A17 ActivateUTS IT Policy

Dates

Policy approved
Policy takes effect
Policy is due for review

Approved by

ActivateUTS Board of Directors Resolution

Implementation Officer

CEO ActivateUTS

Relevant to

All ActivateUTS Staff & affiliated Clubs & Societies & ActivateUTS Board

Related documents

ActivateUTS Risk Appetite Statement (RAS)
ActivateUTS Risk Register
ActivateUTS Risk Framework
ActivateUTS Risk & Audit Committee Terms of Reference
ActivateUTS Staff Handbook
Workplace Health and Safety Induction Forms

Review notes

01

Purpose

The purpose of this IT Policy and its associated procedures is to provide an approved practice for ActivateUTS staff using any IT systems and telecommunication devices controlled by ActivateUTS.

This policy applies to any computer or equivalent and telecommunications equipment owned by ActivateUTS and provided to staff for the execution of their duties and also applies to equipment not owned by ActivateUTS but used to access any systems and networks owned by ActivateUTS or UTS.

It establishes:

- Acceptable use of IT and Telecoms within ActivateUTS
- Procedures to safeguard data, both personal and commercially sensitive, ensuring compliance with relevant legislation

02

Scopes

2.1 Inclusions

This Policy applies to:

- all IT Equipment, Telecommunications and Systems owned and operated by ActivateUTS and UTS;
- all ActivateUTS and UTS Haberfield Club Ltd staff;
- all ActivateUTS Clubs and Societies.

03 Definitions

The following definitions apply for this Policy:

ActivateUTS Clubs and Societies means any affiliated club or society who is provided access to Google for Work to manage their activities.

Data means any information stored electronically either in a document, spreadsheet, and presentation or in a system.

G Drive is the location on the UTS network where all ActivateUTS files are stored

Google for Work is a cloud based system used by ActivateUTS to allow collaboration between departments using an online calendar to manage events and forms to collect data from surveys and online enquires through websites.

Google Drive is the location of files created using Google for Work. This is not on the UTS network.

IT and Telecommunications Equipment means any computer, tablet, mobile or fixed telephone

IT Systems means any system accessible using an electronic device including software, UTS network, the internet and email

Local Drive is commonly the C drive of a computer and is not accessible from the UTS Network

M Number is the staff number provided by UTS to allow access to the UTS Network and UTS email.

Non-staff member means any person who is not paid a salary or wages via the ActivateUTS Payroll.

Security means the safeguarding of any data held by ActivateUTS in any IT system to prevent its unauthorised access and distribution.

UTS Network means the computer network that is managed by UTS and access is granted through UTS IT Department using an M number

Virus means any piece of software, generally distributed through email or websites that damages the hardware, software or data on a computer

04 Policy Principles

The key principles stated below govern all ActivateUTS IT activities.

Principle 1

Security

Security of all systems and data is the paramount to the organisation and should be considered at all times when using any IT system.

Principle 2

Passwords

Passwords should remain secret and only used by one person. Passwords should never be shared.

Principle 3

Responsible Use of Systems

Anyone using any form of IT or Telecommunications Equipment must act responsibly at all times and not use them for illegal, offensive or inappropriate activities (as outlined in the ActivateUTS Staff Handbook).

Principle 4

Risk management

The risks associated with IT are to be managed in accordance with ActivateUTS' risk policy and procedures.

05 Policy statements

5.1 Appropriate Access to ActivateUTS Systems

Access to ActivateUTS IT systems is provided based on the requirements of the position held within the organisation. Access is granted to an individual and that person is responsible for ensuring that no one else uses their user name or password and they keep their password secret.

Training should be provided by the relevant manager on the systems as required, either through peer training or third party provider training. It is the responsibility of the manager providing access to ensure that the employee is appropriately trained and has signed the declaration accepting the conditions of this policy.

5.2 Data Storage

All data should be stored in the appropriate folder on the G Drive. Where a file contains sensitive personal data, it should password protected and only those requiring access to the file should have the password.

Any data collected via Google for Work must be moved from the Google Drive and stored in the appropriate location on the G Drive.

Data should not be stored on a local drive except in the event that the G Drive is unavailable. When the G Drive is restored, all data should be transferred to the appropriate folder on the G Drive.

5.3 Acceptable Usage

All staff who use any IT or Telecommunications equipment are granted access for the purpose of their role within ActivateUTS and UTS Haberfield Club Ltd.

