WESTERN SYDNEY UNIVERSITY

International College

Information Technology Provision and Access Policy

1. Purpose

This Information Technology Provision and Access Policy refers to the conditions and processes by which Western Sydney University International College (WSUIC) staff and students access Western Sydney University and Navitas IT systems based on adherence to:

- Third Party Agreement conditions with Western Sydney University/Western Sydney University Enterprises
- The Western Sydney University International College Summary of Key Responsibilities
- The Western Sydney University IT Acceptable Use of Resources Policy
- The Western Sydney University IT Access Policy
- Navitas IT Acceptable Use Policy

WSUIC has entered into a Third Party Agreement with Western Sydney University/Western Sydney University Enterprises and Navitas Pty Ltd to provide information technology provisions for staff and students to ensure that:

- there are well-maintained and adequate IT infrastructure, software and electronic resources to support students and teaching staff;
- all students readily have access to Western Sydney University electronic information resources required to achieve the learning outcomes of the course of study;
- All IT infrastructure, software and electronic resources are maintained securely.

Western Sydney University and Navitas is responsible for protecting its significant investment in IT resources, and must also meet its legal obligations. It will not jeopardise these through the improper actions of any group or individual. All users of these IT resources are therefore responsible for ensuring that they use them in efficient, ethical, and lawful ways.

2. Definitions

2.1 The following definitions apply for the purpose of this Policy:

2.1.1 "*Authorised User*"

General authorisation to use IT resources is granted upon enrolment, employment or official affiliation with Western Sydney University/Navitas. WSUIC staff and students have access to specific resources as stipulated in the Third Party Agreement.

2.1.2 "*IT* "

Information Technology.

2.1.3 "*IT Resources*"

IT resources include systems, software, hardware and information services. This covers, but is not limited to, computers, terminals, modems, printers, networks (wired and wireless), telecommunication devices (landline and mobile phones, PABX, faxes) storage media and related equipment, data files owned or managed by Western Sydney University/Navitas, information systems; and services such as those on the WSU/Navitas network, (for example, email, internet access).

2.1.4 "*Network*"

Network hardware and the services operating on the hardware or utilising the hardware to perform tasks. Western Sydney University/Navitas utilises both wired and wireless networks.

2.1.5 "*Passwords/Account codes*"

The mode of secured personal access to pre-determined IT resources.

2.1.6 "*User* "

Any person who makes use of any IT system, hardware or service owned or leased by the University.

2.1.7 "WSU"

Western Sydney University

2.1.8 "WSUIC Executive Management Committee"

Comprises the WSUIC College Director and Principal, the WSUIC Director of Quality and Student Administration, the WSUIC Director of Marketing and Admissions and the WSUIC Academic Director.

3. Authorised User Access and Responsibilities

3.1 WSUIC staff and students are authorised users and permitted access to University IT resources.

3.2 WSUIC use WSU and Navitas IT resources to discharge the responsibilities of their positions as employees, to further their studies/instruction as students, to conduct their official business.

3.3 Authorised Users are responsible for ensuring their usage complies with these policies and for informing Information Technology and Digital Services when they cease their association with WSUIC.

3.4 Passwords and login details are provided by WSU for the sole use of the authorised user. They should be treated as private and confidential, and must not be divulged or distributed.

3.5 Authorised Users must use only their own account/password on IT resources. Users are not permitted to access or attempt to access any program, file or other information stored under another person's account.

3.6 Authorised Users must not attempt to obtain passwords they are not entitled to know. This is applicable to accounts or facilities on Western Sydney University/Navitas computers or other computers accessed using the WSU network.

3.7 Authorised Users must not:

a) provide their passwords to others;

b) attempt to interfere with IT resources; and

c) attempt to subvert the security of any University IT resource.

3.8 Authorised Users must not use WSU/Navitas IT resources to copy software, upload or download material that is licensed or protected under copyright or trademark laws unless such activities fall within current licensing conditions and/or copyright legislation.

3.9 Authorised Users must not use WSU/Navitas IT resources to prepare, store, receive, display, transmit or communicate information, material or messages that:

a) are inconsistent with the mission or values of the University/Navitas

b) may have the effect of harassment of any person or

c) may be defamatory

d) include but are not limited to pornography, racism, sexism, obscenities, insults, threats and intimidation

3.10 Authorised Users must not use WSU/Navitas IT resources for commercial or private gain or the gain of a third party, except where there is an established relationship to Western Sydney University/Navitas (e.g. a commercial entity of WSU)

3.11 Authorised Users must treat WSU/Navitas IT resources with care, irrespective of location. No person shall deliberately damage, help to damage or tamper with facilities, resources or services. No WSU/Navitas owned or leased IT resource is to be moved off-site without appropriate permission

3.12 Authorised users must not use WSU/Navitas IT resources to gain unauthorised access to other computers/networks/systems/files/data, regardless of the intention.

4. Responsibilities of WSU and Navitas

4.1 WSU/Navitas are responsible for ensuring the services and resources it provides to its community are used in efficient, lawful, proper and ethical ways.

