IT Acceptable Use Policy (for Students)

Navitas Limited
ACN 109 613 309

Document

Document Name	IT Acceptable Use Policy (for Students)
Responsibility	Chief Technology Officer
Initial Issue Date	01/09/2021

Version Control

Date	Version No.	Summary of Changes	Reviewer Name and Department/Office
15/03/2021	1.00	Initial Release	Navitas IT
21/10/2021	1.01	Inappropriate content update (added to section 2.11) and other minor changes	Navitas IT

Related Documents

Name	Location
IT Acceptable Use Policy (for Staff)	Policy HUB

Contents

1. Purpose and Scope

1.1 Introduction

This IT Acceptable Use Policy ("Policy") sets out the global approach of Navitas Limited and its affiliated group companies (together the "Company") relating to the minimum requirements that users are bound to when using hardware, software, Internet and network equipment (together "IT systems") that is owned and operated by the Company. This Policy supersedes any other IT Acceptable Use Policies published across the Company.

The Company is a professional organisation and users are expected to use the IT systems in order to facilitate successful education outcomes. This policy represents the minimum requirements that must be met by all users.

1.2 Scope

This Policy has been prepared in accordance with the Company's legislative requirements and principles. This Policy is effective across the entire Company and applies only to **Students** ("**Users**") of IT systems, including those users using privately owned computers that connect to the Company network resources and applications.

2. Policy Statement

2.1 Underlying Principles

All users must adhere to all elements of this policy. The principles of behaviour relating to the use of the Company IT systems includes:

- Respect for appropriate legislation and regulations
- Respect Students and Teaching Staff and
- Respect of the Company's mission and values

The principles of conduct of users also expect:

- Integrity
- Diligence
- Economy and
- Efficiency
- Common sense

2.2 Role & Responsibilities

All users of the Company IT systems have a responsibility to maintain compliance with this policy and all relevant policies. Additionally, all users have a responsibility to maintain security and to report anything that may be detrimental to the Company.

The Service Desk may be used (as per the arrangements for the College) for recording all incidents and allocating investigation or remediation work to core services as required. The regional Data Protection Managers are responsible for capturing and escalating data breaches.

2.3 User Accounts & Passwords

You are responsible for any activity that is performed whilst your network account is logged on. Do not share your password with any other person (including IT) and do not log in using any other user's credentials.

Passwords are the "key" into the Company's IT systems - it is your own responsibility to ensure your password is kept secure. There are two key password management practices that make it harder for attackers to access the Company's systems and data.

- Use "Strong Passwords". These can slow down or often defeat the various attack methods used to compromise IT security. The Company requires you to always use Strong

Passwords. A Strong Password is one that is not easily guessed (not your name, family members, pets, relative or anything else that could be attributed to you). Passwords must be minimum of eight characters long and containing a combination of upper and lowercase letters numbers and special characters. Longer passwords (13+ characters) with less complexity (variation in character types) also increase the strength of the password. The stronger the password, the harder it is to guess or crack.

- Always use different passwords for different sites; whilst it's convenient to re-use the same password for personal logins, ensure your password is not one that you use elsewhere. Using a unique password for your User accounts ensures that systems remain secure if any of your personal accounts are compromised and vice versa.

The use of Multi-factor authentication (MFA) is mandatory if operating in the Company network.

2.4 Personal Use of Company Computers and IT Facilities

IT systems should not be used for anything other than academic pursuit.

- A network account is provided to a user for the period of their enrollment
- Users are required to manage their allocated network and email storage quotas
- Users are not to store private data on company IT systems
- Users must not lock IT systems, thereby preventing other users from accessing them
- Users must not consume food or drinks around or near IT systems
- Occasional use of the company IT systems is acceptable using the internet e.g. checking the news, etc. The same applies to other IT facilities such as Internet connectivity, printing or scanning.
- Company IT systems must not be used for the following:
    - Gambling or Internet gaming
    - 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 or the use of on-line security scanning or hacking/cracking tools[1]
    - Use of IT systems for personal financial gain, solicitation or private business purposes, e.g. crypto currency mining
    - Posting information on bulletin boards, blogs or forums that are accessible by the public unless you are specifically authorised to do so
    - Downloading or storage of data which would breach copyright laws
    - Represent the Company on social websites and taking care when posting pictures that they do not contain Company information in the background and that you have permission of your Company employees before posting any pictures of them.

