ALTERNATIVE PROVISION

ICT Acceptable Use 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

Users are expected to use all ICT equipment, Internet access and RAISE-AP data primarily for provision business and education related purposes. Users who are not staff or students at RAISE-AP are considered as a non-RAISE-AP user. As a non-RAISE-AP user, you are expected to conduct yourself honestly and appropriately when using ICT resources including data and the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others.

All existing RAISE-AP policies apply to the use by, and conduct of, visitors using ICT resources, data and the Internet, especially (but not exclusively) those policies that deal with intellectual property protection, privacy, misuse of RAISE-AP resources, safeguarding, sexual harassment, information and data security, general data protection regulation and confidentiality.

Responsibility

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

Scope

ICT equipment and associated technologies are used to support learning, RAISE-AP business and to enhance knowledge. Computer Networks allow access to the Internet, email, personal and shared folders, and allow people to interact with other computers and networks and with a multitude of electronic users.

The deployment and use of the RAISE-AP ICT systems; all computers, peripheral equipment, software and data within and between RAISE-AP property, or belonging to RAISE-AP but located elsewhere. It includes connection to external systems by RAISE-AP equipment and all use of the RAISE-AP 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 RAISE-AP 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 RAISE-AP or located on its property but also used by college students or staff for study or business purposes connected with RAISE-AP.

Statement

This policy is designed to help visitors, contractors, associates and non-employed educational and other user's, understand college wide expectations for the use of ICT resources, and sets out clear guidelines which must be adhered to. These users will be honorary members of staff with restricted facilities.

It is expected that as a general policy, all ICT equipment and computer networks will be used in a responsible, efficient, ethical and legal manner. This policy is designed to help visitors understand RAISE-AP wide expectations for the use of these resources and sets out clear guidelines which must be adhered to.

Key Principles

- All non-RAISE-AP user will be required to read and sign an ICT Acceptable Use Policy for Non- AISE-AP
- Staff form before being issued with a temporary computer account. This form will detail activities that are acceptable and not acceptable and additional general guidance information.
- Refusal to sign the form will result in denial of access to college systems.
- RAISE-AP has software and systems in place that can monitor and record all Internet usage and emails. The security systems are capable of recording (for each and every user) each web site visit, chat, newsgroup, e-mail message, and each file transfer into and out of RAISE-AP internal networks and cloud services.
- RAISE-AP reserves the right to use these systems where appropriate to monitor correct network, Internet and e-mail usage.

Procedures

UNACCEPTABLE USES OF ICT SERVICES

The following activities are examples of unacceptable uses of ICT Services:

- Using the Internet for any illegal purpose.
- Using the network/Internet for any activity promoting terrorism or radicalisation or any activity covered by the Counter Terrorism and Security Act (Prevent Act).
- Storing, sending or knowingly receiving any information that includes pornography, unethical or illegal solicitation, inappropriate language, and/or information used to promote racism or sexism.
- Sexually explicit material may not be displayed, archived, stored, distributed, edited or recorded using the RAISE-AP network or computing resources.
- Sending or knowingly receiving, storing or using copyrighted materials, videos and music without the owner's permission.

RAISE-AP: ICT Acceptable Use

- Distributing software or materials in violation of the General Data Protection Regulation or distribution licence.
- Installing or downloading illegal, pirated or unlicensed software.
- Using the network/Internet to deliberately propagate any virus, worm, Trojan horse, or malicious code.
- Using the network/Internet for financial gain or commercial activity.
- Violating any person's right to privacy.
- Using the network/Internet for product advertisement or political lobbying.
- Changing/deleting files which do not belong to the user.
- Using the network/Internet to make unauthorised entry into other computational, informational or communication services or resources (Hacking).
- Using another person's username and password or allowing someone else to use their password, without prior authorisation from RAISE-AP.
- Storage of non-college related data such as personal photos, music etc. on college equipment or college provided cloud storage.
- Installing or connecting unauthorised equipment to the college network for illegal purpose.
- Inappropriate use of your RAISE-AP identity on social networking sites.
- Physical damage to any ICT equipment or services
- Removal or relocation of any ICT equipment without appropriate permission.
- Copying staff or student's personal data and taking off site unless in an encrypted format or accessing such data from an external source including approved cloud storage.
- Bypassing the firewall using a proxy service.
- Accessing any RAISE-AP data without authorisation.
- Using data for any purpose other than that it was supplied for.

