Aston University

IT REMOTE WORKING POLICY

This document sets out the University's policy regarding IT Remote Working.

Version	2021.7 Final
Executive Sponsor	Chief Operating Officer
Officer Responsible for Policy/ Procedures	Director of Digital Services
Consultation Process	Executive Operations Group
Date of Approval and Committee and/or Executive Officer	Executive Senate Council
Effective Date	July 2021
Reviewed:	Annually

INTRODUCTION AND CONTEXT

The Covid-19 pandemic was a significant catalyst for agile and remote working. An ever increasing amount of people now find themselves in a position where they are working from home or a remote location for at least part of the working week.

It is the person's responsibility to take adequate care and precaution in respect of any IT hardware asset(s) provided by Aston University (for example, notebooks, smartphones and tablets). This is in addition to any data or information accessed whilst using these devices as defined in the IT policy suite.

1. SCOPE OF THE POLICY

1.1 Purpose of the Policy

This Policy aims to set out relevant information to assist users to adapt to working remotely in a safe and secure manner. Although working from home or remotely can benefit both the organisation and the individual, care must be taken to ensure any new risks that may emerge from this change in working practice, are mitigated.

1.2 What is covered by the Policy

This Policy sets out:

- The use of University and personal devices whilst working remotely.
- Precautions to take when in a remote location or travelling with devices nationally and internationally.
- Dealing with data remotely.
- Loss/theft of devices.
- Connecting external devices to your device.
- Wellbeing and safety.
- Getting support.

1.3 Who is covered by the Policy

This Policy applies to all University staff members and all third parties working on behalf of the University, this includes staff, contractors, volunteers etc. Only students who have been provided with a University IT hardware asset are included. Most students use their own IT equipment and their data has the relevant controls in place, where required.

1.4 Breach of this Policy

Accidental breaches of this policy should be reported to Digital Services IT Helpdesk and we encourage staff to highlight such instances so we may minimise any issues that may arise from this.

Breaches of this Policy are treated on a case-by-case basis and could constitute a disciplinary matter depending on the seriousness, if any malice was intended and if it was reported responsibly.

If the breach occurs due to contractors or third parties, then this may constitute breach of contract with the third party involved.

1.5 Policy Ownership

The Executive has approved this Policy, the Chief Operating Officer is the Executive sponsor and the Director of Digital Services is the officer responsible for the Policy. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Director of Digital Services.

2. THE POLICY STATEMENT

2.1 Guiding Principles

The guiding principles and prerequisites of this Policy are as follows:

- You have completed the Aston Cyber Security mandatory training in BlackBoard VLE and that all other mandatory training has been completed to a pass such as GDPR, Prevent, Health and Safety, Fire Safety;
- You have obtained confirmation from your line manager that you may take the relevant equipment home. This evidence may be required if challenged by Security when leaving the Campus;
- A DSE self-assessment must be completed for any location where you may work regularly such as at home.

2.2 Associated Procedures

This Policy forms part of the IT policy suite, which you are required to have read and understood. It is designed to supplement the supporting policies:

- IT Security Policy;
- IT Acceptable Use Policy;
- IT Monitoring Policy; and
- Privacy Policy.

3. UNIVERSITY PROVIDED DEVICES

3.1 Introduction

It is important to always use an Aston University provided device. Most users will already have a notebook as their University provided machine but Digital Services IT Helpdesk can offer limited loan devices, if required. These should be the default method of access to University services as Aston University provided devices have numerous safety controls and protections built in to keep the device, University information and its Infrastructure secure. They provide the required reporting capabilities for our regulatory compliance obligations. If a member of staff has not been provided with a notebook to work on, this can be raised with Digital Services Helpdesk.

3.2 Personal desktops/notebooks

Each member of staff is assigned a device (in the majority of cases, an encrypted notebook) when they start their employment and this device should be used in all cases.

Use of personal desktops or notebooks by staff for University business is not recommended for reasons including compliance with data protection law, ability for Digital Services Helpdesk to support your device, reliability, backups and access to the University's services.

