# Offsite Working Policy and Procedure

| 1. Document Information | |
|---|---|
| **Document Name** | SLMS-IG21 Offsite Working Policy and Procedure |
| **Author** | Trevor Peacock |
| **Issue Date** | 17/06/2021 |
| **Approved By** | Chair of SLMS IGSG |
| **Next review** | One Year |

2. **Document History**

| Version | Date | Summary of change |
|---|---|---|
| 1.0 | 02/08/2013 | SLMS-IG21a Remote Access Policy<br>SLMS-IG21b Remote Working Procedures and Approval<br>This (v1.1 onwards) document replaces the two v1.0 documents |
| 1.1 | 20/03/2020 | First draft of combined policy and procedure circulated for comments |
| 1.2 | 02/04/2020 | Incorporated feedback from Anthony Peacock, David Wong, Jack Hindley, Pia Hardelid |
| 1.3 | 16/04/2020 | Incorporated feedback from Alex Potts, Richard Gilson, Robert Maughan |
| 2.0 | 23/04/2020 | Approved by Chair of IG Steering Group |
| 2.1 | 03/06/2021 | Amended procedure section to clarify and simplify the steps (additional reference to public wi-fi approved on 17/06/2021) |
| 3.0 | 17/06/2021 | Approved by Chair of IG Steering Group |

## 1. Purpose of the policy

Safe handling of information within UCL is reliant upon a combination of policy, procedure, authorisation and technology. In addition to technical controls such as the Data Safe Haven, the UCL working environment includes security staff, CCTV and access controls, such as swipe cards. These form part of a range of measures that reduce the risk of unauthorised access to information. When working offsite, this level of control is unlikely to be in place. The purpose of this policy and procedure is to provide a level of assurance that the risk of unauthorised access to UCL information is managed to an acceptable level while working offsite.

## 2. Exceptions

This policy does not apply where the offsite worker is processing data within another organisation that is the data controller and using equipment that is operated by that organisation. In this case, data for which UCL is the data controller must not be transferred to the other organisation's equipment without a suitable data processing contract being in place and relevant controls being implemented.

## 3. Terminology

**Information Asset Owner ('owner' within this policy)**

In research this is typically the Principal Investigator on a study; the person who is accountable for confidential information. In other contexts, this would be the Data owner or Information owner.

**Offsite work**

Work undertaken anywhere other than a UCL-managed site. This includes:

- Working at other organisations
- Working from home
- Working while on the move

## 4. Policy statements

All of the following statements shall apply to offsite work involving access to confidential information, which shall be undertaken:

- after the responsibilities (section 5) are agreed and signed off via the procedure (Appendix B)
- where there is a justification for working offsite
- in locations where the risk of disclosure is proportionate to the sensitivity of the information
- in line with all other legal, regulatory, contractual and policy requirements which apply
- up to a defined end date
- using devices that are UCL-managed or comply with the UCL's BYOD policy

## 5. Responsibilities

**The owner is accountable for:**

- defining an appropriate scope for offsite working
- authorising the offsite worker
- ensuring the offsite worker is provided with appropriate tools for offsite working
- defining start and end dates for offsite work authorisation
- where necessary, defining information assets which may or may not be accessed offsite
- ensuring the offsite worker confirms agreed working arrangements
- maintaining a record of those authorised to work offsite

**The offsite worker is responsible for:**

- confirming working arrangements in checklist are in place (or agreed equivalents)
- understanding and complying with the scope and duration defined by the owner
- complying with and monitoring of the commitments in the Offsite Worker Checklist
- notifying the owner of any breach of the agreed scope

The responsibilities are captured in a checklist, Appendix B, which must be completed by the owner and offsite worker

**Appendix A - Related policies and procedures**

UCL BYOD (Bring your Own Device) Policy:
https://www.ucl.ac.uk/information-security/sites/information-security/files/byod.pdf

UCL Information Management Policy:
https://liveuclac.sharepoint.com/sites/ISD.InformationSecurityGroup/Team%20Documents/Policy/Information-Management-Policy-IRGG-20170912.pdf

UCL Work Life Balance Policy (section 4.14)
https://www.ucl.ac.uk/human-resources/sites/human-resources/files/work-life-balance-policy-210219.pdf

Display Screen Equipment (DSE)
https://www.ucl.ac.uk/safety-services/a-z/display-screen-equipment

UCL policies currently employ different terminology to the Information Governance Framework, which is based on NHS Digital's Data Security & Protection (DSP) Toolkit.

| DSP Toolkit and this policy | UCL Data Protection Policy | UCL Information Security Policy |
|---|---|---|
| Information Asset Owner | Data Owner | Information Owner |
| Information Asset Administrator | Data Custodian | Information Custodian |

UCL glossary of terms used in policy documents:
https://www.ucl.ac.uk/information-security/sites/information-security/files/glossary.pdf

**Appendix B - Procedure**

**Owner checklist**

1. Justification for working offsite

| |
|---|
| |

2. Record the Scope of authorisation:
   a. Who will be working off-site

| |
|---|
| |

   b. Dates

| From: | To: |
|---|---|

   c. equipment that must be used (e.g. Desktop@UCL laptop)

| |
|---|
| |

   d. any restrictions on data handling, not covered in the list below

| |
|---|
| |

**Offsite worker checklist**

| **Offsite worker to confirm:** | |
|---|---|
| Work will take place in a location that is suitably private | Yes / No |
| Screen positioned so that you are the only person who can see it; this includes positioning away from home security cameras | Yes / No |
| You will **not use** public / unsecured wi-fi (answering 'yes' means you agree) | Yes / No |
| Phone conversations will be appropriately protected to prevent eavesdropping.<br>- Consider whether you should discuss your environment with the person you are speaking with before starting a sensitive or confidential conversation<br>- Ensure internet-connected voice recognition devices (e.g. Alexa) or home security cameras capable of capturing audio are not within range | Yes / No |
| Computer screen will be locked or logged out when away from the computer | Yes / No |
| Clear desk policy will be operated, ensuring any confidential notes are stored securely | Yes / No |

If any of the answers in the offsite worker checklist are **No**, please include details of agreed measures required to mitigate those risks

| |
|---|
| |

Owner confirms approval for offsite working for the named offsite worker as defined within this scope

| | |
|---|---|
| Owner name: | |
| Signature: | |
| Date: | |

Offsite worker to confirm that they understand and will:

- comply with the policy statements
- work within the scope and working arrangements detailed in this checklist
- notify the owner in the event that these are breached
- comply with UCL's BYOD policy (where their own equipment is used)

| | |
|---|---|
| Offsite worker name: | |
| Signature: | |
| Date: | |

Owner to retain the signed form as a record of authorisation