ICT ACCEPTABLE USE POLICY

Introduction

There needs to be commitment to protect College employees, students, academic partners, subcontractors and the wider Joint Academic Network (JANET) organisation from illegal or damaging action by individuals, either knowingly or unknowingly.

As a user of IT services of the College you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse the computing facilities in a way that constitutes a breach or disregard of the following policy you may also be in breach of other College policies.

The E-communication Policy and Social Media Policy governing the use of social networking sites and software should be read in conjunction with this ICT Acceptable Use Policy.

Ignorance of this policy (or those that it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Students and staff who connect their own devices to the College's network and the services available are particularly reminded that such use requires compliance to this policy.

Students are directed to this policy during their induction each year.

Staff are advised of this policy during their induction and of the College's requirement for them to adhere to the conditions therein.

1 Purpose

1.1 The purpose of this policy is to outline the acceptable and unacceptable use of computer equipment or "on-line services" owned by the College, and acceptable or unacceptable general behaviour in areas of the College where there is ICT equipment.

1.2 These rules are in place to protect the College employees and students. Inappropriate use exposes the College and academic partners to risks including virus attacks, compromise of network systems and services, and legal issues.

2 Scope

This policy applies to employees, Board of Governors, students, sub-contractors, consultants, temporary staff, and other workers at the College, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the College and to all equipment connected to the College's network. Use of College ICT equipment and the College network are limited to staff, students and authorised third parties only. Under no circumstances should any person not included in the above list be allowed to access to the College network.

2.1 Disciplinary Procedures

2.1.1 Staff or students who contravene this policy may find themselves subject to the College's disciplinary codes. The Head of Systems Development and Funding, as well as an individual's manager or the College Senior Management Team may take such disciplinary action.

2.1.2 Individuals may also be subject to criminal proceedings. The College reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

3 Definitions

3.1 For the purposes of this policy the term "computing services" refers to any IT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including wired and wireless access to the Internet).

3.2 The term "on-line services" includes services provisioned and accessible (both wired and wireless) through individual accounts and passwords. Such services would include access to internet/intranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP and are the property of the College. These systems are to be used for educational purposes in serving the interests of the organisation, and of our staff and students in the course of normal operations.

3.3 The term "devices" includes but is not restricted to: laptops, tablets and smart phones.

3.3 Definitions of Unacceptable Usage

Unacceptable use of College computers and network resources may be summarised as, but not restricted to:

Use of the lT facilities

- Actions which cause physical damage to any ICT hardware, including peripherals (e.g., mouse, cables, wiring, printers);
- Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate, including pornographic imagery or content;
- Threatening, bullying, intimidating or harassing staff, students or others;
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
- Defamation;
- Unsolicited advertising often referred to as "spamming";
- Sending emails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address;
- Attempts to use the ICT facilities for the purposes of bribery;
- Attempts to break into or damage computer systems or data held thereon;
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, e.g. use of equipment which is inadequately protected against viruses and spyware;

- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;
- Using the College network for unauthenticated access;
- Unauthorised resale of College, or JANET services or information;
- Using the ICT facilities for gambling;
- Using the ICT facilities for carrying out any illegal trading activity;
- Using the ICT facilities for carrying out any terrorist research or activity and;
- Any other conduct which may discredit or harm the College, its staff or the ICT facilities.

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy:

- The use of peer-to-peer and related applications within the College;
- Interfering with data or settings in another person's network account;
- Users must not deliberately visit, view, download, print, copy, forward, share or otherwise transmit any unlawful material or that which is likely to cause offence;
- The downloading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder;
- The distribution or storage by any means of pirated software;
- Circumvention of network access control;
- Monitoring or interception of network traffic, without permission;
- Probing for the security weaknesses of systems by methods such as port-scanning, without permission;
- Associating any device to network Access Points, including wireless, to which you are not authorised;
- Non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of ICT services or which incur financial costs;
- Excessive use of resources such as filestore, leading to a denial of service to others, especially when compounded by not responding to requests for action;
- The use of College mailing lists for non-academic purposes; and;
- The use of portable media for the purpose of copying unlicensed copyright software, music, etc.