4.2 WSU/Navitas (or nominee/s) has the responsibility to:

a) ensure that IT services and resources are being used in an optimal way;

b) fully investigate breaches of this Policy, take action when required and report to other agencies (for example, the police) when necessary;

c) maintain accurate system records and monitoring records, archiving as appropriate;

d) assist the WSU Auditor or any other agencies (with the approval of the Vice-Chancellor and President or nominee) in investigating suspected breaches or conducting random audits;

e) disclose usage where appropriate; and

f) provide access controls where possible to limit usage not consistent with this policy (for example, STD bars, firewalls).

4.3 Navitas will ensure that the core services such as Student Management System, Learning Management System, are provided and used in an efficient way.

4.4 Navitas Service Desk are responsible for recording all incidents and allocating investigation or remediation work to core services as required. The Regional Data Protection Manager is responsible for capturing and escalating data breaches.

5. Responsibilities of the WSUIC Executive Management Committee

5.1 The WSUIC Executive Management Committee have the responsibility to ensure compliance with WSU and Navitas IT usage policies to:

a) ensure that all staff are made aware of WSU and Navitas policies in relation to their work at WSUIC;

b) ensure that all work practices comply with these standards;

c) lead by example with respect to this Policy;

d) notify WSU Information Technology and Digital Services/ Navitas Information Technology Services when a WSUIC staff member's access to a service or system should be withdrawn;

e) review applications for use of IT resources, and take responsibility for any costs incurred in respect to this; and

f) ensure that academics are aware of this policy when teaching students who are required to use IT resources in their studies so that specific subject requirements comply with this Policy.

6. Privacy

6.1 Users are responsible for the security, privacy and confidentiality of data of a private or personal nature, held or transmitted using IT resources. Users should become familiar with the WSU/Navitas and WSUIC's Privacy Policies and the Privacy and Personal Information Act 1998, so they are aware of their responsibilities for the collection, use and storage of personal information.

6.2 Any attempt (successful or otherwise) to invade the privacy of others using IT resources will be regarded as a breach of this policy.

7. Breaches and Penalties

7.1 WSU and Navitas work to ensure that they manage and uses its IT resources efficiently and effectively. To protect the interests of WSU/Navitas and to ensure compliance with this Policy, the WSU Chief Information and Digital Officer/ Navitas's Regional Data Protection Manager (or nominee) retains the right to examine any data or files and to monitor computer usage, and to intervene when necessary.

7.2 Breaches of this Policy will be reported immediately to the WSU Chief Information and Digital Officer/ Navitas's Regional Data Protection Manager. Complaints in relation to breaches may also be forwarded to the Chief Information and Digital Officer/ Navitas's Regional Data Protection Manager for action. In these circumstances confidentiality will be maintained.

7.3 If the WSU Chief Information and Digital Officer/ Navitas's Regional Data Protection Manager believes that unethical or illegal activities, or activities inconsistent with WSU's/Navitas's purpose or mission, have occurred, the following processes will be implemented:

a) the WSU Chief Information and Digital Officer/ Navitas's Regional Data Protection Manager (or nominee) will temporarily suspend the user from access privileges to all IT resources until further investigation;

b) if a breach is found to have occurred, the WSU Chief Information and Digital Officer/ Navitas's Regional Data Protection Manager, may decide to suspend access privileges for a defined period of time, depending on the seriousness of the offence;

c) where a WSUIC staff member has breached this Policy, if the offence is judged to be serious, the procedures outlined in the applicable employment agreement will be followed. Where a student has breached this policy, the procedures outlined in the current WSU Student Misconduct Rule/ Navitas's IT Acceptable Use Policy will be followed;

d) where a breach involves unethical or illegal activities, WSU/Navitas has an obligation to report these to the relevant external law enforcement agencies, and individuals may be subject to prosecution.

7.4 Breaches to this policy will be dealt with by both WSU Chief Information and Digital Officer/Navitas's Regional Data Protection Manager in consultation with WSUIC Board of Directors or delegate.

8. Audits

8.1 All WSU/Navitas IT resource usage is logged and may be audited. WSU/Navitas logs and audits the activities of WSUIC users. Usage and activity records belong to the WSU/Navitas and not to the individual user. In most cases, these are admissible as evidence and are subject to relevant State and Federal Laws.

9. Quality and Compliance

9.1 This policy and procedure is reviewed periodically as required (at a minimum every two years) for regulatory compliance, operational currency and the identification of continual improvement opportunities. This review is reflected in WSUIC's Risk Management Framework.

10. Related Forms and Documents

N/A

11. Related Policies, Procedures and Guidelines

- WSUIC Anti-discrimination, Harassment, Vilification and Bullying Policy
- WSUIC Student Misconduct Rule
- WSUIC Records Management, Retention and Disposal Policy
- WSUIC Privacy Policy
- WSUIC Staff Code of Conduct
- Navitas's IT Acceptable Use Policy
- WSU's Web Policy

Amendment History

Approval Authority:	Western Sydney University International College Board of Directors
Approval Date:	21 October 2016
Date for Next Review:	23 January 2026

Revision Date	Version	Summary of changes
21/10/2016	1.0	New Policy Developed and Implemented
21/01/2020	2.0	Replaced Western Sydney University International College with WSUIC; Re-writing and Re-formatting of the Policy; Inclusion of Navitas as provider of services throughout the Policy Addition of Related Policies, Procedures and Guidelines
14/02/2022	2.0	No amendments
23/01/2024	2.1	Removal of reference to 3rd party arrangements Correction of position titles