



Information Technology Acceptable Use & Security

United Institute seeks to provide our staff members and learners with a secure and timely access to IT equipment as well as online services and resources necessary to be able to carry out their duties and learning. United Institute's IT facilities and services shall be used in an approved, ethical and lawful manner to avoid loss or damage to our operations, image, or financial interests and to comply with official acceptable use. Users of United Institute's IT facilities and services shall contact the Student & Administration Support personnel prior to engaging in any activities not explicitly covered by these policies.

General Information Technology Acceptable Use & Security Principles

United Institute strives to maintain a safe, secure and easy to use information technology systems and networking framework for our staff members and learners.

We aim to do so by ensuring:

- Adequate training is provided in the use of our IT platforms and facilities;
- Our staff members and learners have timely access to IT support;
- Our IT systems and framework are regularly reviewed and undergo maintenance to ensure it is able to fend off any intrusions and cyberattacks, and is upgraded to recognise and incorporate the latest technologies for the benefit of our staff members and learners;
- We build a seamless experience for our users; and
- Our IT personnel and contractors are adequately skilled and knowledgeable to undertake and perform to our expectations and requirements.

Acceptable and Unacceptable Use of IT Facilities and Services

- United Institute's IT facilities and services are provided for use in the professional, administrative, commercial and community activities of the organisation. Some reasonable non-commercial personal use may be allowed, but this is a privilege and is not a right. If that privilege is abused, it will be treated as a breach of this Policy.
- The use of the IT facilities and services must not jeopardise the fair, safe and productive IT environment of our community, nor our operations, assets and reputation.
- The IT facilities and services provided must not be used unlawfully or for an unlawful purpose.

Access and Accounts



- All staff and learners are entitled to access the IT facilities and services, at a level appropriate to their position and role, via a unique password protected account.
- United Institute may impose quotas on the use of the IT facilities and services (including print, file storage, e-mail and internet download) and will revise them as necessary. Where quotas exist, account holders are expected to comply with them. If an account holder exceeds any of their quotas, they may be temporarily prevented from using United Institute's IT facility or service.
- When staff or learners no longer have a relationship with the organisation or are no longer authorised to have access to the IT facilities and services, their accounts will be disabled for a period of 3-months, and then deleted.
- Users may have their IT access suspended immediately where there is a suspected breach of the organisation's Policy.
- All users must:
 - Not use their access to gain any inappropriate personal, professional or other advantage;
 - Not manipulate United Institute's data without authorisation; and
 - Maintain the confidentiality of any personal or confidential information accessed via the IT facilities and services.

Security

- United Institute will take reasonable steps to protect the IT facilities and services from unauthorised and unacceptable use and intrusions.
- To preserve the organisation's standard operating environment and ensure compliance with licensing obligations, users of the IT facilities and services may only modify the standard configuration of any of the IT facilities and services, after first gaining approval from the IT Manager. Users must never install or use unlicensed or malicious software on the IT facilities and must not connect unapproved networking devices to our organisation's IT infrastructure.
- Users of the IT facilities and services must not circumvent the authorised internet connection(s) or subvert our IT security measures.
- All United Institute's IT hardware, especially portable devices, must be kept secured at all times against damage, misuse, loss or theft. In addition, hardware and software containing sensitive information or data must be protected with appropriate security measures such as passwords and encryption.