Students may use their personal devices; we provide a dedicated public Wi-Fi network, which is segregated from our business infrastructure.

4. WORKING FROM HOME (OR REMOTE LOCATION)

4.1 Precautions

In accordance with the Dynamic Working Policy, many staff will work from home or a remote location. The same precautions must be followed when working remotely as when working in the office including the requirements to undertake the following:

- Lock the machine (Windows + L key) if leaving the device for **any** amount of time, whether you are alone or have visitors/family members in the house as visitors may arrive unannounced;

- Switch off when not in use and especially if about to travel. This ensures the data is protected (do not use sleep or hibernation modes) as this the encryption key is then required;
- Family members and friends are not permitted to use the device;
- Keep food/drinks away from the device;
- Do not leave trailing leads when the device is on power, this can be a Health & Safety issue and damage the notebook if tripped over;
- Do not leave on show, place out of sight when not in use;
- Do not place 'post it' notes on the notebook, they can easily fall off and may hold vital information - **never write your password down and/or keep it with the device**;
- Do not use the device on a soft surface for a prolonged period (e.g. cushion, duvet) this can block vents and cause the device to over-heat; and
- Use an appropriate bag with adequate padding and protection when transporting. Consider an alternative to the usual looking notebook bag so it is not obvious to the contents, which can increase opportunist theft.

4.2 VPN

The University has an approved VPN client called Forticlient, which is installed on Aston University work notebooks. It provides an extra layer of security for the transmission of any data through your connection. When using the University notebook from home or another remote location, VPN should be initiated each time the notebook is used if using Wi-Fi in a public space and as regularly as possible when working from home (at least once per week). This allows updates, policies and other important information to be synchronised to your machine as well as affording the extra security during data transmission to keep the data secure. Other VPN providers are blocked and prohibited to help protect data loss from the organisation.

5. TRAVELLING WITH ASTON DIGITAL DEVICES

In addition to the 'working from home' points, when travelling with a University IT asset:

- Do not leave the device unsupervised;
- If using in a public area and handling sensitive/confidential information, a privacy screen filter is recommended to ensure the viewing angle is reduced. Sensitive documents should not be accessed where a member of the public may see your screen and content;
- Do not leave in a vehicle, especially overnight - If this is necessary, keep it out of sight in the locked boot;
- If using on a train or public transport, be aware of your surroundings when operating the device, this is for personal safety reasons but also to ensure no one is able to see any privileged or sensitive information (including watching you enter your password);
- Use hotel safes as they give a secure way of storing expensive items but be aware that hotel management will have access.

6. MOBILE PHONES

Where a smartphone is required for a University role, one will be provided. For those staff that are not provided a work smartphone, staff are permitted to set up work email on their personal device. This use is for checking of emails/calendar appointments only. It is prohibited to download attachments containing sensitive or confidential information onto personal smartphones as adequate protection controls may not be in place for the classification of data being accessed.

7. DOWNLOADING OF WORK FILES/INFORMATION

7.1 University owned devices

Data must be stored in accordance with its information security classification (Open, Public, Confidential, Highly Confidential and Secret) as stated in the IT Security Policy.

7.2 Personal devices

The downloading of files onto personal devices is permitted solely for information that is classified as Open or Public. Notwithstanding staff may store personal documents pertaining to them such as a pay slips.

Any sensitive work related data classified as Confidential or above, is not permitted to be downloaded onto personal devices. It poses a security risk, can contravene data protection law and the IT Security Policy.

8. LOSS/THEFT

8.1 Loss

If a University provided device is lost, staff are expected to make reasonable efforts to retrace their steps to recover the device straight away, but they are unable to locate it then they will need to immediately inform:

- their manager; and
- Digital Services Helpdesk.

A full account of the circumstances will be required, such as date/time & location of the incident. This is for legislative and insurance purposes so we may replace the device as soon as reasonably practical. All University provided devices have an asset label attached to them with the organisation's name and a contact number in case they are found, so the device can be efficiently returned to their rightful owner.

