Commonwealth College of Excellence

Information Technology (IT) Policy

Version	Date	Changes	Reason for Changes	Author/ Reviewer	Next Review
v3.1	January 2025	-	A new policy has been adopted.	Mohammad T Islam (Head of Academics & Quality Control)	January 2026/ As required
v3.2	November 2025	Section 14: Acceptable Use Guidelines (AUG) is added.	To define and formalise acceptable digital behaviour, ensuring responsible IT use and compliance with legal, security, and academic standards.	Mohammad T Islam (Head of Academics & Quality Control)	January 2026/ As required

1.0 Introduction

This Information Technology (IT) Policy sets out the standards, expectations, and procedures governing the use of IT systems, services, and infrastructure at the Commonwealth College of Excellence (CCE).
It aligns with UK Higher Education legislation and regulatory frameworks including:

- the General Data Protection Regulation (UK GDPR),
- Freedom of Speech obligations,
- Prevent Duty under the Counter-Terrorism and Security Act 2015, and
- the Computer Misuse Act 1990.

The policy applies to all users of CCE's IT resources, including staff, students, contractors, and visitors.

2.0 IT Services and Support

CCE maintains an IT department responsible for managing, supporting, and maintaining the IT infrastructure.
The IT Manager oversees daily operations and compliance, reporting risks (including Prevent-related concerns) to the Designated Safeguarding Lead (DSL).
Support is prioritised to ensure academic continuity, security, and institutional integrity.

3.0 Network and System Security

All devices connecting to the College network must have authorised security software.
The College enforces compliance with the Computer Misuse Act 1990, UK GDPR, and other applicable laws.
Breaches can result in disciplinary or legal action.

4.0 Software and Licensing

All software installations on CCE-owned devices must be approved and conducted by the IT department.
Software piracy or unauthorised installation is strictly prohibited.

5.0 Equipment Procurement

IT equipment is procured centrally under a rolling renewal policy.
All equipment must meet College specifications for security, functionality, and compatibility.

6.0 Network Infrastructure

The College’s network is managed exclusively by the IT department.
Tampering with network infrastructure is prohibited and may result in disciplinary measures.

7.0 Email and Internet Use

CCE email accounts are issued upon HR confirmation for staff.
Students also receive CCE emails after confirmation from the Admissions and Enrolment team.

Internet usage is monitored, and prohibited behaviours include accessing extremist content, harassment, copyright violation, and distribution of offensive material.
Staff and students must comply with the Acceptable Use Guidelines (AUG) specified in this policy.

8.0 Email Good Practice

Email is an official medium of communication.
Users must treat emails as formal documents.
Misuse (e.g., inappropriate content, excessive file distribution, data breaches) may result in sanctions.

9.0 Social Media Use

Official College social media accounts must have a named administrator.
Content must comply with College standards, copyright law, and data protection requirements.
Unauthorised disclosures or impersonation are prohibited.

10.0 Website Management

The College website is managed by the IT Manager in consultation with content owners.
All content must be accurate, accessible, and legally compliant, including in relation to data privacy and consumer protection in HE.

11.0 Wireless (WiFi) Access

CCE provides secure WiFi for academic and administrative use.
Use of this service constitutes agreement with the Acceptable Use Guideline.

12.0 Mobile Devices

College-owned mobile devices are issued for work-related use only and must comply with IT security configurations and monitoring protocols.

13.0 Sensitive and Extremist Research

CCE prohibits engagement in or support of extremist content or research.
Research involving sensitive topics must undergo ethical review and meet legal and regulatory standards.

14.0 Acceptable Use Guidelines (AUG)

All users of College IT resources must:

- Use systems lawfully and ethically.
- Not access, transmit, or store offensive, defamatory, or extremist material.
- Not use peer-to-peer or unauthorised file-sharing programs.
- Respect copyright, intellectual property, and licensing agreements.
- Protect login credentials and report suspected breaches.
- Avoid mass emailing without authorisation.

Breaches of the AUG may result in suspension of access and/or disciplinary action.

15.0 Policy Governance and Review

This policy is reviewed annually or following significant changes in legislation, guidance, or institutional structure.

The End