CRONTON SIXTHFORM COLLEGE

Riverside College
Widnes & Runcorn

ICT ACCEPTABLE USE POLICY

Introduction

There needs to be a 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. The **Bring Your Own Device (BYOD) Policy** should also be read in conjunction with this ICT Acceptable Use Policy.

Ignorance of this policy (or those 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** 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 "online 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 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.
- All personnel affiliated with third parties using equipment owned or leased by the College.
- Any equipment connected to the College's network.

Key Conditions:

- Use of College ICT equipment and networks is limited to staff, students, and authorised third parties only.
- Under no circumstances should anyone outside these groups be granted access to the College network.

2.1 Disciplinary Procedures

2.1.1 **Consequences for Staff and Students**

Staff or students who contravene this policy may be subject to the College's disciplinary codes. Actions may be taken by the Head of Systems Development and Funding, an individual's manager, or the Senior Management Team.

2.1.2 **Criminal Proceedings**

Individuals may also face criminal proceedings. The College reserves the right to pursue legal action against individuals causing legal complications due to violations of licensing agreements or other contraventions of this policy.

3. Definitions

3.1 Computing Services

Refers to any IT resource made available to you, including:

- Network-borne services.
- Applications or software products provided to you.
- Infrastructure for accessing services (wired or wireless, including Internet access).

3.2 Online Services

Refers to services provisioned through accounts and passwords, including:

- Internet/intranet systems.
- Computer equipment and software.
- Network accounts, such as email, internet browsing, and FTP.

3.3 Devices

Includes, but is not limited to: laptops, tablets, and smartphones.

3.4 AI Usage Guidelines

3.4.1 Acceptable Use

- AI tools may enhance learning, productivity, and creativity when used in compliance with academic integrity, copyright laws, and data protection regulations.
- Clearly attribute AI-supported content in assignments, presentations, or publications.
- AI may be used for administrative purposes if explicitly authorised by the College.

3.4.2 Unacceptable Use

- Using AI for generating assignments, essays, or other work without proper attribution (plagiarism).
- Inputting confidential, personal, or sensitive data into AI systems without authorisation.
- Creating or distributing offensive, misleading, fraudulent, or harmful content via AI tools.

3.4.3 General Responsibilities

- Exercise critical judgment when using AI tools and verify the accuracy of generated content.
- Report any harmful or inappropriate use of AI tools to ICT Services.

3.4.4 Monitoring AI Usage

The College reserves the right to monitor AI-related activities on its network to ensure compliance with this policy.

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 implies acceptance of this Acceptable Use Policy as part of the College regulations.

Key guidelines include:

- A username and password will be allocated to each user after registration.
- Attempts to access, use, or interfere with unauthorised user accounts are prohibited.
- Users must take precautions to protect College resources, their username, and passwords.

4.2 Purpose of Use

ICT facilities are provided primarily to facilitate work or education. Use for personal purposes is a privilege and may be withdrawn if abused.

Key conditions:

- College email addresses must be used for all official business.
- Social networking during working hours (breaks excepted) is not permitted unless for legitimate educational or business purposes.
- Commercial use of ICT facilities requires explicit permission and may be chargeable.

5. Responsibilities

5.1 Data Protection Officer

Responsible for ensuring compliance with data protection and copyright laws.

5.2 College Managers

Responsible for implementing and monitoring this policy.

5.3 ICT Services

Responsible for investigating breaches and enforcing compliance.

6. Linked Policies/Related Documents

- Information Security Policy
- Bring Your Own Device (BYOD) Policy
- Safeguarding Policies and Procedures
- Data Protection and Document Retention Policy
- E-Communication and Social Media Policy
- Anti-Bribery Policy

7. Relevant Legislation

Includes but is not limited to:

- Data Protection Act 2018
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990

- 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 personal software packages onto a College workstation.
- Access offensive or abusive material.
- Send abusive or inappropriate emails/messages.
- Access "inappropriate" websites (some Internet pages are illegal and may be subject to criminal proceedings).
- Interfere with other users' work.
- Photograph or record 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 on College premises.
- Abuse ICT equipment.

Additional Guidelines for Students:

- Maintain quiet and avoid disruptions in shared ICT areas like the LRC, IT Suite, or classrooms.
- Follow copyright regulations when printing or sharing materials from online sources.
- Always log out or lock your computer when stepping away.
- Ensure any personal electrical device brought to College has a valid electrical safety certificate.

Summary of Policy for Staff

You must not:

- Allow other people to use your account.
- Download or access illegal software onto a workstation.
- Upload your personal software packages onto a College workstation.
- Access offensive or abusive material.
- Send offensive or inappropriate emails/messages.
- Interfere with other users' work.
- Photograph or record staff or students without their permission.
- Use software designed to unblock sites.
- Use online gambling sites.
- Abuse ICT equipment.

Additional Guidelines for Staff:

- Follow copyright regulations when sharing content via Moodle or other online platforms.
- Regularly update and use strong passwords for security.
- Always log out or lock your computer when leaving it unattended.
- Ensure any personal electrical devices brought to the College meet safety standards.

General Notes for Staff and Students:

- College computers are primarily for College-related work. Personal use is allowed only under the following conditions:
  - It does not breach the acceptable use policy.
  - It is not for gambling purposes.
- Conducting financial transactions on shared College equipment is highly discouraged due to potential security risks.
- The policy applies to both wired and wireless access on personal or College devices.