Remote and Mobile Working Procedure

inc. Overseas

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

Document Control	
Title	Remote and Mobile Working Procedure inc. Overseas
Date of review	16/06/2025 (annually reviewed)
Document Owner	Zarina Muminova

Version Control History

Date	Paragraph/section amended	Reason	New issue no.
15/01/24	Created		V1
16/06/25	Reviewed		V2

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

1. Overview

The Intech Centre (the Centre) is committed to protecting the information in its possession and the objective of these Procedures is to mitigate the following risks:

- Equipment damage, loss or theft.
- Loss or theft of electronic and hard-copy information.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to the Centre's information assets.
- Unauthorised introduction of malicious software and viruses.
- Potential sanctions against the Centre or individuals imposed by the Information Commissioner's Office as a result of the loss or misuse of personal data.
- Potential legal action against the Centre or individuals as a result of information loss or misuse.
- Reputational damage to the Centre as a result of information loss or misuse.

All employees (which, in this document, includes volunteers and any other individuals who access Centre systems or data) have additional data security responsibilities when working outside the security of internal networks, particularly when working in locations where people not employed by the Centre (e.g. family and friends) are likely to be nearby or even in the same room.

Non-compliance with these Procedures could have a significant effect on the efficient operation of the Centre and may result in financial loss and/or reputational damage and an inability to provide necessary services to our customers.

1. Introduction

The Centre provides employees with the facilities and opportunities to work remotely as appropriate. Portable computing devices are provided to assist employees to conduct official Centre business efficiently and effectively. This equipment, and any information stored on portable computing devices, should be recognised as valuable organisational information assets and safeguarded appropriately.

All ICT equipment (including portable computer devices) supplied to employees is the property of the Centre and must be returned upon the request of the Centre. Access for the staff shall be given to allow essential maintenance security work or removal, upon request.

All ICT equipment will be supplied and installed by the Centre's.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

Only ICT devices issued by the Centre may be used to access Centre emails, accounts, databases etc. It is prohibited to use any personally-owned devices (e.g. PCs, laptops, tablets, smartphones etc.) to do this.

Delivery staff are responsible for ICT equipment in their possession when moving them between work locations, and must ensure that the equipment is protected from loss or theft.

These Procedures are intended to ensure that all employees who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities. They apply also to all employees who work from home or overseas on a permanent or temporary basis.

2. Scope

These Procedures apply to all employees' use of Centre ICT equipment when working on official Centre business away from the Centre's premises (i.e. working remotely).

They apply also to all employees' use of the Centre's ICT equipment to access Centre information systems or information whilst outside the United Kingdom (see section 6 below).

3. Definition

Portable computing devices include, but are not restricted to, the following:

- Laptop computers
- Tablets
- Mobile phones, including smartphones
- Wireless technologies

4. Risks

The Centre recognises that there are risks associated with employees accessing and handling information in order to conduct official Centre business. The mobility, technology and information that make portable computing devices so useful to employees and organisations also make them valuable prizes for thieves. Securing protected or restricted data when employees work remotely or beyond the Centre's network is a pressing issue – particularly in relation to the Centre's need as an organisation to protect data in line with the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation (see the Centre's Data Protection Guidance Notes) and of the Department for Work and Pensions, Ministry of Justice and other commissioning bodies.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

5. Employee Responsibility

It is the employee's responsibility to ensure that the following guidelines are adhered to at all times:

- Employees who work/propose to work from a domestic location must complete the Home Based and Overseas Working Declaration for their line manager to approve.
- Line Manager must upload the fully completed Home Based and Overseas Working Declaration to OneDrive Staff Folder.
- The use of Wi-Fi must be restricted to secure connections (see clause 8 below).
- Employees must take due care and attention of portable computer devices when moving between home/overseas and another business site.
- Employees must take all reasonable precautions to ensure that portable computer devices which have been issued to them are protected from loss or theft. In the event of negligence on the part of the employee, steps may be taken to recover the replacement cost from that employee, who may also not be issued with a replacement device.

6. Remote and Mobile Working Arrangements

- Employees should be aware of the physical security dangers and risks associated with working within any remote office or other remote working location.
- When working in insecure areas make sure your work cannot be seen and, if on the phone, overheard by unauthorised people.
- Screen-lock your devices when you are not actively working on them.
- Actively control any paper based classified records.
- Paper or other media which contain data (for example, CDs, memory sticks, cameras etc.) must be securely locked away when not in use.
- Equipment should not be left where it would attract the interests of the opportunist thief. In the work location, it should also be located out of sight of the casual visitor. For home/overseas working, it is recommended that the working space should be kept separate from the rest of the location. However, if this is not possible, the employee must ensure that, at the end of the day, all equipment and paperwork are removed from sight and securely stored. Equipment should not be shared with other people living with you.
- If a staff member wishes to work abroad, using their Intech Centre equipment, they must obtain the prior approval, in writing, of a senior

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

manager. The employee must complete the Home Based and Overseas Working Declaration, which the employee's line manager will check for completeness, counter-sign and share with the prime contractor, if needed, for approval (speak to SCM and then email to InfoSec@shaw-trust.org.uk). The employee must also be reminded that the equipment must be kept with them at all times whilst travelling, and stored securely when not in use, and in the event of any loss this must be reported immediately to the line manager.