If you mistakenly access such material you should notify ICT Services. You should be aware that you will be held responsible for any claims brought against the College.

In the event of any use that could be regarded as giving rise to criminal proceedings the College may inform the police or other law enforcement agency. Other uses may be unacceptable in certain circumstances.

4 Key Principles

4.1 Authorisation

In order to use the ICT facilities of the College a person must first be properly registered to use such services. Registration to use College services implies, and is conditional upon acceptance of this Acceptable Use Policy as part of the College regulations, for which a signature or electronic acknowledgement of acceptance is required on joining the College. The lack of a signature does not exempt an individual from any obligation under this policy. The continuing use of the ICT facilities will be deemed to be acceptance by the user of the terms of this policy.

The registration procedure grants authorisation to use the core ICT facilities of the College. Following registration, a username and password will be allocated to each individual user. Authorisation for other services may be requested by application via the College's ICT Helpdesk.

Any attempt to access, use or interfere with any user account or email address for which the user is not authorised, is prohibited and will be regarded as a disciplinary offence.

No one may use, or attempt to use, ICT resources allocated to another person, except when explicitly authorised.

A user must take all reasonable precautions to protect the College's resources (including the ICT facilities and the College's information and data), their username and passwords.

4.2 Purpose of Use

ICT facilities are provided primarily to facilitate a person's essential work as an employee or student or other role within the College. Use for other purposes, such as personal email or recreational use of the Internet, is a privilege which can be withdrawn at any time and without notice. Any such use must not interfere with the user's duties or studies or any other person's use of computer systems and must not, in any way, bring the College into disrepute.

College email addresses and associated College email systems must be used for all official College business, in order to support audit purposes and institutional record keeping. All staff and students of the College must regularly read their College email and delete unwanted or unnecessary emails at regular intervals.

Staff use of social networking sites during working hours (breaks excepted), other than for:

- the support of, or communication with, students,
- maintaining legitimate business contacts,

is not permitted.

Staff ICT accounts have been allocated for use by the member of staff in connection with their job requirements. Student ICT accounts have been allocated for exclusive use by the student in connection with their education whilst at the College.

Commercial work for outside bodies involving the use of ICT systems requires explicit permission from the Head of Systems Development and Funding and the Deputy Principal, Finance and Resources; such use may be liable to charge.

The College recognises that individuals may conduct personal use of email and the Internet. However this must be kept to a reasonable level and must be legal. The College reserves the right to revoke such permission if, in the judgement of the College, these facilities are abused.

4.3 Privacy and Monitoring

All allocated usernames, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other

person. Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.

The College reserves the right for appropriately authorised staff to examine any data including personal data held on College systems or, when operationally necessary, for example to give access to a private account to a line manager or colleague. Certain staff within the College have been authorised to examine files, emails and data within individual accounts, but will only do so when operationally necessary.

It is also occasionally necessary to intercept network traffic. In such circumstances appropriately authorised persons will take all reasonable steps to ensure the privacy of service users. Logs will be kept of usage of IT equipment; this will include dates and times when accounts were accessed.

The College reserves the right to monitor email, telephone and any other electronically mediated communications, whether stored or in transit, in line with the Regulation of Investigatory Powers Act (2000) and other relevant law.

Reasons for such monitoring include the need to:

- Establish the existence of facts (e.g. to provide evidence of commercial transactions in cases of disputes);
- Investigate or detect unauthorised use of the College's telecommunications systems and ensure compliance with this policy or other College policies;
- Ensure operational effectiveness of services (e.g. to detect viruses or other threats to the systems);
- Prevent a breach of the law or investigate a suspected breach of the law, the College's policies and contracts; and;
- Monitor standards and ensure effective quality control.

When a student or member of staff leaves the College (either on completion of course or termination of employment, files left on any computer system owned by the College, including email files, may be removed. The College is under no obligation to recover any data once a person has left the College. Before leaving the College, staff should make arrangements to transfer to colleagues any relevant email or other computer-based information held under their personal account.

