allow others to connect a USB or portable device to any equipment but especially a laptop or mobile phone.
- Plan ahead – understand that there is a possibility you may be questioned by customs officials. Carrying a headed letter in the local language stating that your equipment uses commercial encryption software and that the information is normal business information in relation to your role, might prove to be useful if you do face questioning at a border.
- Never use USB drives or software received as gifts or promotional items until they have been verified clean by the University IS department.
- Backup important data that will travel with you.
- Assume all internet connections as insecure and use a VPN at all times.
- **Do not** plug your device into USB charger kiosks in airports, hotels or other public places[1]. These may be infected with malware that will be uploaded to your device that may result in your device being compromised and data being stolen.
- Disable remote connectivity such as Bluetooth, Wi-Fi, and file sharing where possible.
- Do not leave devices unattended. Even hotel safes should not be considered secure.

[1] If using a USB Data Blocker then charge points may be used – A USB Data Blocker will eliminate the risk of infecting your phone or tablet with malware, and even prevent criminals installer/executing any malicious code that enables access your data.

		Russia / China / Iran	USA	EU	ROW	Other risky countries (1)
Threat						
	Theft of Data	✔	☐	☐	☐	✔
	Acquisition of Data	☐	✔	✔	✔	
TTPs						
	Security checkpoint requisition - Be prepared to turn on and off devices, and present all removable media for customs officials. You may be asked to decrypt data for inspection at international borders. In some countries, withholding your password is a criminal offense.	✔	✔	✔	✔	✔
	Man in the middle attack - method by which attackers manage to interpose themselves secretly between the user and a web service they're trying to access. For instance, an attacker might set up a Wi-Fi network with a login screen designed to mimic a hotel network; once a user logs in, the attacker can harvest any information that user sends, including banking passwords.	✔	✔	✔	✔	✔
	Eavesdropping attack - Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network	✔	✔	✔	✔	✔
	Phishing and spear phishing attacks - likely to be targeted with specific details about the visit abroad increasing complacency as recipient may have advertised the visit	✔	✔	✔	✔	✔
	Social engineering - Unsolicited contact in a social environment may not be what it purports to be. The intention is to gain intelligence through the source and human relationships.	✔	☐	☐	☐	✔
	Pen drive scam - introduction of malware. Free Pen Drive/Gifted Pen Drive following a show or host.	✔	✔	✔	✔	✔

	Surveillance from voice / locations etc. Phone calls, electronic communications and even hotel rooms may be monitored as a standard practice.	✔	☐	☐	☐	✔
Controls before departure:						
	Delete email accounts on devices, both social and University	✔	☐	☐	☐	✔
	Briefing to all staff before travel from cyber team	✔	✔	✔	✔	✔
	No data on local drives	✔	☐	☐	☐	✔
	Issue advisory notices on social engineering TTPs	✔	✔	✔	✔	✔
	Change all passwords on all devices and use different passwords on each. Remove or limit biometric data for authentication. Biometrics have been used before in court cases to compel humans to unlock their phones (unwillingly). The factor of "something you know" literally cannot be compelled in a court of law or other situations	✔	☐	☐	✔	✔
	Enable multi-factor authentication on all accounts used on your device that support it.	✔	✔	✔	✔	✔
	Ensure full-disk encryption on laptops.	✔	✔	✔	✔	✔
	Encrypt mobile phones and tablets (android and apple) - Configuring automatic wiping settings to wipe the device's data after a pre-determined number of passcode entry failures	✔	✔	✔	✔	✔
	Provide "loaner" laptops and burner phones and/or tablet to limit the loss of both University and personal data if the device is lost, stolen or confiscated by officials.	✔	☐	☐	☐	✔
	Issue temporary email accounts.	✔	☐	☐	☐	✔
	Purchase and install a glass "privacy screen cover" to prevent shoulder surfing	✔	✔	✔	✔	✔
	Limit or minimise any data taken to include removable media such as CDs, DVDs and thumb drives.	✔	✔	☐	✔	✔
	Perform a full device back up and secure with a strong password. Store it in a secure location while you are away.	✔	✔	✔	✔	✔