- *Please note the following important restrictions, regarding overseas working, resulting from contractual and/or statutory/ obligations:*
    1. *Employees working at a location outside the United Kingdom are not permitted to access any DWP information whatsoever;*
    2. *Employees working at a location which is outside the UK and outside the European Economic Area are not permitted to access any personal data whatsoever.*
    3. *Only ICT devices issued by the Centre may be used to access Centre emails, accounts, databases etc. at any time or location. It is expressly prohibited to use any personally-owned devices (e.g. PCs, laptops, tablets, smartphones etc.) for any Centre business whatsoever (known as BYOD – Bring Your Own Device). Additionally, it should be noted that DWP has zero tolerance on BYOD.*

    Please contact your line manager, if you need any further clarification, before you start making arrangements to work outside the UK.

- *Please note also that the processes for overseas working must be followed fully and accurately. Due to the possibility of a breach of the Centre's statutory and/or contractual obligations, failure to follow the processes may result in summary suspension of a user's account.*

7. Access Controls

It is essential that access to all the Centre's information assets is controlled. This can be done through physical controls, such as locking the work space and locking the computer. Additionally, it is undertaken through the use of password and user login controls.

Portable computer devices must be switched off, logged off, or the screen locked when left unattended, even if only for a few minutes.

All data must be saved to Centre issued device and OneDrive or prime contractor system.

Please note that all Centre-issued mobile phones (including shared mobile phones) must be locked by a PIN, when not in use.

8. Wi-fi connections:

- It is prohibited to use public connections, such as are offered at internet cafés, retail and other food outlets etc., under any circumstances.
- It is permitted to use private Guest Wi-Fi provided by a 3rd party organisation, but only if it is protected by a complex password and using WPA2 level of security. Evidence must be provided that WPA2 and a complex password are in place. The level of security can be determined by going to 'Settings' and clicking on 'Network & Internet'. Click on 'WiFi' and then select your router (e.g. BTHub6). Scroll down to 'Properties' and look at 'Security type'.
- Password strength can be assessed at this link https://lastpass.com/howsecure.php and passwords should be assessed as "Moderately strong" as a minimum. Alternatively, the Wi-Fi provider must provide the Centre with the number of characters and what minimum combination requirements are in place.
- Non-Centre wireless installations (routers) which are used to carry out Centre business must also be secured to WPA2, with the password assessed as "Moderately strong" as a minimum.

9. Antivirus Protection

Intech Centre will deploy an up-to-date Antivirus signature file to all employees who work away from the Centre's premises.

10. Employee Awareness

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

- All employees must comply with appropriate codes and policies associated with the use of ICT equipment. It is every employee's responsibility to ensure their awareness of and compliance with the Centre's ICT and Information Security Policies, Procedures and Guidance Notes.
- The employee shall ensure that appropriate security measures are taken to stop unauthorised access to restricted information, either on portable computer devices or in printed format. Employees are bound by the same requirements on confidentiality and Data Protection as the Centre itself.
- It is the direct responsibility of the employee's line manager to ensure that the employee has undertaken the relevant Information Security Awareness Training modules.

11. Removal of hard-copy information from the office environment

In the event that classified information is required to be removed from the office or other workplace (e.g. for working remotely, customer or supplier meetings, etc.):

- Ensure that only those specific items required are taken off-site;
- Ensure that a record of what has been removed is maintained and monitored
- Ensure that, while off-site, any such materials are adequately protected;
- Do not make copies of the materials unless absolutely necessary;
- If copies are made, ensure that they are securely destroyed as soon as is practicable;
- Ensure that materials are returned to the office or workplace at the earliest opportunity;
- When the materials are returned to the office or workplace, ensure that they are replaced in the appropriate location;
- In the case of electronic information, ensure that it is deleted from the device as soon as it is no longer required.

12. Disposal of confidential paperwork by home and overseas workers

There are two options available to those remote workers who need to dispose of confidential and/or personal information, which must be stored securely until and out of reach by family members or visitors, until:

1. The homeworker can access Centre premises where there is a cross-cut shredder (P-4 minimum) or

2. The line manager authorises the purchase by the remote worker of a cross-cut shredder as above.

13. Compliance

If any employee is found to have breached these Procedures, particularly with regard to lack of sufficient precautions against loss or theft of portable devices or contravention of the overseas working processes, he/she may be subject to the Centre's disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of these Procedures or how they may apply to you, seek advice from a member of the Senior Manager.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com