User Responsibilities



- It is a condition of use of the IT facilities and services that this Policy, particularly the principles of acceptable and unacceptable use, and its associated procedures must be complied with.
- Users must not:
 - Access pornographic or obscene material or material that could offend others;
 - Let anyone else use any of your accounts or tell anyone else your password;
 - Download videos, music or anything else that is copyrighted by other people;
 - Use the IT facilities to bully or harass other people;
 - Install unlicensed or malicious software;
 - Use the IT facilities to advertise for goods or services for personal purpose;
 - Forget to log out of the computer systems when you have finished using them;
 - Use the IT systems for purposes not relating to your work or learning at United Institute; and
 - Forget to think carefully about your online conduct to protect personal information.
- Users are responsible for all activity initiating from their account.
- Users must only access the IT facilities and services using their own account.
- Users must ensure that their passwords are securely stored.
- Users of the IT facilities or services provided by a third-party provider on United Institute's behalf must comply with any terms and conditions issued by that third-party provider.
- Users of the IT facilities and services must not create, send, store, upload, access, use, solicit, publish or link to:
 - Offensive, obscene, profane or indecent images or material;
 - Material likely to cause annoyance, inconvenience or distress to other individuals or cultures;
 - Discriminating or sexually harassing material or messages that create an intimidating or hostile work environment for others;
 - Defamatory material or material that makes misrepresentations or could otherwise be construed as misleading;
 - Material that infringes the intellectual property (including copyright) of another person or organisation;
 - Malicious software such as viruses, worms or address-harvesting software.
- The IT facilities and services must not be used in the conduct of any personal business or unauthorised commercial activities.



- The IT facilities and services must not be used for any illegal activity such as sending chain letters, breaching the SPAM Act 2003, or attacking of other computer systems.
- Staff must include the appropriate sections of the organisation's official signature and disclaimer on all e-mail messages sent.
- Electronic materials must never be forwarded on without the express or implied permission of the material's creator.
- Peer-to-peer and torrent software must only be used for lawful purposes.
- Any observed security weaknesses in or is a threat to the IT facilities and services, as well as any known or suspected breach of this Policy and its associated procedures must be reported to the Student & Administration Support personnel as soon as practicable.

Managing and Monitoring

- United Institute will manage user accounts, maintain a secure IT environment and keep users of the IT facilities and services informed of their user responsibilities and expected best practice standards.
- United Institute reserves the right to investigate any and all aspects of its electronic information systems if it is suspected that any user of the IT facilities and services is acting unlawfully or violating this Policy or any other business Policy.
- United Institute may take action it considers necessary to remedy immediate threats to the IT infrastructure or security, including suspending authorised accounts and/or disconnecting or disabling relevant IT facilities or other equipment, with or without prior notice.
- United Institute reserves the right to block or filter any network traffic that potentially breaches this Policy or is potentially illegal.

Consequences of Non-Compliance

- Minor breaches of this Policy will be addressed by sending e-mails to users requesting that they desist from the breaching behaviour.
- Ongoing or serious breaches of this Policy or any other related IT Policies by any user will be addressed by the relevant disciplinary procedures.
- If a breach of this Policy, including procedures, appears to constitute an offence under State or Commonwealth law, United Institute may (and in some cases is obliged to) refer the suspected breach to the appropriate law enforcement agency(ies).



Utilising Social Media

- The same standards you use in real life should be applied online – including laws, business policies, behavioural expectations and the rules or common courtesy.



