

Remote Working Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Statement	3
4. Roles and Responsibilities	3
5. Physical Security Requirements for Remote Working.....	4
6. Systems and Network Security Requirements for Remote Working	5
7. Additional Requirements for Line Managers	6
8. Changes Since Previous Standard.....	6
9. Standards superseded by this document.....	6
10. Document Control	7
10.1 Document Revision History	7

1. Purpose

- 1.1. The purpose of this policy is to ensure that OCA implements information security best practice for its remote working activities. This policy identifies remote workers' responsibilities, and highlights requirements for the secure use of all mobile and home-based equipment, and secure remote access to OCA's network infrastructure, thereby minimising the threat of unauthorised information disclosure or corruption, or loss of information and equipment.

2. Scope

- 2.1. This policy addresses OCA's information security requirements for all remote working, applicable to mobile workers and home workers.
- 2.2. Mobile workers include all users who use OCA's information and information processing facilities whilst not located on OCA's premises, e.g. workers who are located in other organisations' offices, in hotels and conferences, and travelling workers. Home workers are users who have been authorised to use OCA's information and information processing facilities whilst based at home, or larger groups of OCA employees required to work from home during exceptional periods of disruption or mandatory changes to working practices.
- 2.3. Whilst OCA issues its own computer equipment for mobile and home working in the case of staff with established working hours, it may also authorise usage of personal equipment for remote working, for example in the case of staff working flexible hours contracts (Flexible Tutors) or fixed-term commissioned developers of content. This policy applies to all computer equipment used to process OCA's information, regardless of whether the equipment is issued by OCA or whether usage of personal equipment has been authorised.
- 2.4. This policy applies to all OCA staff (including employees, temporary staff, contractors, consultants and partners).

3. Policy Statement

- 3.1. The policy of OCA in regard to remote working is as follows:
 - Users shall only be allowed to undertake remote working activities for OCA after authorisation has been granted;
 - Where authorised, remote working shall comply with defined physical requirements and systems and network security requirements to reduce the risk of security threats to OCA's information.

4. Roles and Responsibilities

- The IT Manager is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- Line managers are directly responsible for implementing this policy within their functions/departments, and for adherence by their staff.

- All OCA staff shall comply with this policy and facilitate its implementation.

5. Physical Security Requirements for Remote Working

5.1. The following measures are required to reduce the risk of physical security threats to devices used for remote working and OCA's information. 'Mobile devices' shall be interpreted as computing devices that are easily removed such as laptops, mobile phones, tablets and other handheld devices.

- Mobile devices shall never be left unattended whilst unprotected;
- Where possible, mobile devices shall be stored within a locked cabinet, desk or room when not in use, and the associated keys shall be protected to prevent unauthorised access to the devices;
- Whilst within an OCA office, unsecured mobile devices shall not be left unattended for any length of time in an unmanned open plan area or unlocked office, and at night, mobile devices shall be physically secured or locked away out of sight;
- Any issued electronic security access tokens shall be kept separate from any laptop or PC when left unattended, otherwise unauthorised access to OCA's network and systems may be possible;
- Computer equipment shall not be positioned or left so that it can be easily seen through ground floor windows by members of the public, whilst working at home;
- Computer screens and printers shall be positioned so that OCA or customer information cannot be overlooked by fellow travellers, co-residents of the premises, family, visitors, or any other unauthorised person. Screen visors can be obtained upon request;
- A quiet, separate working area shall be selected to minimise and control unexpected interruptions and possibilities of sensitive information being viewed by unauthorised persons;
- Family members, friends, visitors or anyone else shall not use OCA's equipment and sensitive information;
- A clear desk policy shall be implemented and all documentation, files, and removable computer media, e.g. CDs and DVDs, containing OCA's information, shall be stored securely when left unattended, and removable media shall be removed from computers when not in use;
- A clear screen policy shall be implemented and when left unattended, PCs and laptops shall be logged-off or secured by a password-protected screen saver, or similarly secured by a password or PIN number for other devices, including tablets, mobile phones and other handheld devices;
- When transporting mobile devices by road vehicle, at no time shall the device be left unattended. Mobile devices can be locked away out of sight if unobserved by strangers, but shall not be left there for long periods of time or overnight;
- Mobile devices shall be carried as hand luggage when traveling and kept within sight and reach at all times, including at airport security checkpoints;

- Mobile devices shall not be left in hotel rooms unless they can be locked securely in a safe, drawer or wardrobe, and are completely hidden from view;
- Users shall only use hands-free mobile devices whilst driving.