	Inform banks and credit card companies of travel plans to include dates, locations and any special instructions. International transactions are typically flagged as fraud, and purchases may be delayed or your card can cancelled without advanced travel notice.	✔	✔	✔	✔	✔
	Consider using virtual credit card numbers that offer one-time use and are disposable, yet will display on the credit card bill.	✔	☐	☐	☐	✔
	Pack only essential ID, credit and debit cards. Leave the others in a secure location.	✔	✔	✔	✔	✔
	Update data protection software such as operating systems, anti-malware, anti-virus, security patches and others prior to departure. After you have updated the device, turn off automatic updates in the device and app store	✔	✔	☐	✔	✔
	Delete all saved Wi-Fi networks your device has “previously connected to” Your device will attempt to login to previously connected networks, and someone can log those probes including the passwords.	✔	☐	☐	✔	✔
	Disable “side-loading”, which is a way for the device to allow installation of software from 3rd parties not using the trusted app store.	✔	✔	✔	✔	✔
	Turn on ‘find my phone’ features and ensure the device is configured to send the last known location. Test to make sure it works from another device or from the related website.	✔	✔	✔	✔	✔
Controls while on travel (You have no reasonable expectation of privacy in some countries):						
	Do NOT leave your device unattended.	✔	✔	✔	✔	✔
	Sensitive or confidential conversations, transactions or data transfer should be kept to a minimum until you return home.	✔	✔	✔	✔	✔
	Use the same rules for your personal and University devices to separate acceptable social networking communications versus sensitive transactions. Understand there is a difference	✔	✔	☐	✔	✔

	between sharing a photo on social networking versus connecting to your bank or credit card company.					
	Use end-to-end encrypted applications (like Signal) for communications. SMS is not secure. 1) Monitor your device's network traffic to determine if any unencrypted communications occur and address, as needed. 2) Google Voice provides encrypted messages on all of your devices, e.g. for MFA one time login codes. 3) Use an application like Wickr or Wire that can automatically delete messages after a certain amount of time.	✔	☐	☐	✔	✔
	Use safe ATMs in public areas during daylight. Cover PIN entry and cash output as much as possible.	✔	✔	✔	✔	✔
	Determine the availability and cost of purchasing a local mobile phone, prepaid local phones limit costs by not working after exceeding a maximum number of minutes. They are cheaper for local calls and have better connectivity. Buying local SIMs, especially PAYG, adds a level of anonymity, which may be good for privacy/security. Obtain and install a local SIM card ONLY IF NEEDED, plugging anything unknown into your device is dangerous.	✔	☐	☐	✔	✔
	Use trusted VPN connections as much as possible. If you don't have a VPN available, use HTTPS connections as much as possible.	✔	✔	✔	✔	✔
	Follow the principle of least privilege. While traveling you will likely be connecting to many new, probably poorly managed, and potentially unsafe networks (e.g. in airports and hotels). Expect to be targeted by malicious users on these networks. Do not use an administrator account as your primary user account.	✔	✔	✔	✔	✔
	Work only from MS OneDrive	✔	✔	✔	✔	✔

	Connections in cyber cafes, public areas and hotels can be safe with a VPN, but should otherwise be considered insecure and probably monitored by state agents and/or criminals. Physical PCs in such places may contain keystroke logging or other malicious methods to gather your information.	✔	☐	☐	✔	✔
	Do not loan your device to anyone, or attach unknown devices such as thumb drives. Thumb drives are notorious for computer infections.	✔	✔	✔	✔	✔
	Disable device illicit access via wireless technologies by: 1) Using airplane mode to disable or suspend all connectivity. 2) Disabling Wi-Fi when not in use. Wi-Fi ad-hoc mode or unsecure file sharing enables direct access to devices. 3) Disabling Bluetooth when not in use (or set it to “hidden,” not "discoverable”). Consider rental car Bluetooth PBAP (Phone Book Access Profile) functionality loads the entire address book, while Bluetooth (Personal Area Network) functionality enables connections with other Bluetooth devices. 4) Do not automatically join any wireless networks from laptops, tablets, or mobile phones. Manually pick the specific network you want to join.	✔	✔	✔	✔	✔
	Report lost or stolen devices as soon as possible to whomever it concerns. This might include the University, mobile provider, hotel, airline, insurance company and/or local authorities. Local authorities have a better chance to find stolen property if it is reported stolen as soon as you know it is missing.	✔	✔	✔	✔	✔
Controls Upon Returning Home (Very simply, assume that you have been compromised while traveling abroad and act accordingly):						
	Return the loaner device(s).	✔	☐	☐	☐	✔
	Have all devices, media and thumb drives reviewed for malware, unauthorised access or other corruption. Do not connect it to the University network until you have tested it for malware.	✔	✔	✔	✔	✔