8.2 Theft

If a device has been stolen, the steps set out in section 8.2 will need to be followed and the member of staff will also be required to inform the police and obtain a police incident number, which is needed for insurance purposes.

9. DEVICE CONNECTIONS

9.1 Bluetooth

Bluetooth must be disabled on all devices when not being used. It is commonly left on by mistake and if left on, this greatly increases the risk of being targeted and is often misused to allow a malicious actor to hack into notebooks and phones.

9.2 Wi-Fi

Never connect to any public Wi-Fi including hotels, cafes or fast food services unless it is essential. They often have very weak security and are easily hacked.

Utilise the VPN connection for more protection wherever possible. If in a hotel, perhaps use the room connection rather than in a more public lobby/reception to reduce possibility of data interception.

Only use the connection for the minimum time required and do not use any accounts where data could potentially being leaked. Assume someone has access to everything you are doing whilst connected. Using a VPN can help protect with this in part, but only if that service is not illegal in that country.

9.3 Using public chargers or facilities

It is safe to use your charger in a mains power point however, please refrain from using public charging facilities in areas such as shops, cafes or airports. There are devices that can copy your data through a USB or similar connection without your knowledge and airports can present a risk in this area.

9.4 External storage considerations

Hardware encrypted USB memory sticks and hard drives are available for purchase via Digital Services Helpdesk. Unencrypted external storage is not permitted for University use whilst travelling, especially where sensitive and/or personal data is being stored in accordance with the IT Security Policy.

10. SAFEZONE APP

All staff and students are encouraged to download the SafeZone app to their mobile devices and is available for Apple and Android smartphones from the relevant app store. It is designed with your safety in mind and you are able to check in and out of locations, set as lone working, or even notify Aston University Security Team that you require help or assistance.

11. IT SUPPORT WHEN WORKING REMOTELY

Digital Services Helpdesk will support the University asset throughout its lifecycle. Contact the Helpdesk or raise a self-service ticket in Solve and an engineer will be in touch. This support may be completed remotely if you are not on Campus.

On rare occasions where the issue cannot be resolved remotely, staff may be asked to bring the item to Campus at an agreed time. Staff may be able to wait if it is a relatively quick task, or staff may have to return at an agreed time/date depending on the issue at hand (notebook loans are available where repairs will take an extended period of time).

Where support is needed, if you are working internationally, please bear in mind the difference in time zones but Digital Services will do their best to assist during normal working hours, ‘Norman’ out of hours service is available when outside of University core hours.

12. STAFF WELLBEING

When working from home for periods of time, it is important that users are mindful of the potential negative effects of working from home such as:

- **Working for extended hours -** Try to keep your working hours to a usual working day or agree a flexible working approach with your manager that fits your work/life balance.

- **Lone working/Loneliness -** Be mindful of the Health and Safety issues concerning this and make time to engage with colleagues over video and voice chat. Especially if you/they live alone. This will maintain your connections to your colleagues.
- **Take regular screen and desk breaks** – Get up, walk about, consider going for a walk during your lunch break and break up sedentary habits.
- **Engage with mental health champions or use the PAM Assist service** - to voice any issues of concern or worry.

Please refer to the Dynamic Working Policy for more information.

13. TRAVELLING INTERNATIONALLY FOR UNIVERSITY BUSINESS

13.1 Introduction

When travelling abroad on Aston University business, staff are reminded that travel advice can vary dramatically from country to country due to differences in laws, regulations and local traditions.

It is essential that staff research these areas in advance and develop an acceptable plan in accordance with the University's Health and Safety Policy.

Getting the correct information can often take time, so it is advised to do this as far in advance as possible. As set out in this Policy, staff may need to request certain licenses or gain authorisation to use specific services and leaving this to the last minute may lead to disappointment and delays. There is an article in the self-help Solve site called "*KI 0412 International Travel for Aston business - IT Recommendations*" that provides a short cheat sheet for users travelling or working abroad on Aston University business.

