Sheffield Hallam University

Staff Responsibility for Information Security Policy

Issuing Authority:	Leon Etherington, Acting Chief Information Officer, Information Systems and Technology
Signed:	
Date Effective:	March 2016
Review date:	February 2018
Version:	2016.2

Staff Responsibility for Information Security Policy

Objective

To minimise the risks to information security from human error, fraud or misuse of the University's IT systems. To ensure that users are aware of their responsibility to support the University's **IT Security - Policies, Procedures and Related Guidance** (formally the Electronic Information Security Framework EISF) in the course of their work.

Scope

This policy applies to all University staff, students, data processors, partners, suppliers and contractors and other authorized users when working with University IT systems and infrastructure.

Policy Requirements

1. All users shall comply with the University's information security policies and guidelines. Any information security incidents that ensue from non-compliance may result in appropriate action being taken by the University which may include disciplinary action.
2. The University's standard terms and conditions of employment include requirements not to misuse or inappropriately disclose any confidential information which may be obtained during the course of employment, or by having privileged access to systems and data, or a specific security role or responsibility. The requirement to maintain confidentiality continues after a member of staff has left the University.

Relevant guidelines and regulations are available for staff via the HR intranet site and for students via SHUSpace, including the sections headed:

- ***Code of Behaviour – Guidelines for Good Professional Conduct at Work***
- ***Confidentiality***
- ***Data Protection Act 1998***
- ***Regulations for the Use of IT Facilities***
- ***Staff Guidelines on the Use of IT Facilities***

3. All new employees shall be given guidance on information security issues during Faculty, Directorate or University induction. This information shall be in accordance with the current IT regulations and other associated policies.
4. Temporary staff, and their managing or employing agency, shall receive instruction about the University's information security requirements at the start of their period of employment at the University.
5. All employees of the University should receive training on any new systems that they are required to use, to ensure that they do not compromise information security
6. Technical staff should, where their role demands, receive training in information security threats and technical safeguards.
7. All users have a responsibility to report incidents or suspected incidents. This should include software anomalies which could indicate compromised workstations, applications or a malware infection.