RESPONSIBILITY OF A USER

A responsible education user will:
- Be polite and never send or encourage others to send abusive messages.
- Use appropriate language and promote high standards in 'Netiquette'.
- Delete old messages and stored files on a regular basis. (Housekeeping of emails and files is very important so that the data storage areas are not clogged up with unwanted files and emails).
- Comply with the General Data Protection Regulation and Copyright legislation.
- Comply with the ICT Security Policy.
- Comply with BYOD Policy.
- Treat all ICT equipment with respect and keep it always secure.

THINGS TO CONSIDER

- Non-RAISE-AP User may use their Internet facilities for non-business research or browsing during breaks, or outside of work hours, provided that all usage policies are adhered to. RAISE-AP directors reserves a right to charge for the use of Internet and Email for personal use.
- Non-RAISE-AP Staff with Internet access may not use RAISE-AP Internet facilities to download and/or store music, entertainment software or games, or to play games against opponents over the Internet.
- User with Internet access may not upload any software licensed to RAISE-AP or data owned or licensed by RAISE-AP without explicit authorisation from the educational directors.
- Any software or files downloaded via the Internet into the RAISE-AP network will become the property of RAISE-AP. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. RAISE-AP reserves the right to inspect any files stored in private areas of the RAISE-AP network or on the RAISE-AP computers to assure compliance with RAISE-AP policy.
- RAISE-AP has software and systems in place that can monitor and record all network, Internet usage, emails, and cloud storage. RAISE-AP reserves the right to use these systems where appropriate to monitor correct Internet and e-mail usage and for the purposes of the PREVENT strategy.
- Ensuring any data accessed from non-RAISE-AP equipment both internally and externally is secured appropriately and not shared with any third party.
- RAISE-AP data should not be emailed/forwarded/saved to personal accounts.

PASSWORD RECOMMENDATIONS

- Your staff user account must use a complex password, it must be a minimum of 12 characters and contain at least 3 of the following 4 requirements: 1) An Uppercase Letter, 2) A Lowercase Letter, 3) A Number, 4) A Special Character (for example @, !, $, etc). NCSC (National Cyber Security Centre) suggests using three random words in mixed case separated with punctuation.
- Don't use a password that is the same or like one you use anywhere else.
- Make passwords hard to guess, even by those who know a lot about you, such as the names and birthdays of your friends and family, your favourite bands, and phrases you like to use.
- Do not reuse organisation password anywhere else. The use of organisation passwords in external websites greatly increases the likelihood that cybercriminals will compromise these passwords.
- If a password is suspected to be compromised, it should be changed immediately.
- Usernames, staff numbers, and passwords should be protected appropriately. If a password manager is used, the master password should be stored securely.

ARTIFICIAL INTELLIGENCE

The use of Artificial Intelligence (AI) in RAISE-AP 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.

Reporting

Any breach of the policy should be reported to the H RAISE-AP Educational 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 BYOD policy.

Appendix I

User Acceptance Form – Acknowledgment

I acknowledge that I have received this written copy of the Information Communications Technology Acceptable Use Policy for Non-RAISE-AP User. I understand the terms of this policy and agree to abide by them. I realise that RAISE-AP security software may record and store for management use the electronic e-mail messages I send and receive, the Internet address of any site that I visit, and any network activity in which I transmit or receive any kind of file.

I understand that any violation of this policy could lead to action being taken and possible criminal prosecution.

Signature ……………………………….... 	Name ………………………………...

(Capitals)

Date …………………………………. 	DoB ……………………………….

*DoB needed to generate initial password

RAISE-AP: ICT Acceptable Use