	If the device is found to be compromised, contact IS/College IT to reformat it and rebuild it from trusted sources/media. Then restore data from backups taken before the trip.	✔	✔	✔	✔	✔
	Change all University and personal passwords. If possible, change the passwords for things like University network accounts, banks, etc., using a device other than the one you travelled with.	✔	☐	☐	☐	✔
	Change all passwords on all devices and use different passwords on each	✔	☐	☐	✔	✔
	Inform your bank or credit card companies of your return and review transactions.	✔	✔	✔	✔	✔
	Continue to monitor your business and personal financial institution transitions for unauthorised or unapproved use.	✔	✔	✔	✔	✔
Damage to University						
	Loss of high grade IP data	✔	✔	✔	✔	✔
	Loss of personal data and data breaches	✔	✔	✔	✔	✔
	Loss of commercially sensitive data	✔	☐	☐	✔	✔
		☐	☐	☐	☐	
Risk score		HIGH	MEDIUM	LOW	MEDIUM	HIGH
Type of Data						
	Intellectual Property	✔	✔	✔	✔	✔
	Personal data	✔	✔	✔	✔	✔
	Commercially sensitive data	✔	☐	☐	✔	✔

(1) Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao PDR, Syria, Yemen, Pakistan, Democratic People's Republic of Korea

Other HEI's

In Summary;

The significant majority of respondents offered staff (usually via a policy) who are traveling to certain countries a clean laptop and a burner phone, on return to the UK these are flattened.
Other respondents also indicated that staff who travel with either their own or University devices were heavily encouraged (some had polices) to not access any services where data may be stored, use a secure VPN, don't use public Wi-Fi and when returning to the UK do not connect to University systems/services until a complete check had been carried out on all devices which could result in the devices being flattened

Staff traveling to China, North Korea, Iran, or the United States should not take any electronic gear with them; i.e. laptops, smart phones, tablets, etc.
Any data they may need to access while overseas should be securely transferred before they leave. The only kind
of mobile phone they should carry with them is one that can do no more than make or accept phone calls and, possibly, text messages.
No texts should be stored on the phone. No contact details should be stored on the phone.

If a flash drive is transported to any of these countries, make sure it is encrypted, and pack it in your checked luggage, not your carry-on bags.

The dangers are fairly obvious for the first three countries listed. However, Customs officials in the US are allowed to examine and/or impound any electronic equipment from any traveller, without having or providing a reason for doing so.

Some further advice:

- Keep any documents or electronic equipment which contain personal data or intellectual property out of sight in your hotel room; don't leave them unattended if you are giving a presentation or out in public.
- Password protect and encrypt any documents and electronic equipment; don't write the passwords down.
- Avoid using computers in internet cafes or hotels, as they may be monitored or infected with malware.
- Take a full back up of everything before you go .
- Do not purchase or download new software while abroad as they could be counterfeit or contain malicious programs.
- Do not have any of your electronic devices repaired or worked on while abroad.

4.0 Appendix B - Definitions

Term	Definition
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialling into AOL or other Internet service provider (ISP). Being on a Brunel University-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Brunel University and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the service provider’s network.
ISDN	There are two flavours of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signalling info.
Remote Access	Any access to Brunel University's corporate network through a non-Brunel University controlled network, device, or medium.
Split-tunnelling	Simultaneous direct access to a non-Brunel University network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Brunel University's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunnelling" through the Internet.