FALMOUTH
UNIVERSITY

IT SECURITY POLICY – OVERVIEW

UCISA represents the whole of higher education, and increasingly further education, in the provision and development of academic, management and administrative information systems, providing a network of contacts and a powerful lobbying voice.

The UCISA Information Security Management Toolkit has been constructed for use by information security/governance professionals wishing to put in place an Information Security Management System in their organisation.

The UCISA Information Security Management Toolkit fulfils the following:

- assists those who have responsibility for implementing information security across the organisation by providing advice and guidance to them;
- helps them to provide senior university management with an understanding of why information security is an important, organisation-wide issue.

There should be an over-arching IT Security Policy, and a number of sub-policies to cover various areas of user, data and system protection to provide assurance to the organisation.

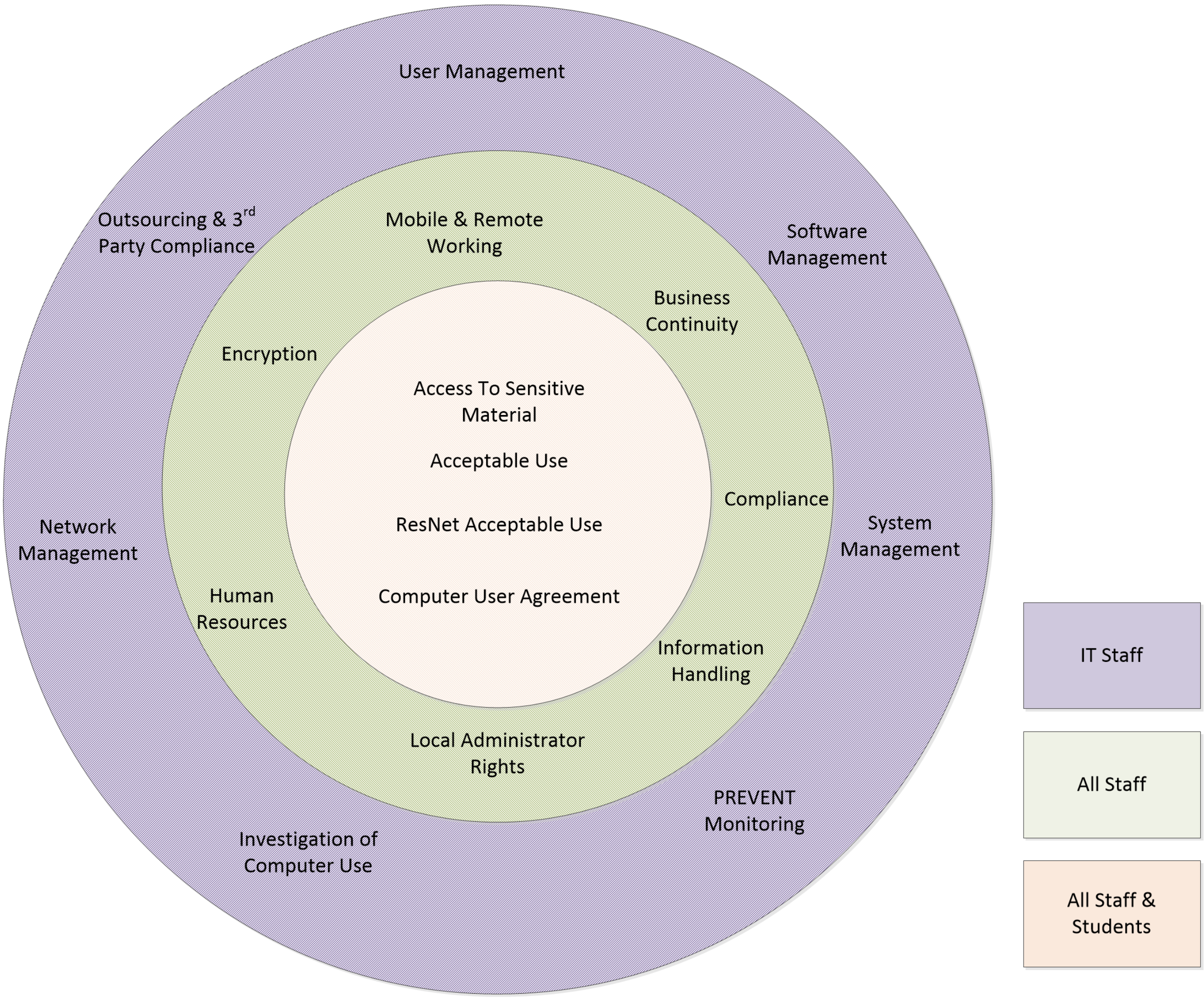
These sub policies commonly consist of the following:

