Sheffield Hallam University

Information Security Policy for Staff Who Work Off-Campus

Issuing Authority: Leon Etherington,
Acting Chief Information Officer,
Information Systems and Technology

Signed: 

Date Effective: March 2016

Review date: February 2018

Version: 2016.2

Information Security Policy for Staff Who Work Off-Campus

Objective

To ensure the security of information accessed by users working off campus or using non - University equipment, stored either on static or portable computers, small portable devices or storage media.

Scope

This policy applies to all University staff, students, data processors, partners, suppliers and contractors and other authorised users who have access to the University infrastructure.

Policy Requirements

1. All employees of the University have the ability to participate in mobile working from remote locations through the use of Virtual Private Network (VPN), staff remote desktop or on-line remote file access technology. Access from remote locations to sensitive information held in University systems, such as e5, is not allowed without the written authorisation of the system owners. System owners must assess the risks to information security before granting authorisation, and a log kept of all access granted.
2. Mobile and remote workers should familiarise themselves with the University's ***Data Protection Policy Statement***, ***Data Protection Secretariat Page***, and ***Working Off-Campus: Guidance on Data and Records***.
3. Mobile and remote workers should ensure the amount of confidential or sensitive information held on portable devices is kept to a minimum and a secure copy or back-up stored elsewhere. Furthermore, sensitive University information must be encrypted in accordance with the University's **Electronic Data Encryption Policy.** This specifies that all personal and sensitive data stored on portable devices shall be encrypted. Data must not be disclosed whilst working in transit or working offsite.
4. All non-University devices must have, anti-virus controls in place, (unless not technically possible), current security patches installed, personal firewall protection in place, individual user accounts if used by more than one person, password protection, and time-out protection enabled to prevent unauthorised access.
5. Portable equipment and storage media should not be left unattended in public places. Users are responsible for the safe-keeping of University information, assets and equipment. Any loss of equipment or storage media (whether University owned or personal) which contained sensitive or personally identifiable University data, must be reported as soon as possible to the University Information Governance Officer, giving details of the loss and type of data stored.

In addition all University owned IT equipment lost or stolen should be reported to IT Help irrespective of data content.