Group Acceptable Use Policy

LAST MODIFIED	01 February 2021
REVIEW DATE	01 February 2022
APPROVED BY	Group Chief Executive

1. Policy statement and application

a. This policy applies to all UP Education Limited and UP Education Australia Pty Ltd (together, "Group") employees, including fixed term, casual and permanent employees, including all individuals employed or engaged in the Group's various New Zealand and Australian entities.

b. The objective of this policy is to establish acceptable and unacceptable uses of IT Resources.

c. The Group provides access to, and use of, IT Resources provided you comply with the terms of this policy.

d. This policy is not incorporated as part of any award or enterprise agreement nor does it form any part of an employee's contract of employment.

e. The Group reserves the right to vary, replace or terminate this policy from time to time.

f. Failure to comply with this policy may lead to a suspension or withdrawal of access to IT Resources and disciplinary action being taken, which could include dismissal.

g. Where you are unsure of your obligations or feel a conflict may exist between the terms of this policy and your employment agreement or other Group policy you should seek advice from your manager or Group Human Resources.

2. Definitions

a. IT Resources – includes, but is not limited to, all systems and IT equipment (servers, Software, Cloud Services, collaboration platforms, mobile devices etc.), used to store, manage or transmit company information.

b. BYOD (Bring Your Own Device) – a Mobile Device owned by the User to access IT Resources.

c. Cloud Services – includes, but is not limited to, Software or services that are leased on a subscription basis.

d. Mobile Device – a device which may be able to communicate over the mobile data network or Wi-Fi networks (for example, mobile phones, iPads, Android tablets, mobile data cards) and provides communication and access to IT Resources. These may be Group owned or personally owned by the User (BYOD).

e. User Devices – includes any device accessing IT Resources (for example tablets, computers, Mobile Devices etc.).

f. Security Controls – safeguards or countermeasures to detect, counteract, or minimise security risks and ensure legal compliance to IT Resources. Includes, but is not limited to, technical controls such as passwords and administrative controls such as policies.

3. Access to IT Resources

a) Access to the IT Resources is controlled by the use of User IDs, passwords and two factor authentication. All User IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all actions associated with their IDs.

b) Password Complexity:

- Passwords must be at least 10 characters in length;
- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters; and
- Cannot be the same as previous passwords
- Must contain characters from three of the following four categories:

    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

c) Individuals must not:

- Allow anyone else to use their user ID/token and password;
- Leave their user accounts logged in at an unattended and unlocked computer;
- Use someone else's user ID and password to access Group businesses IT systems;
- Leave their password unprotected (for example writing it down);
- Perform any unauthorised changes to Group businesses IT systems or information;
- Attempt to access data that they are not authorised to use or access;
- Exceed the limits of their authorisation or specific business need to interrogate the system or data;
- Store Group data on any unauthorised equipment; or
- Give or transfer Group data or software to any person or organisation outside Group without authority.

4. Use of IT resources

a) IT resources are provided for business use and the delivery of our business services. You may use IT Resources for appropriate purposes related to your role.

b) Line managers must ensure that individuals are given appropriate training on the use of resources and provide clear direction on the extent and limits of their authority with regard to these resources.

c) You must store any content created in the appropriate repositories and not third-party sites (e.g. Dropbox) so that we can manage information security, storage costs, and provide optimal support.

d) You may also use IT Resources for purposes which do not relate to your role, including work on personal files, sending or receiving personal email, as long as the use is minimal. It would not be considered minimal use if it impacts on your ability to carry out your role satisfactorily.

e) Personal Use is a privilege not a right and may be withdrawn from any User who abuses it.

f) Individuals must not:

- Use IT resources to create, store, access, or copy information for the purposes of harassment or abuse;
- Use profanity, obscenities, or derogatory remarks in communications;

- Access, download, send or receive any data (including images), which the Group considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material;
- Place any information on the Internet that relates to the Group, alter any information about it, or express any opinion about the Group, unless they are specifically authorised to do this;
- Send unprotected sensitive or confidential information externally;
- Forward Group mail to personal (non-UP Education Group) email accounts;
- Download copyrighted material or breach licensing agreements;
- Download any software from the internet without prior approval of the IT team;
- Connect Group devices to the internet using non-standard connections;
- Use external media (such as USB sticks) to upload, download or transfer any information whether belonging to the Group or personal.
- Absolutely no sensitive data is to be copied to on external media; or
- Signup for cloud services without the prior agreement from the IT team.