When a member of staff is away it may be necessary for appropriately authorised members of staff to access the absent member of staff's email account to deal with matters in their absence. This should be borne in mind when using the ICT facilities for personal reasons. Users should consider adopting appropriate markers for personal and private emails.

For operational reasons and for the continuing delivery of services, the College has the right to access the account of a staff member after that person leaves.

Users of ICT facilities should be aware that the College conducts random monitoring of communications, regardless of whether the use is business or personal.

Where abuse is suspected (especially criminal activity and/or gross misconduct), the College may conduct a more detailed investigation involving further monitoring and examination of stored data (including employee-deleted data) held on servers/disks/drives or other historical/archived data.

Where disclosure of information is requested by the police (or another law enforcement authority) the request where possible will be handled by the College's Data Protection Officer or other appropriate senior person.

The College is committed to achieving an environment which provides equality of opportunity, and freedom from discrimination. Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene College codes on harassment. No carrying out of unauthorised surveillance, audio and/or visual, of a student, staff or member of the public on Riverside College premises is permitted.

No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.

All users will abide by laws relating to the use and protection of copyright.

Users of services external to the College are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. The use of College credentials to gain unauthorised access to the facilities of any other organisation is similarly prohibited.

4.4 Copyright Compliance

All users must not download, copy or otherwise re-produce material for which they have not obtained permission from the relevant copyright owner. If such material is required for any purpose e.g. teaching or research then copyright permission must be obtained and documented before such material is used.

All users are reminded that the College treats plagiarism very seriously and will investigate any allegation i.e. the intentional use of other people's material without attribution.

5 Responsibilities

5.1 The Data Protection Officer is responsible for ensuring that issues around data protection and copyright compliance are monitored.

5.2 All College Managers are responsible for the implementation and monitoring of the policy.

5.3 All persons as defined in Section 2 have a responsibility to comply with this policy.

5.4 The responsibility for the supervision of the Acceptable Use Policy is delegated to ICT Services by the College SMT. Any suspected breach of this policy should be reported to a member of ICT Services staff. A responsible senior member will then take the appropriate action within the College's disciplinary framework, in conjunction with other relevant branches of the College ICT Services staff will also take action when infringements are detected in the course of their normal duties. Actions will include, where relevant, immediate removal from online information systems of material that is believed to infringe the law. The College reserves the right to audit

and/or suspend without notice any account pending any enquiry. Where necessary, this will include the right to intercept communications.

5.5 This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered here at present. In the first instance students should address questions concerning what is acceptable to their student adviser. Staff should approach their line manager. Where there is any doubt the matter should be raised with ICT Services Helpdesk, whose staff will ensure that all questions are dealt with at the appropriate level within the College.

6 Linked Policies/Related Documents

Information Security Policy

ICT Acceptable Use Policy

Safeguarding policies and procedures: Protecting Children, Young People, Adults at Risk and Staff

Data Protection and Document Retention Policy and Guidelines

Staff Disciplinary Procedure

Student Disciplinary Policy

Guidance for Safer Working Practices

Bring your own device (BYOD) Policy

E-Communication and Social Media Policy
Bring your own device (BYOD) Policy

Anti-Bribery Policy

7 Relevant Legislation

Copyright, Designs and Patents Act 1988
Malicious Communications Act 1988
Computer Misuse Act 1990
Criminal Justice and Public Order Act 1994
Trade Marks Act 1994
Data Protection Act 2018
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Communications Act 2003
Bribery Act 2010
UK-GDPR

Summary of Policy for Students

You must not:

- Allow other people to use your account.
- Download or access illegal software onto a workstation.

