

University of New England

Peer-to-Peer File-Sharing Policy

Document data:

Document type:	Policy
Administering entity:	ITD
Records management system number:	D11/30643
Date approved:	14 November 2011
Approved by:	Vice-Chancellor
Indicative time for review:	3 years or sooner where circumstances warrant.
Responsibility for review:	Information Technology Directorate
Related policies or other documents:	UNE Risk Management Policy, Rules for the Use of Information and Communications Facilities and Services, IT Security Policy, Audit Vulnerability Scan Policy, IT Security Objectives and Framework General Server Security Policy, General Password Policy, P2P File Sharing Policy, Personal Mobile Computing Policy, Standards and Guidelines for all Users of University Computing and Network Facilities, Standards and Guidelines for Desktop Computers, Standards and Guidelines for Non-Strategic Systems, Standards and Guidelines for Strategic Systems

1. Rationale and Scope

As an addendum to the University's Acceptable Use Policy—which details the utilization of the University network, the Internet, e-mail, and employees' personal computers—this policy prohibits the use of Peer-to-Peer (P2P) file-sharing applications. This policy covers Staff and Students using University computing resources and networks.

The University's goal with this policy is to:

- Realize the maximum productivity from each employee;
- Address any potential liability from instances when employees download copyrighted material;
- Minimize network disruption;
- Protect the network from exposure to malicious code (worm, virus, Trojan horse); and
- Protect the University's intellectual property.

2. Definitions

Peer-to-Peer (P2P) - is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives. Napster and Gnutella are examples of this kind of peer-to-peer software. P2P can create significant loads on participating computers and the connected network along with security risks if the program is poorly or maliciously configured.

Spyware – is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else

3. Policy

Peer to Peer (P2P) software is prohibited from being run or installed on University owned or operated networks or Personal Computing equipment.

4. Principles

The following outlines the threat presented by file-sharing applications..

4.1. Liability

Although many materials have been placed on P2P networks with a creator's consent, much of the material (images, software, movies, music, video) have been duplicated from copyrighted materials. Downloading such files onto the University network or a client machine places the University at significant risk for legal action by the copyright holder and other organizations. File-sharing networks also provide ready access to pornography or other offensive material, subjecting the University and its employees to additional legal risk.

4.2. Network disruption

Although the University has sufficient Internet bandwidth to accommodate all business-related activity, performance can degrade significantly when P2P file-sharing applications are used, especially when large files are being downloaded. This problem is compounded when other users on the P2P network use University bandwidth to download files from the employee's computer, which can greatly slow other services, such as e-mail, Web browsing, and—more significantly— the University web site and the future Voice over IP (VOIP) phone and video services.

4.3. Security

P2P networks can introduce serious gaps in an otherwise secure network. Threats such as worms and viruses can easily be introduced into the University's network. P2P applications, if modified, can also allow users outside the University to gain access to data on the employee's computer or even the corporate network. (Although most P2P applications allow users to disable file-sharing, such measures do little to prevent threats from being downloaded onto a user's machine.) Some P2P applications will also allow third parties to see the user's IP address. The installation of spyware is also common with many P2P applications. P2P software can also cause/produce Denial of service attacks on the network.

4.4. Protecting the University's intellectual property

The use of P2P file-sharing applications can sometimes allow other members of the P2P network to have access to everything on a local machine, putting the University's intellectual property assets, as well as an employee's personal information, at risk.

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Approval signature

Vice-Chancellor