5. Confidentiality

a) You must only access and keep confidential the information you have access to, in line with your employment contract or engagement.

b) You will return all confidential information in your possession on termination of employment or engagement.

6. Devices

a) All Group supplied equipment is provided for the purposes of carrying out your role and you are responsible for this device while it is in your possession. You must keep it secure and any loss or damage should be reported immediately to the IT Helpdesk.

b) You must not leave devices unattended in public places or visible in parked cars.

c) Access to IT resource from personal devices is provided and uses two-factor authentication as an added layer of security.

d) You must not store company information on personal devices.

7. BYOD (Bring Your Own Device)

a) At UP we allow employees to connect and use personal smartphones or tablets of their choice for work purposes and for their convenience.

b) Connectivity issues are supported by IT; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

c) Devices must be presented to IT when you decide to BYOD for proper provisioning and configuration of standard apps, (such as browsers, office productivity software and security tools) before they can access the network.

d) The employee's device may be remotely wiped by IT if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, virus or similar threat to the security of the company's data and technology infrastructure.

e) We reserve the right to revoke this privilege if users do not abide by this policy.

8. Mobile Phones

a) If your manager decides that you require a company mobile as part of your role, you will be provided with the standard company iPhone model and connected to the UP corporate mobile plan. Deviation from this will be at Executive level discretion.

b) There is no upgrade schedule for these devices, and it will only be replaced if we deem it no longer fit for purpose.

c) It is the employee's responsibility to take reasonable care to protect the device from damage. This should include protective cases. Repair required due to a lack of reasonable care will be the employee's responsibility.

d) You can also choose to purchase or bring your own device and connect to the UP corporate mobile plan if you prefer. In this instance please instead read the section on BYOD.

e) UP has a zero-tolerance policy for texting, calling or emailing while driving and only hands-free talking while driving is permitted.

f) If UP thinks your personal use is unreasonable, it may ask you to reduce your non-business use of your mobile.

g) If UP believes your device use is unacceptable, it may cancel your plan and ask for the return of the device.

h) International roaming can be expensive, and you will require your manager's permission to use your UP mobile outside New Zealand. It will only be granted if required for business reason. If we think your roaming costs are unreasonable, we may ask you to contribute to the cost of these charges.

i) UP reserves the right to request immediate return of an UP mobile phone at any point during your employment.

9. Security and compliance

a) All users have responsibilities to protect confidential information. Managers will communicate these responsibilities during induction.

b) You will receive regular security awareness updates which you need to take into consideration when carrying out your day-to-day activities.

c) 'Phishing' (pronounced Fishing) is the act of attempting to acquire information such as usernames, passwords and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy party via an email.

d) You must not respond to or click on any links in emails you receive from suspect sources requesting confidential details or personal information. If you suspect you have received a phishing email, please contact the IT Helpdesk.

e) We will regularly execute phishing campaigns and security training as part of our Security Awareness Program.

f) Note: The IT Helpdesk will never request confidential or personal information details via email.

10. Antivirus

a. Some material delivered by email may be deemed unsuitable or present a risk to the business. This can be due to attachments that contain trojans, worms, viruses or other malware, or due to emails containing spam or originating from known spam sites.

b. A system generated email will notify you of the barred message and the reason. If you require access to any business-related emails barred by the email filtering software, then please contact the IT Helpdesk

11. Monitoring and Filtering

a) All data that is created by or stored on Group IT Resources is the property of UP Education. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.

b) The Group has the right to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

c) The Group is not responsible for any loss you suffer if any of your personal files or personal email is lost.