- **Business Continuity**
  Sets out the process for assessing and addressing risks to business continuity and defines the responsibilities for preparing and implementing business continuity plans
- **Compliance**
  outlines the organisations requirement to comply with certain legal and regulatory frameworks
- **Outsourcing and Third Party Compliance**
  outlines the conditions that are required to maintain the security of information and systems when third parties, other than FX Plus or our partner universities own staff or students, are involved in their operation.
- **Human Resources**
  sets out the Human Resources processes that must be implemented to ensure that employees are able, trained and required to protect the University's information assets.
- **Information Handling**
  sets out the requirements relating to the handling of information assets. Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur
- **User Management**
  sets out the requirements for the effective management of user accounts and access rights
- **Acceptable Use**
  sets out the responsibilities and required behaviour of users of the FX Plus information systems, networks and computers. Including references to PREVENT legislation

- **System Management**
  sets out the responsibilities and required behaviour of those who manage computer systems on behalf of FX Plus and our university partners.
- **Network Management**
  sets out the responsibilities and required behaviour of those who manage communications networks on behalf of Falmouth Exeter Plus and our partner universities
- **Software Management**
  sets out the principles and expectations for the security aspects of managing software by IT staff and end users where relevant
- **Mobile and Remote Working**
  sets out the additional principles, expectations and requirements relating to the use of mobile computing devices and other computing devices which are not located on campus premises when these devices are used to access corporate or university information assets with a classification of confidential or above.
- **Computer Users Agreement**
  outlines the expectations of FX Plus and our university partners regarding what is permissible usage of supplied equipment/networks. Including references to PREVENT legislation
- **Access To Sensitive Material**
  outlines the process for requesting access to material on the Internet that may be construed as offensive or sensitive.
- **Encryption**
  sets out the principles and expectations of how and when information should be encrypted.
- **ResNet Acceptable Use**
  sets out the additional responsibilities and required behaviour of users of the campus Residential Network service
- **Investigation of Computer Use**
  outlines the circumstances in which it is permissible for Falmouth Exeter Plus (FX Plus) to access the IT accounts, communications and other data of staff and students using FX Plus equipment and networks
- **Local Administrative Rights**
  outlines the expectations of FX Plus and our partners universities on staff who have been granted local administrator rights
- **PREVENT Monitoring**
  outlines the process for highlighting activity that may indicate actions in breach of Government counterterrorism legislation

These policies have been written as co-branded documents for Falmouth Exeter Plus and Falmouth University, but now need to go through the necessary approval processes of both organisations.

The diagram below shows how the policies relate to staff at Falmouth Exeter Plus and staff/students of Falmouth University.


User Management
Outsourcing & 3rd Party Compliance
Software Management
Network Management
System Management
Investigation of Computer Use
PREVENT Monitoring
Mobile & Remote Working
Business Continuity
Encryption
Compliance
Human Resources
Information Handling
Local Administrator Rights
Access To Sensitive Material
Acceptable Use
ResNet Acceptable Use
Computer User Agreement
IT Staff
All Staff
All Staff & Students