- Download or copy any software packages from the College network onto portable media, etc.
- Upload your own personal software packages onto a College workstation.
- Access offensive or abusive material.
- Send abusive or inappropriate e-mails/messages.
- Access "inappropriate" websites – some Internet pages are illegal and may be subject to criminal proceedings. The College is committed to meeting the duties cited within the Anti-Terrorism Prevent agenda which means filters on websites that may contain messages of hate, radicalisation, extremism and terrorism are in place and set to high
- Interfere with other users' work.
- Photograph or record members of staff or students without their permission, using devices such as mobile phones, cameras or digital recorders.
- Use software designed to unblock sites.
- Use online gambling sites.
- Use peer-to-peer and related applications anywhere on College premises. These include, but are not limited to, Ares, BitTorrent, Direct Connect,
- Abuse equipment.

Please remember, when in teaching and learning areas such as the LRC, IT Suite or classrooms:

- Keep noise to a minimum to avoid disrupting others.
- Copyright regulations apply to electronic sources - please check before you printout from online services.
- No unauthorised use of chatlines.
- Logout or lock your computer when leaving a computer, even for a short time.
- Be able to show a certificate showing that any portable electrical device (such as your personal laptop/power supply etc.) has been electrically tested, before using it on College premises.

Anyone found abusing the College policy on the use of computers may have their network rights removed, and may be subject to further disciplinary action.

College computers are provided primarily for college work. However, you may use the equipment for personal use providing:

- You do not breach the acceptable use policy.
- You are not doing so for gambling purposes.

If you use the College equipment for personal use you should note the following:

- Conducting any financial transaction on shared equipment carries a very high risk. Your personal data may not be safe.
- If you are using communal ICT facilities (such as the library), you may be asked to log-off where the demand for the equipment is high.
- This AUP policy applies to both wired and wireless access and use of network on your own devices or on college equipment.
- In order to use the ICT facilities of the College a person must first be properly registered to use such services.
- Registration to use College services implies, and is conditional upon acceptance of this Acceptable Use Policy as part of the College regulations, for which a signature or electronic acknowledgement of acceptance is required on joining the College.

- The lack of a signature does not exempt an individual from any obligation under this policy.
- The continuing use of the ICT facilities will be deemed to be acceptance by the user of the terms of this policy.

Summary of Policy for Staff

You must not:

- Allow other people to use your account.
- Download or access illegal software onto a workstation.
- Download or copy any software packages from the College network onto portable media, etc.
- Upload your own personal software packages onto a College workstation.
- Access offensive or abusive material.
- Send offensive, abusive or inappropriate e-mails/messages.
- Access "inappropriate" websites – some Internet pages are illegal and may be subject to criminal proceedings.
- Interfere with other users' work.
- Photograph or record members of staff or students without their permission, using devices such as mobile phones, cameras or digital recorders.
- Use software designed to unblock sites.
- Use online gambling sites.
- Use peer-to-peer and related applications anywhere on College premises.
- Abuse equipment.

Please remember:

- Copyright regulations apply to electronic sources - please check before you make content available to your students via Moodle or any other internet source.
- You should reset your password at regular intervals and ensure that it is a strong password.
- You must logout from or lock access when leaving a computer, even for a short time.
- You must be able to show a certificate showing that any portable electrical device (such as your personal laptop/power supply etc.) has been electrically tested, before using it on College premises.

Anyone found abusing the College policy on the use of computers may be subject to disciplinary action.

College computers are provided primarily for College work. However, you may use the equipment for personal use providing:

- You do not access social networking sites during working hours (breaks excepted) other than for:
- the support of, or communication with, students as properly authorised and agreed
- maintaining legitimate business contacts.
- You do not breach the acceptable use policy.
- You are not doing so for gambling purposes.

If you use the College equipment for personal use you should note the following:

- Conducting any financial transaction on shared equipment carries a very high risk. Your personal data may not be safe.
- This AUP policy applies to both wired and wireless access and use of network on your own devices or on college equipment.

- In order to use the ICT facilities of the College a person must first be properly registered to use such services.
- Registration to use College services implies, and is conditional upon acceptance of this Acceptable Use Policy as part of the College regulations, for which a signature or electronic acknowledgement of acceptance is required on joining the College.
- The lack of a signature does not exempt an individual from any obligation under this policy.
- The continuing use of the ICT facilities will be deemed to be acceptance by the user of the terms of this policy.