Personal use of such equipment is a privilege and is subject to the following:

5.3.1 Personal use is limited to ensure that the work or the organisation is not affected;

5.3.2 When using the internet for personal use, inappropriate, offensive or illegal websites are not permitted and may be subject to disciplinary action;

5.3.3 When accessing personal emails via the internet, staff take the necessary precautions to ensure that no viruses are downloaded;

5.3.4 Personal use of UTS email is limited to ensure that the UTS email network is not overloaded.

5.4 Google for Work

Google for Work is used solely for the purpose of collaboration on events using the google calendar and for ActivateUTS Clubs and Societies.

Google for Work must not be used for any other activity and no data is to be stored on the Google Drive.

Where data is collected via a website using Google forms, access must be restricted to those staff who require access, links to the files must not be activated and as soon as the data is complete, it is moved to an appropriate location on the G Drive.

5.5 ActivateUTS Clubs and Societies

The incoming executive for ActivateUTS Clubs and Societies will be required to sign a declaration at the start of each calendar year confirming that they understand and agree to the conditions set below:

- Access to Google for Work is provided solely for the purpose of ActivateUTS Clubs and Societies Activities.
- Where data is collected via a website using Google forms, access must be restricted to those staff who require access, links to the files must not be activated and as soon as the data is complete, it is moved to an appropriate location on the G Drive.
- No data is to be stored that is illegal, offensive, malicious or inappropriate.
- The President of the Club or Society or their nominated delegate is responsible for ensuring that the data stored is secured and does not contain sensitive or personal information, including student numbers.
- No credit card or bank details are to be stored on Google Drive.

Failure to comply with these conditions will result in access being revoked and all data permanently deleted by ActivateUTS. Further disciplinary action may be taken by ActivateUTS against Clubs who do not comply with these conditions.

5.6 Credit Card Payments

It is acceptable to take credit card payments over the phone in certain situations, however the following procedure must be followed:

- Credit card numbers should never be written down or sent via email. If the transaction cannot be processed immediately, call the customer back.
- The card details should entered directly into the EFTPOS terminal or online payment terminal. A copy of the receipt may be sent via email as it doesn't contain the credit card number.
- Any forms sent to customers requesting payment must not include credit card details. There should be a section providing details of the payment methods available and clearly stating that credit card payments will be taken over the phone and that these should not be included on the form or sent via email.
- If credit card details are received via email, the email must be permanently deleted and the customer notified.

5.7 Distribution of data

Staff are expected to take all reasonable steps to ensure that the data held in ActivateUTS IT systems is secure. This includes not distributing data to third parties unless they are authorised to receive it.

All staff will sign a non-disclosure agreement at the commencement of their employment stating that they agree to maintain the security of data they have access to in the role and not to distribute it to anyone not authorised to receive it.

Failure to adhere to this may result in disciplinary action which can include dismissal.

5.8 Telephones

The Senior Management Team and certain managers throughout the organisation are provided with mobile telephones for business use. Personal use is acceptable but must be reasonable.

It is the responsibility of the individual to ensure that the mobile phone has a case to protect it from damage (this cost will be reimbursed) and that they are contactable during business hours. In some instances, out of hours contact is required and individuals are expected to answer such calls.

5.9 Using personal equipment

Where an individual uses their own equipment to access ActivateUTS IT systems, or their own mobile phone with a company funded sim card, all measures outlined in these policies will apply.

5.10 Disciplinary Action

Failure to comply with the policy statements set out above may lead to disciplinary action. Types of disciplinary action may include:

5.10.1 Counselling and/or user education;

5.10.2 Verbal or written warning;

5.10.3 Termination of employment;

5.10.4 Criminal or other legal proceedings in accordance with State and Federal legislation.

5.11 Relevant Legislation

In addition to the ActivateUTS policy statements set out above, the following legislation is applicable:

- Copyright Act 1968 (Cwlth) and the Copyright Amendment (Digital Agenda) ACT 2000 (Cwlth)
- Telecommunications Act 1997 (Cwlth) and associated Acts
- Crimes Act 1914 (Cwlth)
- Broadcasting Services Act 1992 (Cwlth) and associated Acts
- Privacy and Personal Information Protection Act 1998 (NSW)
- State Records Act 1998 (NSW)
- Crimes Act 1900 (NSW)
- State and federal anti-discrimination legislation
- Freedom of Information Act 1982 (Cwlth)