- The following principles provide some additional guidance specifically relevant to social media use:
 - Be respectful, genuine and credible.
 - Remember each social media platform is different. Make sure you understand the nuances and accepted communication style of each tool, before you jump in and start posting.
 - Remember social media spreads far and wide – please therefore post appropriately. If you would not do something in front of a room full of people, you should not be posting it online either.
 - If you make a mistake, admit it and fix it quickly.
 - Maintain confidentiality. Social media is inherently unsecure and far-reaching in its audience. Do not share any confidential, private or sensitive information through social media.
 - Protect your own safety and privacy. Consider your own privacy and safety before broadcasting real-time details about where you are or what you are doing. make sure you fully understand the privacy settings you have for limiting who can see your information or posts.
 - Be aware of liability. You are responsible for your own posts, and they are almost impossible to erase. Be sure that what you post would not come back to haunt you later.
 - Think about how your posts might affect other people. If you write something negative or inflammatory about someone on a social media site, the whole community can see it – so it may have a much greater impact on others, even though you may not see that impact first-hand. If you would not say it to someone's face, do not post it online.
 - Think about what capacity you are acting in. if you are acting in an official United Institute capacity, or as a person with a United Institute connection, see the additional guidance below. If you are acting in your personal capacity, be sure to make that clear (especially where people might get confused as to whether you are speaking on behalf of the organisation).
 - Distinguish between your personal and professional capacity. Make it clear when you are not speaking on behalf of the organisation. If an issue relates to your role within United Institute and you are commenting on it, you should identify yourself and your connection to the organisation. You must then behave as the business directs through policies, codes and employment terms.
 - Act within your authority. Just as you need authority to speak on behalf of the organisation to the media or to any outside entities, you need authority to speak as a United Institute representative on social media sites.
 - Do not use your online presence to damage the organisation and its reputation.
 - All staff and learners should exercise careful judgement when interacting with others on social media sites. The guiding principles should be the same as for your relationships with others in the non-online world, including that you do not exert undue influence (or give the perception of exerting undue influence, or make the other feel like they are being influenced).
 - Something posted on a social media site is still a written communication, so the same legal ramifications can flow, such as defamation, trade practices or fair trading violations, or a breach of privacy or confidentiality – and because it is written in a permanent forum, hard copy communication. Do not post anything on behalf of the organisation without prior approval from the CEO, as it may have legal consequences.
 - Respect the organisation's reputation and branding.
 - Reach out to others across the organisation who are maintaining our social media sites or posts, especially when they are targeted to the same audience. Work collaboratively to ensure a consistent tone and approach.

- Ask yourself whether there is anyone you should keep informed about your social media communications on behalf of the organisation. Think about who you would include in on the same communication if it was in hard copy or e-mail from – the same people should be informed about your social media posting.

United Institute Pty Ltd | RTO No. 45843 | CRICOS Code: 04011J | Website: www.united.edu.au

Campus Address: Level 10, 474 Flinders Lane, Melbourne VIC 3000 Australia

Workshop Address: 673 Spencer Street, West Melbourne, VIC 3003 | Phone: +61 434 455 708 | Email: info@united.edu.au



E-mail Etiquette

- Efficient and effective use of e-mail is crucial to many business activities. Please observe the following recommendations when using United Institute's e-mail services:
 - Make sure your e-mail messages are concise and limited to relevant individuals.
 - Use United Institute's recommended signature and disclaimer on all e-mails.
 - Ensure that all e-mails sent complies with the SPAM Act 2003 – this means that commercial electronic messages should not be sent except to e-mail lists or groups that have been established specifically for the purpose of buying or selling goods or services. Commercial electronic messages may only be sent from United Institute e-mail accounts if:
 - The consent of the recipient can be construed, a functional unsubscribe facility allows the recipient to withdraw their consent at any time, and any requests to unsubscribe are actioned within **5 business days**; or
 - The message relates to goods or services supplied by United Institute and is sent to current or former employees, clients or candidates that have previously registered their details with United Institute.
 - Use a meaningful subject to ensure the recipient will know what the e-mail is about.
 - Lay out the message neatly for clear readability and do not use very long sentences. Use spaces and breaks between paragraphs.
 - Take care with sarcasm and humour so that you are not misinterpreted. E-mail lacks the cues of body language and intonation which are present in verbal communication.
 - Take time to consider and re-read your message before sending it. Do not reply in the heat of the moment as a message may not be able to be recalled.
 - Do not write anything you would not say in public – e-mail is not confidential.
 - When sending attached files such as spreadsheets or word-processed documents, use a version which is likely to be supported by the recipient.
 - When replying to all, review the list of addresses and only include those who need to receive your reply.
 - Keep the thread when replying to an e-mail and use the reply option to preserve the thread of the discussion.
 - Carefully check the addressee before sending.
 - Do not re-direct message without the original sender's permission – it may not be appropriate.