UCPL-4-6

UC Policy Library

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Internet Usage Policy

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

Introduction

This policy defines what the University considers appropriate usage of the internet and how access to the internet will be managed and monitored.

Definitions

Firewall – a network security system, either hardware or software-based, that controls incoming and outgoing network traffic based on a set of rules.

Inappropriate material – material which could reasonably be described as unsuitable or offensive having regard to the nature of the particular workplace, as determined by the Senior Management Team (SMT).

Infringing file sharing – as defined in Section *122A* of the *Copyright Act 1994 (New Zealand Legislation website)*; generally refers to the sharing of music, movies, and other copyright or licenced material using peer to peer file sharing mechanisms, for example, ‘torrenting’.

Objectionable material – material that it is illegal to view or possess, such as child pornography and depictions of bestiality. Accessing such material is an offence punishable at law with serious penalties, including, for certain offences, imprisonment. For further information see the *Films, Videos, and Publications Classification Act 1993 (New Zealand Legislation website)*.

Website (site) – a destination endpoint on the internet; a URL or an IP address.

Policy

The management of internet access as noted in this policy and the *IT Policy Framework (PDF, 304KB)* is intended to

- promote a harmonious workplace,
- manage the costs of the provision of the internet service,
- ensure the University complies with relevant New Zealand legislation, and
- prevent the University from becoming the subject of an external investigation.

The *IT Policy Framework (PDF, 304KB)* is the core document that describes the ways that information technology (IT) resources may or may not be used at the University. It should be referred to alongside this policy.

Students, staff (including adjunct appointments), and visitors are provided with facilities and equipment to allow them to access the internet for legitimate University work, study, and research related activities. The access quota available to each user has been determined by the University to be sufficient for the needs of the user. Further information for students is available at *Charges and Allowances (University IT website)*.

A reasonable amount of non-work related activity is acceptable; this must not interfere with work related activities.

If a website containing inappropriate or objectionable material is inadvertently opened the website must be immediately exited.

Access to the internet is open, subject to the following restrictions:

- **Access to objectionable material is prohibited.** Where the accessing of objectionable material is required for research purposes, the formal written approval of the appropriate *Ethics committee (University Human Ethics website)* must be obtained. For other purposes, the Vice-Chancellor's formal written approval must be obtained, with supporting reasons and a specified time limitation.

  Note – there are no exemptions for research purposes in the Films, Videos and Publications Classification Act 1993 (New Zealand Legislation website) and thus accessing such material may still lead to Police action against the accessing individual.

- **Access to inappropriate material is prohibited.** Where such material is required to be accessed, the accessing individual must ensure that such content is not observable by others. Such material may cause offense to others, who may make a complaint which will result in an investigation. The outcome of such an investigation may be disciplinary action as noted in the relevant Codes of Conduct, even where such access is fully appropriate, for example, for research purposes.

- **All peer to peer usage must be for legitimate University business only.**

- **All use, sharing, or reuse of licenced and/or copyrighted materials must be in accordance with the *Copyright Policy (PDF, 510KB)*.**

Technical mechanisms will be implemented by ITServices (ITS) to enforce these restrictions. Restrictions that are implemented by ITS will be in accordance with directives from the University; ITS is not a decision-maker in terms of what is restricted.

Firewall Management

Some restrictions will be enforced via the University firewall to assist compliance with this policy. It should be noted that even without this firewall enforcement the restrictions applying to internet access are still applicable.

Requests to have firewall rules removed, or amended, should be made to the *IT Service Desk (University ITS website)*. The scope of the removal or amendment (i.e., for an individual, a group, or the whole University) and the reason must be included in the request. Appropriate documented approval will also be required.

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 monitoring.

The University monitors the usage and content of University computers, servers and associated devices. Monitoring is an ongoing activity of the IT Services Department which uses software tools to check the digital characteristics of files that may signal compliance or cyber security risks. Monitoring can occur at any time, and without prior notice to the staff member or student using the computer. When a problem file is found, IT Services may initiate a further investigation and take action to resolve the risk in accordance with the relevant University policies and procedures.

The University may, with the prior approval of the Registrar or the Vice-Chancellor examine in detail the content, of any computer which has been provided by the University, or which is connected to its networks, at any time, and without prior notice to the staff member or student using the computer. This includes accessing emails or other electronic communications, and any data stored on or processed through the University networks.

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.

Section 122A of the Copyright Act 1994: Infringing File Sharing

Under Section *122A* of the *Copyright Act 1994* (the "Act"), the University is an Internet Protocol Address Provider (IPAP). This means that all users of the University's internet facilities are Account Holders.

As an IPAP, the Act requires that the University undertakes various activities, including the management of 'notices' under the Act. Because the University does not permit peer to peer file sharing (except for legitimate University business), any notices that the University is required to issue to staff or students will also be the subject of disciplinary action. Should a user be issued an enforcement notice (a 'third strike'), the University will fully comply with its obligations under the Act to assist a Rights Owner to bring an enforcement action against an Account Holder before the Copyright Tribunal. An appearance before the Copyright Tribunal can result in awards against the individual concerned of up to $15,000.

For the avoidance of doubt, the University takes its position as a good internet citizen seriously and will investigate and, where appropriate, take disciplinary action as a result of valid complaints received under the Act. Notices received that are not strictly compliant with the Act but which are technically valid will also be investigated and may lead to disciplinary action.

Related Documents and Information

Legislation

- Copyright Act 1994 (New Zealand Legislation website)
- Films, Videos, and Publications Classification Act 1993 (New Zealand Legislation website)
- Official Information Act 1982 (New Zealand Legislation website)

UC Policy Library

- Copyright Policy (PDF, 510KB)
- IT Policy Framework (PDF, 337KB)
- Official Information Policy (PDF, 374KB)
- Staff Code of Conduct (PDF, 481KB)
- Student Code of Conduct (386KB, PDF)

UC Website and Intranet

- Ethics committees (University Human Ethics website)
- IT Service Desk (University ITS website)
- Charges and Allowances (University ITS website)

<table>
<tr><th colspan="4">Document History and Version Control Table</th></tr>
<tr><th>Version</th><th>Action</th><th>Approval Authority</th><th>Action Date</th></tr>
<tr><td colspan="4"><i>For document history and versioning prior to 2013 contact ucpolicy@canterbury.ac.nz</i></td></tr>
<tr><td>1.00</td><td>Document drafted and approved.</td><td>Director, Learning Resources</td><td>July 2016</td></tr>
<tr><td>2.00</td><td>Scheduled review by Contact Officer, minor changes</td><td>Executive Director, Learning Resources</td><td>August 2017</td></tr>
<tr><td>3.00</td><td>Scheduled review by Contact Officer</td><td>Policy Unit</td><td>Sep 2019</td></tr>
<tr><td>4.00</td><td>Schedule review, no changes to substantive content.</td><td>Policy Unit</td><td>Sep 2020</td></tr>
</table>

This policy remains in force until it is updated.