13.2 Before travel

It is essential that staff inform Digital Services Helpdesk in plenty of time regarding the details of your travel arrangements so that each case can be assessed and recommendations can be made based on the requirements for the proposed destination. Country specific advice is subject to constant change and the Digital Services Helpdesk will not be responsible for obtaining the necessary information. The staff member is responsible for compliance with the international travel procedures.

A loan service for qualifying users is offered where a managed iPad can be collected from Digital Services Helpdesk and used whilst away by prior arrangement. When returned, it is then wiped to ensure no user data is retained and in case it has been compromised whilst away, the wipe will remove any malicious software.

13.3 Local laws and regulations

Every destination is different and presents their own set of laws, legislation and requirements when travelling. For example, China, Russia or Saudi Arabia are deemed more restricted countries to visit due to the higher risk of data compromise from state actors.

This highlights the importance of using the Digital Services Helpdesk to review each individual needs. Although the Helpdesk will assist insofar as it is possible within its remit, staff are required to undertake personal checks using Government information and embassy resource subject always to compliance with the international travel procedures. Ultimately, it is the

responsibility of the staff member to verify the local laws and obtain any special permissions required.

Staff should visit the relevant UK Government website, search for the planned destination and review the latest and current travel advice. Accessing the "Local laws and customs" information for the relevant destination should provide the following information:

- Local laws and traditions;
- Travel advice;
- Whether an import licence;
- Blocked websites/services;
- Whether VPNs are allowed (Aston University's notebooks use VPN to maintain extra data security); and
- If the country permits encrypted devices (Aston University's notebooks are encrypted by default to protect the notebook's data).

Staff are advised to submit enquiries on the UK Government website under the 'further help' link if the answer to your question is unclear.

13.4 Import licence

An import licence gives permission to take an encrypted electronic device to a destination. It is the user's responsibility to obtain this and it is advised to do this in plenty of time as it can sometimes take longer to get an import licence than a visa.

Authorities can request that a member of staff show any encrypted devices to them and require the provision of any pins or passwords to access them. Non-compliance could lead to delays or possibility jail.
The University strongly recommends that staff comply, but if staff are required to provide any such information, please change the password/pin as soon as possible afterwards and inform Digital Services Helpdesk of this instance. To verify the requirement for an import licence, staff are asked to contact the embassy of the host country and specifically ask if an import licence is required for encrypted devices.

13.5 Encryption

Most people see encryption as a good thing and a way of protecting information from being accessed by users that should not have access. However, some countries do not permit encrypted devices and staff may be breaking local laws if you were to take an encrypted device into the country.

The University asks that staff not take their IT devices to such countries for the security of Aston University data and also for their own personal safety. As at the date of this Policy, some countries that ban the use of encryption technologies are China, Russia, North Korea & Saudi Arabia. This list is subject to change so staff are required to check before travel. Certain countries have an agreement to allow encrypted devices into the country and this is part of the 'Wassenaar Arrangement'. The UK Government website will provide the required information whether encryption is permitted and whether an import license is required.

13.6 VPN

As with encryption, VPN is a way of securing data. Any data transmitted over the University's in-house VPN is protected. Certain countries do not permit this and actively block VPN connections. Again, the University asks that you check the requirements at your proposed destination before you travel.

13.7 Restricted access to internet or services

Certain countries restrict the use of certain websites or services. Staff are asked to inform themselves that before they travel to their proposed destination. Some blocked or monitored services include:

- Google apps;
- Gmail;
- Yahoo Web mail; and
- Skype video calls.

13.8 On return to the UK

Keyloggers or monitoring over Wi-Fi connections are becoming more common. On return to the UK, staff are required to change their University account password as soon as reasonably practicable if those credentials were utilised whilst overseas to safeguard the University's information security. Staff are also required to change their voicemail password if they accessed their voicemail while outside the UK.

Aston University
Birmingham
B4 7ET, UK

+44 (0)121 204 3000
aston.ac.uk

UNIVERSITY OF THE YEAR 2020 The Guardian

POSITIVE ABOUT DISABLED PEOPLE

Race Equality Charter
RACE CHARTER