WESTERN SYDNEY UNIVERSITY

International College

IT Acceptable Use Policy

1. Purpose

1.1 This policy outlines the rules applicable to the use of IT resources at Western Sydney University International College (WSUIC) by providing and maintaining a secure, effective and reliable IT infrastructure and services to support WSUIC's operations.

2. Scope

2.1 This policy applies to all students, staff and any authorised users accessing IT resources at WSUIC.

3. Definitions

BYOD: Bring Your Own Device- the practice of allowing WSUIC employees to use their own computers, smartphones, or other devices for work purposes.

Email: Email means the Western Sydney University or Navitas provided electronic mail systems and computer accounts.

Authorised User: any person who has been given permission by WSUIC to access any IT system or IT facility at WSUIC, including but not limited to:

- Staff of WSUIC
- Staff of any entity/company in which WSUIC has an interest or commercial arrangement with
- Students of WSUIC/WSU or WSU The College studying at the WSUIC campus.

Credential – user identification and password, username and passcode, or PINs used to gain access to University ICT Services.

Personal Information - information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent.

Confidential and Sensitive Material: any information or material that a person knows or ought reasonably to know is confidential or sensitive, including but not limited to:

- The Personal Information of staff or students
- Student or staff health information
- Unpublicised strategic, legal, financial, or research information
- Any data that could compromise any facet of WSUIC, WSU or Navitas, including reputation

IT Resources: systems, software, hardware, services, communications and network facilities (including email, internet, and Wi-Fi access), and supporting infrastructure provided by or on behalf of WSUIC.

3. Policy Statement

3.1 WSUIC grants access to IT Resources to all Authorised Users, for the purpose of pursuing and advancing its business and educational goals.

3.2 WSUIC requires that all Authorised Users are aware of what conduct is expected of them in making use of IT Resources, and provides information and guidance (including this policy) to aid Authorised Users in determining its expectations

3.3 WSUIC IT Resources are and remain the property of WSU or Navitas. This includes named email accounts that are provided to Authorised Users for use with their study or work.

3.4 WSUIC is committed to allowing its Authorised Users to make incidental personal use of the IT Resources, provided such use is legal, and does not breach WSUIC policies.

3.5 If an Authorised User breaches the terms of this policy, their access may be restricted or revoked. Any breaches of this policy will be reported to the relevant WSUIC or regulatory authority or the police to take appropriate action, depending on the nature and seriousness of the breach.

4. Procedures

4.1 Access to and Use of IT Resources

4.1.1 Only Authorised Users may access or use IT Resources for purposes related to their relationship with WSUIC.

4.1.2 Accessing WSUIC IT Resources (internally or remotely) as an affiliate or associate requires an application to be approved by the College Director and Principal or delegate.

4.2 Termination of Access

4.2.1 When Authorised Users leave WSUIC, their User accounts — including documents, email and internet access (and records of access) — are archived and retired. Before leaving WSUIC, Authorised Users are responsible for tidying their own documents and mailboxes, making copies of any personal information that they will require, and contacting any internal or external correspondents to make them aware that their email address will be retired.

4.2.2 After access is terminated, WSUIC will only consider requests for creating a data extract for email or consolidated document retrieval if the request relates to:

4.2.2.1 A legal or investigative matter, as determined by the WSU - Office of General Counsel, a valid external authority (such as the State or Federal Police, or the ICAC, or an authorised investigator) or

4.2.2.2 A compelling, legitimate business reason supplied by the requester, approved by the College Director and Principal.

4.3 Acceptable and Unacceptable Use of IT

4.3.1 This Policy reinforces the provision of a fair, safe and productive computing environment by establishing clear responsibilities for Authorised Users of IT Resources that do not adversely impact the WSUIC's operations and reputation.

4.3.2 All Authorised Users must act in accordance with this Policy and all other WSUIC policies.

4.3.3 Authorised Users have a personal responsibility to be aware of the jurisdiction that applies to them when using IT Resources at WSUIC.

4.3.4 Authorised Users are permitted to use IT Resources at WSUIC for authorised purposes, providing that the use:

4.3.4.1 is lawful;

4.3.4.2 is in a responsible, ethical and equitable manner;

4.3.4.3 is consistent with the values of WSUIC as outlined in the WSUIC's codes of conduct;

4.3.4.4 does not create an intimidating or hostile work or study environment for others;

4.3.4.5 does not jeopardise the provision of a fair, safe and productive computing environment; and

4.3.4.6 does not adversely impact the WSUIC's operations, assets or reputation.

