Keele UNIVERSITY

IT AGILE WORKING CODE OF PRACTICE

1. INTRODUCTION

1.1 This Code of Practice has been developed to provide interim guidance on the IT requirements to be followed to support staff to work in an agile manner. The Code will ultimately inform the development of a Keele Agile Working Policy and will promote the protection of personal, sensitive, or business data and maintain the overall security of university data and equipment whilst employees are working remotely or in an agile manner.

1.2 Agile, or remote, working is a work arrangement that permits an employee to conduct all or some of their work at an approved alternative worksite such as the home, at a family member's home, or at another higher education institution.

1.3 Staff members must always ensure the security of information and systems including when accessed during periods of agile working, are given due consideration. This Code of Practice emphasises the importance of staff understanding the University's current Information Security policies and procedures and everyone's responsibilities in relation to these which must be always adhered to.

2. SCOPE

2.1 This Code of Practice is intended for all University staff who use agile working as part of their agreed working arrangement with the University. This Code of Practice will detail how staff should conduct their work in terms of IT provision, what IT and Data Protection policies to be familiar with and how to comply with IT requirements.

3. IT APPROACH

3.1 Colleagues must assess if the business activity they're undertaking is sensitive and use the appropriate level of security during the discharge of their duties.

3.2 Accessing business as usual apps (e.g., email, teams) should be done through a web browser, on a Keele-owned device. The provision of IT equipment must be discussed with your line management to ensure that it is sufficient to allow you to complete your job role. Equipment to be supplied can be selected and purchased through the Keele Procurement process.

3.3 Staff wishing to use their own IT equipment should first refer to the Bring Your Own Device (BYOD) guidance.

3.4 Accessing confidential or sensitive data must be done through the University VPN service. (e.g., finance systems, estates, trial data) and on a Keele-owned device. Information on the VPN can be accessed on the IT Service Desk Knowledge Portal.

3.5 To minimise the risk of data loss when agile working, it is preferred that printing at home or on another organisations' print service is not undertaken, however, it is recognised and understood that there are specific use-cases where printing is required and therefore has to be undertaken.

3.6 When using Public Wi-Fi (e.g., airport, exhibition etc) colleagues must use the University VPN to access Keele resources. Information on the VPN can be accessed on the IT Service Desk Knowledge Portal.

3.7 There are a number of general security measures that will assist in preserving the confidentiality and integrity of Keele data:

- You must not use personal devices for storing, accessing, or transmitting personal or commercially sensitive information relating to Keele.
- Where possible, an appropriate secure location should be used for meetings and confidential conversations. Headsets must be worn where necessary.
- If working in a public area, make sure that people cannot see your screen to prevent shoulder surfing.
- You must lock your screen when leaving your device unattended as this will prevent data loss in the event of theft.

- You must not leave your device unattended when in a public place for any reason and at any time as this will prevent data loss.
- If staying at a hotel, you should use any provided lock boxes, if large enough, or hotel controlled storage rooms) if leaving the device unattended for any length of time.
- You must not allow any third part IT support to install or diagnose any issue on your university device or supply your password, please contact the IT Service Desk for assistance.

https://servicedesk.keele.ac.uk

Email: it.service@keele.ac.uk

Phone: 01782 733838

4. ROLES AND RESPONSIBILITIES

4.1 The University must abide by this Code of Practice as failure to do so constitutes non-compliance with the University's IT Acceptable Use Policy and thereby also Jisc's Acceptable Use Policy with the possible withdrawal of Jisc's network infrastructure services.

4.2 Members of the University are expected to **promote and encourage** compliance with the principles and spirit of this Code.

4.3 Individuals who fail to ensure that the provisions of this Code of Practice are adhered to may be liable to disciplinary action in accordance with University Regulations, policies, and procedures, in addition to any possible prosecution for breach of the law.

4.4 The University's principles of integrity, professionalism and ethical practice must be applied equally when agile working. All staff should consider how their reputation and that of the University might be affected by how they communicate and conduct themselves.

4.5 The University authorises:

- The Chief Information Officer (CIO) with responsibility to ensure that the University complies with the provisions of this Code of Practice

5. RELATED POLICIES AND PROCEDURES

5.1 The following Policies, Guidance and Procedures should be read in support of this Policy. All documents are available in the Policy Zone :

- IT Acceptable Use Policy
- Data Classification and Handling Policy
- Data Protection Policy
- Information Governance Framework
- Information Security Policy
- Records Management Policy
- Records Retention Schedule
- Freedom of Information Act (FOI) Policy
- Email Code of Practice

5.2 Details of IT related guidance can be found on the Information & Digital Services staff intranet pages: IDS Working from Home Guidance - Home (sharepoint.com)

5.3 HR guidance on Agile Working can be found at: Agile Working (sharepoint.com)

6. REVIEW, APPROVAL & PUBLICATION

6.1 The University will review formally the operation of this Code of Practice at least every three years, led by the Associate Director – Projects and Service Assurance (IDS), in consultation with key stakeholders across the University including:

- The Information and Digital Services (IDS) Directorate's Strategic Executive Group (SEG)
- The Information Governance Group
- Information Governance Champion Network (where/when appropriate)
- Digital Champion Network (where/when appropriate)

6.2 The University Executive Committee (or its sub-group) shall have final responsibility for approval of any changes to this Code of Practice, in accordance with the University Policy Framework.

6.3 This Code will be available within the Policy Zone

7. DOCUMENT CONTROL INFORMATION

Document Name	Agile Working Code of Practice
Owner	Simon Clements, Head of Projects and Service Assurance, Directorate of Information and Digital Services
Version Number	V1.0
Equality Analysis Form Submission Date	NA
Approval Date	27/February/2023
Approved By	University Executive Committee
Date of Commencement	27/February/2023
Date of Last Review	27/February/2023
Date for Next Review	27/February/2026
Related University Policy Documents	IT Acceptable Use Policy, Data Classification and Handling Policy, Data Protection Policy, Information Governance Framework, Information Security Policy, Records Management Policy, Records Retention Schedule, Freedom of Information Act (FOI) Policy, Vulnerability Disclosure Policy
For Office Use – Keywords for search function	