IT Acceptable Use Policy

Policy Owner	College Director & Principal
Contact Officer:	IT Officer
Policy Number:	QBIPO020
Approved by:	Senior Management Group
Date Approved:	November 2013
Last Reviewed:	September 2019
Related Policies:	Email and Internet Policy Navitas IT Acceptable Use Policy Navitas Information Security Policy Navitas Delegation of Authority and Authority Limits Policy Privacy Policy Risk Management Policy
Related Documents:	Code of Conduct Navitas Delegation of Authority and Authority Limits Procedure

1. PURPOSE AND SCOPE

This policy is effective at Curtin College and applies to all system users at any location, including those using privately owned computers or systems that connect to Curtin College computer and network resources.

This policy represents the minimum requirements that must be met. In general, this policy is not intended to inhibit access to information services that Curtin College has made accessible for public inquiry (eg. internet) via Curtin College computer and network resources. However, use of such services to access or attempt to access information not intended for public display or use, or to circumvent or violate the responsibilities of system users or system administrators as defined in this policy, is prohibited.

The computers and computer network at Curtin College together with access to the internet and email are provided primarily for educational, professional and business purposes. The use of these facilities should therefore be consistent with that purpose.

2. UNDERLYING PRINCIPLES

Users must adhere to all elements of this policy. The principles of behaviour relating to the use of Curtin College IT resources include:

- Respect for the law;
- Respect for other people; and
- Respect of the Curtin College's mission and values.

The principles of conduct of users also assume:

- Integrity;
- Diligence;
- Economy; and
- Efficiency.

3. ROLES & RESPONSIBILITIES

3.1 Navitas Board

Curtin College is a wholly owned subsidiary of Navitas Proprietary Limited. The Navitas Board is ultimately responsible for ensuring the services and resources it provides within the group are used in efficient, lawful, proper and ethical ways (appropriate use). The Navitas Board delegates this responsibility to the Executive team.

3.2 Navitas Chief Executive Officer (CEO) and Executive & Group General Managers

The Chief Executive Officer is accountable to the Navitas Board for the appropriate use of information assets, with all Executive and Group General Managers having a responsibility for the effective implementation of this Acceptable Use Policy in their business unit. This will be achieved through the delegation of responsibility for the management of acceptable use to the Navitas Managers. To support this, common tasks will include:

- Authorising User account establishment for all users who require access to the network and its resources;
- Ensure all users are made aware of this Policy in relation to their work at Navitas;
- Ensure all users are made aware of their responsibilities for IT Security;
- Ensure that all work practices comply with this Policy;
- Lead by example with respect to this Policy;
- Notify service.desk@navitas.com when a staff member's access to a service or system should be withdrawn; and
- Review use of IT resources and take responsibility for any costs incurred in respect to this.

3.3 Chief Technology Officer

In addition to ensuring the effective implementation of this Policy in their business unit the CTO is accountable for the ongoing development, approval, implementation, awareness and effectiveness of this Policy and the supporting processes and documentation. To support this, common tasks will include:

- Ensure that IT services and resources are being used in an optimal way;
- Investigate breaches of this Policy, taking action when required and reporting to other agencies (eg. the Police) when necessary;
- Maintain accurate system records, monitor records and archive as appropriate;
- Disclose usage where appropriate;
- Provide access controls where possible to limit usage not consistent with this Policy;
- Management of IT Security Policy including the maintenance of the IT Security Policy;
- Authorise certain Navitas staff of the IT Support Division to monitor accounts, files, stored data and network data or to disconnect IT equipment in the event of an IT security breach;
- Authorise any extraordinary action taken to monitor IT services;
- Instruct IT Support authorised staff in privacy, confidentiality and need-to-know principles in relation to treatment of data, information and material discovered by IT Support Authorised staff whilst monitoring.

3.4 Curtin College IT Officers

Under delegation from their Managers, and the Navitas CTO, they are responsible for IT security matters within Curtin College. To support this, common tasks will include:

- Receiving reports of IT security breaches from users and to take appropriate remedial action;
- Abiding by the Curtin College Privacy Policy;
- Providing additional information for users that request assistance on understanding their responsibilities under the IT Security and Acceptable Use Policies;
- Ensuring IT Resources provides adequate security of staff information through limiting of access to information by non-authorised users.