4.3.5 IT Resources at WSUIC must not be used in any manner, which WSUIC considers to be inappropriate, this may include, but is not limited to:

4.3.5.1 Accessing pornography;

4.3.5.2 Unauthorised monitoring of electronic communications;

4.3.5.3 Knowingly downloading, storing, distributing or viewing of offensive, obscene, indecent, or menacing material. This could include, but is not limited to, defamatory material, material that could constitute racial or

religious vilification, discriminatory material, material that incorporates gratuitous violence or frequent and highlighted bad language;

4.3.5.4 Stalking, blackmailing or engaging in otherwise threatening behaviour;

4.3.5.5 Any use which breaches a law, including copyright breaches, fraudulent activity, computer crimes and other computer offences;

4.3.5.6 Transmitting spam or other unsolicited communications;

4.3.5.7 The introduction or distribution of security threats, including a virus or other harmful malware.

4.3.5.8 Examining, copying, renaming, changing, or deleting programs, files, data, messages, or information belonging to WSUIC or any other Authorised User;

4.3.5.9 Modifying, uninstalling or disabling any software or hardware;

4.3.5.10 Altering any restrictions associated with any WSU computer system, computer account, network system, personal computer software protection or other of the IT Resources at WSUIC;

4.3.5.11 Running network wide security assessment tools without permission from the area supervisor and WSU ITDS;

4.3.5.12 Removing any IT Resources from WSUIC premises without authorisation.

4.3.6 Authorised Users must not attempt to gain unauthorised access to WSUIC IT Services (and the information stored thereon) to which they have not been given access or permit others to do so.

4.3.7 Authorised Users must not tamper with WSUIC IT Services that may potentially cause performance degradation, service instability, or compromise operational efficiency, security or fair use.

4.4 BYOD — Bring Your Own Device

4.4.1 When using BYOD, Authorised Users must take all reasonable steps to:

4.4.1.1 prevent the theft or loss of WSUIC Digital Information;

4.4.1.2 keep information confidential where appropriate;

4.4.1.3 not hold any WSUIC digital information that is Confidential and Sensitive on a BYOD device;

4.4.1.4 delete any WSUIC business information from any personal devices immediately after it is no longer required. This includes information contained within emails;

4.4.1.5 ensure that relevant information is copied back onto WSUIC systems and manage any potential data integrity issues with existing information;

4.4.1.6 report the loss of any device containing WSUIC data (including stored or saved email) to the WSU IT Service Desk;

4.4.1.7 advise WSUIC if the device is lost or stolen. Be aware that if WSUIC is advised that the device is lost or stolen, WSU IT Digital Services or Navitas IT Shared Services may wipe messages, by remote action, from the device. WSUIC is not responsible if unrelated or personal information is lost in this process;

4.4.1.8 remove all data belonging to WSUIC on any BYOD devices before leaving WSUIC; and

4.4.1.9 be aware of any data protection issues and ensure Confidential and Sensitive WSUIC Digital Information is handled appropriately (see the Privacy Policy for more information).

4.5 Breaches of this Policy and its Penalties

4.5.1 Breaches of this Policy may be grounds for serious misconduct.

4.5.2 A breach or alleged breach of this Policy may result in a referral of the matter to the police and/or other relevant external authority

4.5.3 WSUIC may immediately suspend an Authorised User's account in the case of a breach or an alleged breach of this Policy.

4.5.4 If an alleged breach of this Policy is reported to the College Director and Principal, action will be taken. This action includes protecting a person who has made a Public Interest Disclosure.

5. Quality and Compliance

5.1 This policy and procedures is reviewed periodically as required (at a minimum every two years) for regulatory compliance, operational currency, the identification of continuous improvement opportunities and risk identification and mitigation. This review is reflected in the Western Sydney University International College's Quality and Compliance and Risk Management Frameworks.

6. Related Forms and Documents

N/A

7. 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

Amendment History

Approval Authority:	Western Sydney University International College Academic Board
Approval Date:	25 October 2019
Date for Next Review:	17 December 2023

Revision Date	Version	Summary of changes
25/10/2019	1.0	New Policy Developed and Implemented
18/12/2021	1.0	No Amendments