Specific agreement is required between the Company and the consumer when it provides a service such as Internet for personal use.

[1] Unless used as part of a persons documented working duties.

2.5 No Outside Internet Use

Company IT systems are only to be used for academic purposes. The only exception is the occasional use permitted in 2.4 above. Any form of outside interest use is prohibited, unless the Company has given prior written authorisation. This means that users of the Company's IT systems must not use and must not allow any non-Navitas person or organisation to access or use the Company's IT systems, services and equipment for any purpose.

This includes but is not limited to the follow types of actions:

- Sending unsolicited emails to persons
- Using email or social media platforms to solicit interest in goods or services, participation in surveys, events or group activities or links to any third-party URL or hosted sites
- Data mining for personal information including email addresses, telephone numbers, social media profiles or other personal information that may be stored or accessible on the Company's system

2.6 Equipment, Security & Loss

The Company will supply all the necessary equipment/devices to access its computer systems and networks. Ensure that Company assets are treated with respect. Do not leave any Company assets unattended where they could be stolen or abused. Users are personally responsible for all equipment issued to them by the Company. Lost or stolen devices must be immediately reported to the Company through the normal Student contact points.

Hardware always remains the property of the company, on cessation of enrolment hardware must be returned in a clean, tidy, working and prompt fashion to the company.
All devices, i.e. tablets, mobile devices, notebooks, laptops and desktop computers are issued for uses teaching and learning needs only. Any such device is not provided for non-students to use (i.e., friends, family, etc).

The unauthorised duplication of copyrighted computer software violates the law and is contrary to the Company standards of conduct and business practice. The Company will comply with all licensing terms and conditions regulating the use of any software it acquires.

2.7 Shared Printing

Take care when printing sensitive or confidential material to a shared printer that is not controlled by a Student ID, login or print account system. Most printers support the use of password protection and secure print.

2.8 Information Security Threats

All users are responsible for the security of information that is owned by or entrusted to the Company. All actual or suspect security weakness are required to be immediately reported to the Service Desk.

The Company has inbuilt security features and controls in our email system, network and computers that can detect viruses and malware, but it can never protect you and the Company from every threat. Ensure you are familiar with how to recognise fraudulent email (e.g. phishing attacks) or links and websites[2]. Also, be careful with external USB, hard disk and other storage devices where you cannot verify the contents or the source of the device. Users are the first line of defence. Do not click on a link or open a file that you do not recognise.

Users are always required to remain vigilant. Formal Information Security Awareness training is available. Users can request access to this training via their teacher.

2.9 Use of Personal Email Addresses

[2] As advised through security awareness programmes.

Students should access information relating to their studies via their College Email Account. Although not preferred, Users may choose to forward their College Email account to a personal or work email account, so they do not miss out on important information. Users are responsible for all information sent to them via their College email account. If a User chooses to forward his or her Company email account, he or she is responsible for all information, including attachments, sent to those other email accounts.

2.10 SMS

The use of instant messaging (SMS) communication with Users will occur in the following circumstances:

- As a primary method to communicate with students
- In crisis situations where User's safety is deemed to be at risk

2.11 Inappropriate Content

Do not download inappropriate material, store it on your computer or on the Company network, or include within email or other communications means. Inappropriate content includes but is not limited to the following:

- Creation or transmission, or causing the transmission, of any offensive, obscene, or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creation or transmission of material, which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the College or a third party or which promotes discrimination based on race, gender, religion or belief, disability, age or sexual orientation.
- Creation or transmission of material with the intent to defraud or which is likely to deceive a third party, or which advocates or promotes any unlawful act.
- Unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others.
- Unsolicited or bulk email (spam), forge addresses, or use mailing lists other than for legitimate purposes related to College's activities.
- Material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party.
- Material that brings the College into disrepute.
- Deliberate unauthorised access to networked facilities or services or attempts to circumvent College security systems.
- Pursuance of commercial activities for personal gain.
- Deliberate activities having, with reasonable likelihood, any of the following characteristics:
    - Wasting employee's effort or time unnecessarily on IT management.
    - Corrupting or destroying other users' data.
    - Violating the privacy of other users.
    - Disrupting the work of other users.
    - Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).
    - Continuing to use an item of networking software or hardware after a request that use should cease because it is causing disruption to the correct functioning of the network.
    - Other misuse of network resources, such as the introduction of computer viruses, malware, or other harmful software.
    - Any breach of industry good practice that is likely to damage the reputation of any connected external network e.g. JANET or AARNet, will also be regarded as unacceptable use of the College Network.
- Introduce data-interception, password-detecting or similar software or devices to the College's Network.

2.12 Software

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

Software and apps and device licences always remain the property of the Company. Users are not permitted to install their own software on any Company computer, mobile device, tablet, laptop or workstations, without prior approval from the Company. Failure to comply may result in users being held personally responsible for any data loss or penalties imposed for breach of copyright.

Installation or use of peer-to-peer file sharing programs by Users is not permitted on computers or devices connected to the Company network. Users shall not download or authorise downloading of information or software from the internet or emails to provide to a third party violate copyright, license agreements or contract of usage.

2.13 BYOD

The Company and its Partners allows users the privilege of using their own devices (BYOD) to access the computer network for their convenience. Use of any BYOD device is subject to the same conditions as defined in this policy whilst performing work for the Company, or Partner using the Companies network to access its services.

2.14 Monitoring

The Company reserves the right to regularly audit User activity and IT systems to ensure compliance with this and other Company policy. Our tools provide us with the information to monitor your physical location, however we only review this information when required to recover lost devices or investigate Information Security incidents. Access to Company IT systems is provided on condition that users consent to monitoring in accordance with Policy. Your use of Company IT systems constitutes your consent to the monitoring.

3. Compliance

3.1 General

All users of the Company's IT systems, services and equipment are required to read this policy and to agree that they have read, understood and are willing to abide by its contents. The method on how this agreement is presented and accepted is to be explicit.

3.2 Breaches

Any user that suspects conduct contrary to this Policy must report the conduct to appropriate Student contact points. Breaches of policy compliance may result in disciplinary action being taken.

3.3 Relevant Legislation

The Company is a global organisation with the responsibility to maintain compliance with the laws within our host nations. All Company users are responsible for aiding the Company in identifying relevant legislation and for complying with all relevant legislation.

4. Responsibilities

Each of the positions involved in implementing and achieving policy objectives and carrying out procedures are shown here.

Responsibility	CTO	Company IT Gov.	All Users	Company IT Leaders
Approver of Document	A			
Maintenance of Document		A		
Review of Document				C
Understanding of document			R	

R = Responsible, A = Approve, S = Supporting, C = Consulting, I = Informed.

5. Definitions

Unless the contrary intention is expressed in this Policy, the following words (when used in this policy) have the meaning set out below:

Term	Meaning
BYOD	Bring Your Own Device (abbreviation).
College	The legal entity at which the student is enrolled at.
Company	Means Navitas Limited and its affiliated group companies.
Partner	A Partner of the Company, e.g. a University, where Students may attend and access facilities owned and operated by a Partner.
Website (where relevant)	Means the Company's website where information is available to users, shareholders and other interested persons or organisations.

6. Review

This Policy is tested and reviewed and any changes to the regulatory compliance requirements, legislation, regulation and guidelines. This review process aims to ensure alignment to appropriate strategic direction and continued relevance to the Company's current and planned operations.

7. Records Management

All records in relation to this document will be managed as follows:

Record type	Owner	Location	Retention	Disposal
Policy	Chief Technology Officer	Electronic	Permanent	N/A