



THE WOMEN'S COLLEGE

Within the University of Sydney

INTERNET POLICY AND CONDITIONS

The way students engage and use the College computer network must reflect the ethos of The Women's College, as articulated in the Student Code of Conduct. The network is provided for the benefit of all students in the College and may be used for internet access, workgroups and backup of files. All users are responsible for ensuring that they use the College's IT resources in a legal and ethical way and in observance of the conditions listed below.

This policy operates in conjunction with the University of Sydney's [Policy on the Use of University Information and Communication Technology Resources \(ICT Resources\)](#). Students must familiarise themselves with both College and University policies, and ensure that they comply with them at all times. A breach of either policy could result in the withdrawal of access to the College and/or University networks, or other disciplinary action, and in some instances, breaches may be deemed criminal offences and be referred to the relevant authority.

Conditions of Use

All users must comply with the following conditions:

1. The College's IT network and resources must not be used to send messages, photos or publish or store material that is discriminatory, abusive, rude, insulting, threatening, offensive, defamatory or otherwise inappropriate.

Material will be regarded as breaching this policy if a reasonable person could be expected to find it discriminatory, abusive, rude, insulting, threatening, offensive or otherwise inappropriate. It does not matter if the author or sender did not intend to cause offence.

Any student who is the subject or recipient of material that breaches this policy may take action under The Women's College Grievance Management Policy.

2. The College forbids the use of its IT network and resources in a way that infringes copyright. The law permits copying and/or printing only with the permission of the copyright owner. Users must not use the College network and resources to download and/or store copyright material, transfer copyright material to others or burn copyright material to storage devices, unless the copyright material is appropriately licensed. If unsure, check with the Business Manager. Users must not utilise the College network to install, access or provide links to sites that offer file-sharing software. Infringement of copyright can lead to individuals being prosecuted, and students will also be personally liable for damages and costs if any copyright owner takes action for infringement.

Please note: "copyright material" includes, but is not limited to, software, files containing picture images, artistic works, live pictures or graphics, computer games, films and music (including MP3s) and video files.

3. Illegal activities are strictly forbidden. These include, but are not limited to, tampering with the College computer hardware or software, unauthorised access into College computers or other students' accounts, vandalism or destruction of computer files (including uploading or creation of computer viruses) and impersonation of other users.

4. The College forbids the use of its IT network and resources to access, store or transmit inappropriate material. This includes pornography (except where the individual has specific College and University approval for research purposes) and gambling activities.

5. Security is a high priority. If a student feels that they have identified a security issue or other serious problem on the network, she must notify the Business Manager immediately. The student must not demonstrate the problem to others. Revealing a personal address or phone number, or the personal information of others, is prohibited. Students must not use other students' identities or passwords. Individuals must take responsibility for their own actions, words and online profile. While College will make every effort to protect the privacy of the students' identities and passwords it will not be liable for any breaches outside the College's control.



THE WOMEN'S COLLEGE

Within the University of Sydney

6. Problems experienced while using the internet and network should be reported immediately to the Business Manager.

7. The College IT network and resources must not be used in any way that may cause embarrassment to The Women's College or damage its reputation.

8. The College is not responsible for students' excessive use of their allocated data allowance. The College provides 100 Gb of data per student per month and any usage in excess of this is the responsibility of the student.

9. It is the responsibility of the student to install virus and other protective software on any devices that she connects to the College network. The College is not responsible for any loss of operating capability, files, spam or viruses that may infect or impact the student's devices as a result of being connected to the College network.

10. No additional routers are to be installed within the College without first having the device approved by the Business Manager or the Internet Provider.

Access

The College reserves the right to access email, personal websites, files and data stored on or transmitted through its network for the purpose of investigating any complaints or suspected breaches of this, or any other College or University policy. Should a breach of this policy occur, it will result in access privileges being revoked, and/or College disciplinary action (including cancellation of enrolment), and/or appropriate legal action being taken.

Document Title:	Document Number:	Effective Date:
Internet Policy and Conditions	TWC-IT-D01	February 2013
		Revised: annually
	Version 1.8	Reviewed: February 2019
		Reviewed: November 2023

Dr Tiffany Donnelly
Principal