3.5 Curtin College Line Management

All Curtin College Managers are responsible for ensuring that all employees and students are aware of this Policy and their responsibilities defined here.

3.6 All Curtin College Users (e.g. employees, students, visitors)

All Curtin College users have a general duty of care and are responsible for being aware of, and complying with this Policy. This will include:

- Ensuring their usage complies with this Policy, and for informing the IT department when they cease their association with Curtin College;
- Respecting the physical hardware and network configuration of Curtin College owned networks. Users must not extend the physical network on which their system resides (eg. extra switches or a wireless connection);
- Not performing any unauthorised, deliberate action that damages or disrupts a computer system, alters its normal performance, or causes it to malfunction;
- Not using Curtin College systems to gain unauthorised access to other computers, networks or information regardless of the intention;
- Reporting any suspected security problems or unacceptable use to service.desk@navitas.com , and not demonstrating the problem to others. Any user who believes their files have been tampered with should immediately change their password and contact service.desk@navitas.com with the specific details;
- Respecting the Curtin College Privacy Policy and treating all confidential or sensitive information appropriately; and
- Not using any of Curtin College's official branding materials (eg. name or logo) on their personal web pages; email, or other messaging facilities.

4. Acceptable Use Principles

4.1 User Accounts (e.g. employees, students, visitors)

Users are ultimately accountable for all actions attributed to their User Account.

To support this Users are responsible for safeguarding their passwords and/or other sensitive access control information related to their accounts or network access.

Similarly, system users must recognise the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share or divulge such information. Any attempt to conduct such actions by a system user is a violation of this policy.

Users shall ensure access privileges are restricted to their own use only. Users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorised computer and network access privileges to others. System users must not implant, execute or use software that allows them unauthorised remote control of computer and network resources, or of accounts belonging to others. If specific access is required, service.desk@navitas.com should be contacted rather than disclosing a password.

System users must not implant, execute or use software that captures passwords or other information while the data are being entered at the keyboard or other data entry device.

Users must not obtain nor attempt to obtain any electronic communication or information not intended for them. In particular, system users must not attempt to intercept or inspect information (e.g., packets) en route through Curtin College computer and network resources, nor use Curtin College computer and network resources to attempt to intercept or inspect information en route through networks elsewhere.

Unattended workstations must always be logged off or left in the Workstation Locked mode (Mac: Ctrl + Shift + Power, Windows: Windows key + L) when the operator leaves their workstation unattended.

All passwords must meet the following minimum standards:

- All accounts must have passwords.
- Passwords for accounts must not be shared, unless a Group account has been specifically authorised in writing.
- Passwords for user accounts must have an expiration date of 90 days. Passwords for system accounts may have a longer duration.
- Passwords must be resistant to a computer program that checks passwords against previously used passwords and passwords that are easily discovered or compromised by human or computational means.
- Passwords must use a mix of alpha and numeric characters and contain at least 8 characters if the operating system supports passwords of that length.
- Passwords to computer and network resources containing computerised institutional data will not be issued over network media in clear text unless a secondary means of authentication is provided (eg, smart cards).

4.2 IT Systems Use

Users will, by default, only have access to the information and systems that they need, to perform their function. Elevated local access privileges must only be granted for essential and specific purposes.

Removable media items including but not limited to USB connected media, Hard Drive, SD or other memory cards or optical media (CD/DVD) are not to be used on Navitas systems or networks without express (documented) permission by Company IT.

Sensitive information stored on portable devices (e.g. laptops, PDAs) must be encrypted. This ensures that the data remains confidential if the device is lost or stolen. Users may not copy any information or software stored on their desktop or laptop computer, for personal use.