6. Systems and Network Security Requirements for Remote Working

6.1. The following measures are required to reduce the risk of security threats to information systems and networks, i.e. OCA's information and software on computing devices used for remote working and on OCA's corporate network and systems. As relevant, computing devices include PCs, laptops, tablets, mobile phones and other handheld devices.

- Workers shall comply with the [Acceptable Use Policy](#).
- Workers shall only attempt to access OCA corporate network and systems by means that have been authorised.
- Workers shall only process OCA information on computing devices that have been approved by the IT Department as being in compliance with minimum security requirements, e.g. where users are authorised to use personal devices to process OCA information.
- OCA's password security requirements, documented within the [Access Control Policy](#), shall be implemented.
- Workers shall ensure that all OCA information is securely and regularly backed up to the central OCA network systems, in order to avoid the risks of lost and out-of-date information.
- Workers shall not tamper with or reconfigure security controls, settings and applications that have been implemented by the IT Department, e.g. controls used to access OCA's corporate network and systems, and controls used to protect computer devices such as personal firewalls, anti-virus software, and password controls.
- Personal firewalls shall always be in operation when using computer devices, such as PCs and laptops, outside of OCA's offices, whilst anti-malware software shall be in operation at all times.
- Anti-virus software shall always be up-to-date and activated on computing devices used for remote working. Failure to do so could result in disciplinary action. Wherever possible, the IT Department has configured devices to automatically update anti-virus software when connected to OCA's corporate network or the Internet. If there are any concerns regarding anti-virus software not being up-to-date, immediately contact the Service Desk.
- When working at any site not designated as your remote working address as stated within your contract with OCA you shall use the provided VPN software designated by the IT department for conducting business for OCA or accessing OCA data.
- When working remotely all OCA data shall be stored only on your designated OCA device if supplied or within your designated OCA supplied remote data location (i.e. your OCA Google Drive)

- Workers shall not download any software onto devices used for remote working without authorisation from IT Security and from their line manager. Use of unauthorised software could lead to breaches of copyright legislation or unauthorised access to OCA's information.
- The operating system of the computing device shall not be changed without approval from the IT Department.
- All software, including operating systems and all applications in use, shall be updated with the latest security patches. If workers are notified of new security patches that need to be applied, then the updates shall be implemented on the same day.
- Hardware alterations, additions or upgrades shall not be conducted without the approval and involvement of the IT Department.
- Remote connectivity shall comply with the [Network Security Policy](#). Wireless connectivity shall be used with precaution, by weighing up the possibility of unauthorised access by other wireless users in the immediate vicinity. Workers shall also comply with the [Information Classification and Handling Policy](#) when transmitting information over any network, including wireless networks.
- Workers acknowledge that they are responsible for and will pay for any Wi-Fi charges incurred, outside of normal usage of the corporate Wi-Fi, unless approved by the IT Department.
- Workers shall immediately report any real or suspected security incidents involving devices used for remote working to the IT Help Desk, including loss, damage or theft of equipment, and unauthorised access to OCA's information or corporate network and systems.
- If devices used for remote working are stolen, workers shall also immediately report the incident to the Police. Workers will be given an incident number which must be provided to the IT Help Desk, so that an insurance report can be compiled.
- To protect OCA's information and software, OCA shall remotely wipe a college-owned mobile device immediately, if it is lost or stolen, or if there are any concerns with the security of the device. A similar wipe of OCA's information and software shall be undertaken when an employee leaves OCA. OCA accepts no liability for the loss of or destruction of any data stored on a mobile device..

- 6.2. All devices covered by this policy shall be regarded as OCA devices where college information and security are concerned, and treated accordingly.

7. Additional Requirements for Line Managers

- 7.1. Line managers are also required to comply with the following requirements:

- Line managers shall formally make a request to the Service Desk for any remote working computing requirements for any of their staff members;
- Line managers shall ensure that their staff members sign a form stating that they understand and agree to comply with the policy, before they use any computer devices for remote working or are able to remotely connect to OCA's network and systems;

- When a staff member no longer requires remote working facilities, e.g. staff leavers and movers, the line manager shall ensure that the Service Desk is formally notified as soon as practically possible and shall ensure that relevant equipment is collected and returned to the IT Department.

8. Changes Since Previous Standard

- 8.1. This is the first version of the Remote Working Policy.

9. Standards superseded by this document

- 9.1. This is the first version of the policy. It supersedes any policies previously contained in V2 of the Information Security Policy set.

10. Document Control

Document Control	
Title:	Remote Working Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

10.1 Document Revision History

Version	Date	Author	Summary of changes
0.1			Initial draft
0.2	02/10/2025		Changes to section 6 regarding VPN usage and data storage
1.0	05/11/2025		Final revisions approved and version updated to 1.0 for release



The Open College of the Arts



The Open
University