**ALTERNATIVE PROVISION**

# ICT Security Policy

Approval Date: January 2026

Revision Due Date: January 2027

Approved by: RAISE-AP Educational Directors

Approval Signatures

*RAISE-AP Directors*

## Table of Contents

## Introduction

ICT Systems at the provision are used to support learning and to enhance knowledge. Computer Networks and ICT Systems can be damaged by misuse, vandalism, hacking, virus attacks and several other means, both locally and via the Internet. This policy details the responsibilities of staff when using systems.

## Responsibility

This policy will be reviewed and monitored by the RAISE-AP Educational Directors.

## Scope

The deployment and use of the provision's ICT systems; all computers, peripheral equipment, software and data within provision property and located elsewhere. It includes connection to systems by RAISE-AP equipment and all use of the provision's computer networks, email facility, website(s), intranet, internet, and cloud use.

The security of hardware, software and data, the security of personnel using ICT systems, and the security of the provision's assets that may be placed at risk by misuse of ICT systems. In respect of copyright and data protection aspects, the policy covers the use of ICT systems not only owned by the provision or located on its property but also used by students or staff for study or business purposes connected with the provision.

## Statement

RAISE-AP seeks to protect its ICT assets and data from loss and to provide a secure working environment for its students and staff. The objectives of the Policy are to ensure as far as is reasonably possible that the provision's assets are secure against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence, and RAISE-AP is protected from damage or liability resulting from use of its facilities for purposes contrary to the law of the land.

## Key Principles

Ensure robust security is in place for ICT equipment and systems. It is the specific responsibility of the Head of Provision  to ensure that the Policy is carried out. All students, staff and visitors have a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the Policy.

---

## Procedures

**ACCEPTABLE USE**

All users must read, accept the terms, and sign the appropriate Acceptable Use Policy before being allowed to have a logon and password to the systems. Acceptable use is defined as use for the purposes of:

- Teaching and learning
- Research
- Personal educational development
- Administration and management of provision business
- Development work and communication associated with the above
- Consultancy work while contracted to the provision.
- Reasonable use of computer facilities for personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable at the discretion of the person's manager or tutor.
- Use for other purposes may be permitted by the RAISE-AP educational directors

Detailed lists of acceptable (and non-acceptable) use are available in the Acceptable Use Policies.

It is provision policy that there will be a Code of Good Conduct which will be reviewed regularly and circulated to all members of the provision. All users are expected to abide by the Code. It is provision policy that all use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people.

The Head of Provision has responsibility to take all reasonable steps to stop unacceptable use of ICT systems. The Head of Provision will be guided on policy issues by the RAISE-AP educational directors and advice from appropriate external bodies.

## REGISTERED USERS

The following are eligible to register as users and must complete the appropriate AUP if seeking to use ICT in scope of this policy:

- Any student currently registered on a course.
- Any person currently holding a contract of employment with the provision.
- Any person appointed as a Governor to the provision.
- Any person holding an honorary position recognised by the provision.
- Any person acting as a contractor/advisor to the provision.
- Any person of another educational establishment, teaching on the premises.

## OPERATIOAL PRACTICE

It is the responsibility of the RAISE-AP educational directors to attend to the following:

- Securing the integrity of data and software held and processed on the provision's information systems.
- Securing the integrity of data stored in cloud.
- Robust backup and restoration facilities of all central systems.
- Securing the integrity of all data storage areas, cloud storage, servers & computers.
- Ensuring file stores of servers & computers are secure and purged of inappropriate material, especially copyrighted material.
- In the event of a suspected security breach, enforcing appropriate restrictions to the service and user account until confidence is restored.
- Provision of appropriate antivirus, anti-spyware, anti-spam, anti-phishing, anti-malware, other security and protection tools on computer equipment under their control.
- Provision of effective controls on access to restricted facilities, such as business support data systems, cloud storage and shared storage areas.
- Provision of an appropriate software update system for servers and computers.
- Provision of a central firewall blocking facility for web access allowing the provision to restrict inappropriate use and specific facilities and websites.
- Provision of blocking inappropriate and potential security risk emails through appropriate monitoring systems.
- Provision of an encryption system to restrict access to data taken offsite.
- Provision of advice and guidance on Information and Data Security matters.
- Provision of a remote access system for approved use only.
- Any other security measures that may become necessary at any time.

It is the responsibility of the computer user to attend to the following:

- Taking appropriate security precautions in respect of computers under their control.
- Observing good practice recommendations for security in respect of facilities provided on computers and networks.
- Keeping their username and password secret.
- Using the appropriate encryption technique when sending data in external emails.
- Using the appropriate encryption technique when it is necessary to take data off site on laptops, USB drives and other portable disks or devices.
- Reporting breaches of security to the Head of Provision.
- Not connecting inappropriate equipment to the network.
- Only using college installed remote access software and in an approved manner.
- Use of provision approved cloud storage such as One drive for Business to store college related data.
- Damage to equipment, software or data resulting from failure to observe this policy is deemed to be the responsibility of the defaulter.
- Provision data should not be emailed/forwarded/saved to personal accounts.

## Artificial Intelligence

The use of Artificial Intelligence (AI) in the provision is guided by principles of ethical use, data privacy, and academic integrity. We are committed to using AI responsibly, ensuring it is used for educational enhancement, and not for plagiarism or other unethical activities.

We regularly review our AI usage and stay updated with the latest developments in AI technology to ensure our practices are current and in line with legal and ethical standards.

## Physical Security

All provision equipment will be secured against theft and damage to a level that is cost-effective. Users must not physically connect unauthorised non-provision equipment to the network.

Equipment loaned to staff must be kept in a secure environment when not in immediate use and they may be held responsible for any losses if considered irresponsible.

---

## Monitoring

RAISE-AP educational directors are responsible for ensuring that usage of resources will be logged in sufficient detail and at an appropriate level to identify defaulters where technically possible.

RAISE-AP educational directors will authorise ICT Services staff whose duties require them to monitor and police the use of computer facilities. Monitoring data will be collected only to assist investigation of a suspected security breach or other misuse, including activities covered by the PREVENT Strategy

ICT Services staff shall not monitor personal information except in specific instances where a suspected breach of security or other substantive offence requires it. Every such incident will be centrally recorded, and serious incidents will be reported to the Head of Provision. The central record will be made available for inspection by personnel authorised by the RAISE-AP educational directors.

The Head of Provision is empowered to authorise a hardware and/or software audit of provision equipment, where it is deemed necessary and to authorise removal of offending items. The provision may use services such as Dark Web monitoring to protect the provision and its users.

---

## Advice and Training

It is the responsibility of the Head of Provision to ensure that all users are made aware of the risks of security breaches and of their responsibility to take adequate precautions. This will be undertaken by:

- Giving appropriate security information during staff inductions.
- Publishing articles in staff updates.
- Publishing advice on the staff VLE.
- Email reminders.
- Any other method as deemed appropriate.

---

## Reporting

It is the duty of the Head of Provision to take appropriate action to prevent breaches of the policy.

All breaches should be reported to Head of Provision and RAISE-AP education directors.

## Raise Values

Our RAISE-AP values (Resolve, Attitude, Invest, Social Skills and Education) are key in everything we do, specifically with attitudes (modelling and expectations), invest (tailoring setup for our young people) social skills (becoming part of a community) which are linked to our ICT Security policy.