Users may not use Curtin College systems for any of the following activities:

- Gambling or Internet gaming.
- Share trading (unless you have express permission due to your company role)
- Use any Curtin College IT systems for personal financial gain, solicitation or private business purposes.
- Posting any Curtin College information to internet bulletin boards, discussion lists, news groups, chat groups or other internet discussion forums that are accessible by the public unless you are authorised by your Manager to do so.
- Any political activity
- Sending offensive, harassing, intimidating or discriminatory messages or attachments, or to transmit offensive, sexually explicit or other inappropriate material
- Downloading malicious software or applications
- Browsing, sharing, downloading from or otherwise accessing illegal websites
- The use of on-line security scanning or hacking/cracking tools
- Downloading or storage of data subject to intellectual property or copyright

4.3 Safe Practices

Users (e.g. employees, students, visitors) shall work in accordance with safe computing practices to minimise the risks associated with computer viruses.

Users are advised to use caution when opening email attachments from unknown sources. Users shall not open any received .exe, .pif, .com, or .scr files without prior consultation with IT staff. If virus protection software detects a virus from an incoming file, inform the person who introduced that file so they can ensure it does not happen again. If a computer is acting strangely, there may be an undetected virus. This does not happen often, but it is worth checking with IT Support. The wilful introduction of computer viruses or other disruptive/destructive programs into Curtin College computers or networks, or into external networks using the Curtin College network, is not permitted.

4.4 Inappropriate Material

Do not download inappropriate material, store it on your computer or on the Curtin College network, or include within email or other communications means. Inappropriate content includes but is not limited to the following; information or media that could be considered illegal, harassing, offensive, sexually explicit, racist, sexually discriminatory, in violation of other Curtin College policies or that could reflect adversely on the college.

4.5 Email

Emails must be written with the same consideration as any physical communication, which would feature the Curtin College logo.

Users must not use Curtin College resources to forward chain letters or spam mail, alter messages so they appear to have been sent by someone else, or delete/edit the automatic signature that appears on the bottom of Curtin College emails.

Automatic or manual forwarding of emails to non-college or non-Navitas email addresses is not permitted. Where there is an approved business requirement exception, it will be considered by the Global Head of Information Security.

Do not use college email accounts for personal use.

Do not send unsolicited emails to persons.

Do not use Curtin College email to solicit interest in goods or services, participation in surveys, events or group activities or links to any third-party URL or hosted sites.

Do not use Curtin College email addresses when registering with 3rd party web sites (especially social media) unless you have permission to do so from the college as part of your job role.

4.6 Monitoring

Curtin College reserves the right to regularly audit IT systems to ensure compliance with this policy.

As part of normal system operation, Curtin College reserves the right to maintain logs of email system activity. These logs identify sender, recipient, message size, relay, date and time.

As part of normal system operation, Curtin College network systems generate logs of all www activity and access. These systems are the DNS and internet cache. The logs from these sites identify destination sites, pages, page download size, and originating Curtin College computer.

Remote access connections to Curtin College are monitored. Monitoring includes connection dates and times and may include access to system resources.

To ensure compliance to licensing obligations Curtin College reserves the right to scan all Curtin College equipment to detect illegal or non-Curtin College registered software and remove it.

All files, including those generated via internet email and proprietary email systems, are generally accessible by persons with system administration privileges (eg, Curtin College IT staff). Users are discouraged from maintaining anything private on the servers or desktop computers.

Access to Curtin College IT systems is provided to you on condition that you consent to monitoring in accordance with this and the IT Security Policy. Your use of Curtin College IT systems constitutes your consent to the monitoring.

4.7 Curtin College Assets

Hardware always remains the property of Navitas Pty Ltd, on cessation of employment all hardware must be returned in a clean, tidy, working and prompt fashion to Curtin College.

Laptops and desktop computers are issued for use by Curtin College staff only. Laptops and accessible Curtin College resources (e.g., internet access) are not provided for non-Curtin College staff members to use (i.e., friends, family, etc.).

The unauthorised duplication of copyrighted computer software violates the law and is contrary to Curtin College's standards of conduct and business practice. Curtin College does not permit such copying.

All software used on the Company provided devices must be approved by Navitas IT. Users may request additional software through their line management where a business justification exists.

