UC Policy Library

IT Policy Framework

Last Modified September 2020
Review Date September 2021
Approval Authority Executive Director – Planning, Finance and ITS
Contact Officer Security Analyst, ITS – Planning, Finance and ITS

Introduction

This is the core document that describes the ways that information technology (IT) resources may or may not be used at the University. This document applies to everyone who makes use of the University's IT resources, including students, staff and visitors to the University.

This is not a complete statement of all University policies relating to IT, there will be other policy documents you should refer to as necessary. These are listed in the '*Advice for Students and Staff*' and '*Advice Specific to Staff*' sections of this document.

Definitions

IT users – all staff (including adjunct appointments), students and visitors to the University who make use of the University's IT resources.

Usercode – unique identifier assigned to an IT user that will allow access to the University's IT and information resources, usually seen in the format 'abc123'.

Policy Framework

The University strives to deliver a robust and fit for purpose computer network and associated computer systems to support its strategic mission, objectives and priorities. Students and staff are encouraged to use the computer systems to the fullest extent to support teaching, research, study and other related University work. You are further encouraged to bring your own devices and use them in conjunction with University supplied facilities.

All IT users have responsibilities which must be honoured, and will be held individually responsible for any and all activities undertaken by them.

You may not undertake any activity with any element of IT that you would not ordinarily be allowed to undertake under your existing relationship with the University. Such restricted activities include:

- You may not break (or assist another to break) the law, for example, copyright violations, or viewing or holding objectionable material.
- You may not harass or bully people, including, for example, by text, or invade their privacy.
- You may not send unsolicited bulk mail (spam) or undertake for-profit personal activities using University resources.
- You must be mindful of Intellectual Property (IP) rights, and handle materials bound by such rights appropriately.

None of these responsibilities differ in the electronic context from your responsibilities in a non-electronic context.

Unique to electronic communication and systems is malware. You must take care that any

IT systems can be used to **harass**, **bully** and **abuse** people, and this is also expressly prohibited. For further details see the *Prevention of Harassment and Bullying Policy (PDF, 180KB)*.

Passwords are an important part of system security. For most systems, the system itself will show and enforce the minimum quality rules that are required of a password; the rules themselves and further guidelines may be found in the *Password Policy (PDF, 224KB).*

The University is required both by law and contract to honour **copyright**, and therefore it is important that you are aware of copyright generally. In particular, the use of University IT facilities to violate copyright and most particularly by means of infringing file sharing ('Peer to Peer') is expressly prohibited. See the *Copyright Policy (PDF, 362KB)* for more information. The University is also a creator of **intellectual property**, to which copyright applies. You should refer to the *Intellectual Property Policy (PDF, 534KB)* for further information.

The University provides access to the **internet**; and to **email**, and in using the internet or email facilities, you must not undertake any activity which is illegal, or risks the reputation of the University. More details on internet use are available in the *Internet Usage Policy (PDF, 222KB)*. The *Emails to Enrolled Students Policy and Guidelines (PDF, 300KB)* covers the general use of email and the rules around the use of **mailing and distribution lists.**

If you have your own **mobile device** such as an **iPad**, **iPhone**, or **smartphone**, then your use of that device must comply with the *Mobile Voice and Data Policy (PDF, 149KB).*

The *Student Printing Services Policy (PDF,176KB)* outlines the use of University printing facilities.

Monitoring and Enforcement

Computing equipment and access to the internet are provided by the University to staff and students for work, study, and research purposes and not for personal use. If you decide to use your University supplied computer or other digital device for personal use, you will be subjected to University mon1ds0 0 595.38 841.98 reW*nBT/F4 12 Tf1 0 0 1 240.14 288.8 T

ITS will advise the relevant Pro-Vice-Chancellor (PVC) or Director, and/or the Director of Human Resources, and/or the Registrar and the Executive Director, Learning Resources as appropriate of any suspected breaches of this policy. Any concerns will be investigated in accordance with the relevant University policies and procedures. Breaches of this policy may be viewed as serious misconduct which could result in disciplinary action being taken.

Advice Specific to Staff

The following compliance documents are of particular use to staff:

Computer Replacement Policy (PDF, 155KB): Staff computing device acquisition, replacement and disposal is governed by this policy.

Staff Printing Services Policy (PDF, 155KB)