

# Information Security Training Policy



Document Title:	Information Security Training Policy
Version Number:	1.2
Document Status:	Approved
Date Approved:	19 April 2018
Approved By:	Data and Information Management Oversight Group
Effective Date:	19 April 2018
Date of Next Review:	March 2020
Superseded Version:	1.1

## 1 Purpose

The University's Information Security Framework needs to be communicated to and understood by those who access information on behalf of the University and those who play a part in maintaining the technical, physical and environmental security of the University and its information. Accordingly this policy establishes a requirement for delivery of information security training to all relevant individuals as part of the Information Security Framework, and defines the objectives and scope of that training and related responsibilities.

## 2 Scope

This policy covers all Cardiff University staff, other Members of the University and other workers who handle Classified Information on behalf of the University, referred to below as 'relevant individuals'.

## 3 Relationship with existing policies

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy and all supporting policies.

## 4 Policy Statement

All Cardiff University staff and relevant individuals will be aware of and fulfil their information security responsibilities.

## **5 Policy**

5.1 All staff will receive regular, mandatory training in information security which is relevant and proportionate to the type of information they are required to access and their role in maintaining the technical, physical and environmental security of the University, as set out in the attached Schedule A.

5.2 All other relevant individuals will be offered training in information security which is relevant and proportionate to the Classified Information they are required to handle on behalf of the University, as set out in the attached Schedule A.

5.3 Staff and relevant individuals will be properly briefed on their information security roles and responsibilities prior to being granted access to Classified Information or information system.

5.4 Staff will achieve and maintain a level of awareness on information security relevant to their roles and responsibilities and this will be measured.

5.5 The information security training will be tailored to the intended audience and will normally cover:

5.5.1 The need to be familiar with and comply with University information security policies as set out in the Information Security Framework in addition to all applicable laws, regulations and contracts;

5.5.2 Personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the University and external parties;

5.5.3 Basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks as appropriate);

5.5.4 Contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

5.6 Mandatory information security training will be delivered in an accessible manner to enable all categories of staff and relevant individuals to readily access the training.

## **6 Responsibilities**

6.1 The Senior Information Risk Owner will ensure that appropriate information security training is available for all staff and relevant individuals.

6.2 The Department of Strategic Planning and Governance will ensure that both the content of the training materials and the administrative processes remain fit for purpose and to raise awareness of this policy.

6.3 The Human Resources Department (in conjunction with IT Services) will facilitate the enrolment of staff onto the mandatory information security modules and the flow of data between Learning Central and Core, and HR will provide regular and appropriate management information

reports relating to the uptake and successful completion of the module for all staff registered through Core.

6.4 The HR Business Partners will use the management information provided by HR to actively promote compliance within their College or Professional Services.

6.5 All line managers will facilitate the uptake of information security training for their staff and act on non-compliance with any mandatory requirements. Line managers will keep records of completion of any alternative training provision for those relevant individuals who are not able to take the mandatory module via Learning Central. The relevant individuals will self-report completion.

6.6 The Secretary to Council will ensure that lay members have undertaken the training.

6.7 The Chief Executive of the Students Union will ensure that Students Union staff have undertaken the training.

6.6 It will be the responsibility of all staff and relevant individuals to avail themselves of the training opportunities provided within the required timescales and to complete all mandatory information security training activities.

6.7 The Data and Information Management Oversight Group will oversee the implementation of this policy and ensure that it remains fit for purpose.

### Definitions

Classified Information is information that is confidential, highly confidential or requires enhanced protection to ensure integrity or availability due to its nature. Further explanations of these classifications can be found in the University's Information Classification document.

University Members are as defined in Statute and Ordinances.

## SCHEDULE A INFORMATION SECURITY TRAINING SCHEDULE

Category	Type of Training	Frequency
All Staff (with a Core HR record)	On-line module provided through Learning Central with assessment test recorded in CORE HR.	Within first 30 days plus annual refresh
Senior Information Risk Owner and Data Leads	On-line module provided through Learning Central with assessment test recorded in CORE HR.	As per all staff plus specific training as one off at

	<i>Civil Service E-learning resources tailored to these roles</i>	commencement of role
Lay Members of University committees	On-line module provided through <a href="http://sites.cardiff.ac.uk/isf/advice/information-security-training/">http://sites.cardiff.ac.uk/isf/advice/information-security-training/</a>	One off at commencement of role plus annual refresher
Students Union staff	On-line module provided through <a href="http://sites.cardiff.ac.uk/isf/advice/information-security-training/">http://sites.cardiff.ac.uk/isf/advice/information-security-training/</a>	At induction plus annual refresher
Agency workers and other types of staff not on Core HR  <b>Contractors on site:</b> Cleaning staff  Building workers  IT workers   <b>Contractors Off-site:</b>  IT workers	On-line module provided through <a href="http://sites.cardiff.ac.uk/isf/advice/information-security-training/">http://sites.cardiff.ac.uk/isf/advice/information-security-training/</a>	One off at commencement of role