Users are not permitted to install their own software on any company computers, without prior approval from Navitas IT. Failure to comply may result in users being held personally responsible for any data loss or penalties imposed for breach of copyright.

4.8 Breaches

Any security exposures, misuse or non-compliance must be reported as soon as an occurrence is identified to service.desk@navitas.com.

Breaches of policy compliance may result in disciplinary action being taken against the offender.

4.9 Confidential Information

Curtin College staff members have a duty to keep confidential:

- All Curtin College data unless the information has been approved for external publication; and
- Information provided in confidence to Curtin College by other entities.

Each staff member is under a duty not to disclose Curtin College business information unless authorised to do so. Breach of confidentiality through accidental or negligent disclosure may expose a User to disciplinary action.

4.10 What is Confidential and Sensitive Information

Company and/or sensitive information includes and will include all trade and business secrets and other confidential information and documents relating to the affairs or business of the Company or any person with whom you come into contact as a result of your employment with the Company or who may come into your possession in the course and by reason of your employment whether or not the same were originally supplied by the Company.

Confidential information includes any information (written or verbal) of a commercial, technical or financial type which is not publicly available.

Users must not make unauthorised copies of any material (original or not) such as correspondence, company manuals, computer printouts, removable media, computer lists, diaries, file notes or any other material whether or not compiled or made by you, or to which you have access as part of your employment.

All such material is and remains the property of the company. All company property must be returned upon termination of your employment.

4.11 Legal Requirements

For legal purposes, email has the same standing in court as paper documents. Users must be aware that Curtin College can be involved in litigation. Any records relating to use and activities in relation to email, internet and intranet are discoverable by way of court order or subpoena. These include matters affecting legal proceedings, affecting personal affairs of employees, parents, students, or third parties, as well as relating to research, or other communications even if communicated in confidence.

Email residing on or transmitted across the Curtin College system is the property of Curtin College. All electronic files are the property of Curtin College, and users should act on the basis that they can be, and where necessary will be, held accountable for their messages and their stored files.

While all transmissions remain the property of Curtin College by law, all efforts to retain professional confidentiality will be made. All internet activity is recorded for individual users. If required Curtin College have the right to view an individual's Internet activity at any time.

Should access to an individual's files or internet logs be necessary for an alleged criminal offence or serious disciplinary matter, the individual concerned will generally first be told the circumstances of the complaint and be present when the files or logs are opened. Notwithstanding the above, Curtin College reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any Curtin College computer.

4.12 Relevant Legislation

Users need to be aware that certain conduct may breach laws outside of Curtin College and lead to criminal or civil proceedings and/or penalties for which they will be held personally accountable. In Australia these laws include:

- Equal Opportunity Act 1984 (WA)
  http://www.austlii.edu.au/au/legis/wa/consol_act/eoa1984250/
- Sex Discrimination Act 1984 (Cth)

  http://www.austlii.edu.au/au/legis/cth/consol_act/sda1984209/
- Disability Services Act 1993 (WA)
  http://www.austlii.edu.au/au/legis/wa/consol_act/dsa1993213/
- Disability Discrimination Act 1992 (Cth)
  http://www.austlii.edu.au/au/legis/cth/consol_act/dda1992264/
- Racial Discrimination Act 1975 (Cth)
  http://www.austlii.edu.au/au/legis/cth/consol_act/rda1975202/
- Censorship Act 1996 (WA)
- http://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/wa/num_act/ca199640
- Copyright Act 1968 (Cth)
  http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/

- Privacy Act 1988 (Cth)
  http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/
- SPAM Act 2003 (Cth) http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366/index.html and
- Other relevant Commonwealth and/or State laws such as those relating to the transmission of offensive material and Telecommunications.

In countries other than Australia there are similar laws that provide guidance relevant to this policy. Local legislation must always be adhered to, however if the local legislation does not meet the baseline statements in this Policy the local business unit shall adhere to these baseline statements.

Version (Date):	**Improvements made:**
V1.2 (Sept 2019)	Removed outdated information, aligned with Navitas IT policy and updated links.
V1.1 (July 2016)	Updated links in policy and change in title re item 3.3