Peer to Peer File Sharing Policy

Section 1 - Rationale and Scope

(1) 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.

(2) The University's goal with this policy is to:

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

Section 2 - Policy

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

Principles

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

Liability

(5) 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.

Network disruption

(6) 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.

Security

(7) 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.

Protecting the University's intellectual property

(8) 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.

Enforcement

(9) Any employee found to have violated this policy may be subject to disciplinary

Section 3 - Definitions

(10) 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.

(11) 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

Status and Details

Status	Historic
Effective Date	27th July 2015
Review Date	13th January 2015
Approval Authority	Vice-Chancellor and Chief Executive Officer
Approval Date	14th November 2011
Expiry Date	6th June 2017
Unit Head	Angie Hendrick Chief Information Officer 02 6773 2044
Author	Robert Irving Chief Information Officer
Enquiries Contact	Technology and Digital Services +61 2 6773 5000