Engineering College of Technology.

DIGITAL TEACHING AND IT ACCEPTABLE USE POLICY

Contents

1. Purpose 3
2. Scope 3
3. Legislative and regulatory alignment 3
4. IT & the Prevent duty — operational requirements 4
5. Implementation 4
6. Roles and responsibilities 5
7. Management responsibility 6
8. Ethical considerations and academic freedom 6
9. Definitions 6
10. Student-facing terms (for VLE/handbook) 6
11. Enforcement, reporting and sanctions 7
12. Related policies and documents 7
13. Good-practice sources reflected in this policy 8

1. Purpose

1.1 This policy sets requirements and guidance for teachers, academic and professional services staff, managers, and system administrators on the ethical and acceptable use of ECT's digital systems and online learning platforms. It embeds ECT's duties under the Counter-Terrorism and Security Act 2015 (the Prevent duty) and sector good practice for distance and blended delivery, while protecting freedom of speech and academic freedom within the law.

1.2 It also introduces student-facing terms (Section 9) for use on the VLE and in induction materials, so that staff and students share the same expectations.

2. Scope

2.1 This policy applies to:

- All ECT staff (including visiting lecturers, hourly-paid tutors, contractors and placement supervisors) when using ECT systems or external platforms for ECT purposes.
- System administrators and managers with elevated access to ECT systems and data.
- All teaching and learning activities delivered via the VLE, e-mail, Teams/Zoom, e-assessment systems, remote labs/cyber ranges, discussion forums and third-party platforms used for ECT teaching.
- Bring-Your-Own-Device (BYOD) access to ECT services.

3. Legislative and regulatory alignment

3.1 This policy operates alongside and supports compliance with:

- Counter-Terrorism and Security Act 2015 (Prevent duty)
- Prevent duty guidance for England and Wales (latest)
- Office for Students (OfS) Prevent monitoring framework and ADR (accountability and data return) guidance
- UK GDPR and Data Protection Act 2018
- Equality Act 2010
- Consumer protection and competition law guidance for HE providers
- Terrorism Act 2000 and relevant criminal law

3.2 ECT recognises its statutory duty to have due regard to the need to prevent people from being drawn into terrorism. This policy is implemented in adherence to ECT's Prevent Duty Policy and associated safeguarding procedures.

4. IT & the Prevent duty — operational requirements

4.1 To meet Prevent expectations proportionately in a higher-education context, ECT will:

a. Filtering and/or monitoring: Consider and implement proportionate web filtering and/or monitoring to safeguard users. Decisions, configurations and exemptions are risk-based, documented and reviewed at least annually.
b. Sensitive/extremism-related research: Provide a simple approval route for legitimate research/teaching that requires access to extremist material (see Access is facilitated through controlled means (e.g., whitelisting, offline copies) with supervisor sign-off and activity logging.
c. Transparent notice: Publish clear information for users about what is monitored, why, legal bases, data retention and rights.
d. Incident escalation: Route potential Prevent-related concerns to the Prevent Lead and record/report in line with OfS expectations.

5. Implementation

Privacy & monitoring transparency

5.1 ECT uses proportionate filtering/monitoring to safeguard users and comply with its legal duties. We will:

- Tell users clearly what may be monitored and why;
- Access logs only where necessary for safeguarding, security or alleged policy breaches;
- Retain data for defined periods and review controls annually;
- Offer contact points for questions or concerns.

Sensitive/extremism-related research approvals

5.2 Where teaching or research requires access to extremist content, staff must:

- complete the Sensitive Research Access form (short form), and obtain module leader/supervisor approval;
- use the approved access method (e.g., whitelisting, offline copy);
- ensure activity logging is enabled and stored securely;
- provide student guidance within the module on lawful, safe access to such materials;
- seek advice from the Prevent Lead where needed.

Online events & external speakers (virtual delivery)

5.3 When ECT platforms are used for online events with external speakers or public audiences, organisers must:

- complete a proportional risk assessment;
- ensure moderation is in place (including chat/Q&A);
- keep chat/Q&A logs where lawful and necessary;
- apply the Student-facing Terms (Section 9) to participants;
- escalate concerns to the Prevent Lead.

Recording of live teaching and meetings

5.4 Recording by students is only permitted (a) as a reasonable adjustment, or (b) with explicit staff approval for a specific justification.

- Staff may stop recording at any time if conditions are breached.
- Unauthorised recording or sharing of recordings is a disciplinary matter.

6. Roles and responsibilities

6.1 All staff (including teachers):

- Model and enforce the Student-facing Terms in online spaces.
- Signpost students to welfare/Prevent contacts and use the “Report” mechanisms where concerns arise.
- Use the Sensitive Research Access route where needed and brief students accordingly.

System administrators

- Implement and maintain approved filtering/monitoring controls.
- Maintain controlled access (allow/deny lists) for sensitive research; manage accounts and backups.
- Promptly escalate Prevent-related alerts and maintain incident records.

Prevent Lead (Head of Academics and Operations)

- Chair triage for flagged content and online-event risks;
- oversee ADR data/returns as required; ensure annual review of IT controls and user notices
- Maintain links with safeguarding/HR and provide staff updates/training.

Managers/Module leaders

- Approve sensitive research access and risk assessments for online events.
- Ensure modules display student-facing notices and etiquette;
- Complete mandatory Prevent training.

7. Management responsibility

7.1 Decisions on access permissions and network use are overseen by management, with careful vetting of individuals holding delegation rights.

7.2 Managers must ensure administrators have the competence and resources to discharge these duties and that activity aligns with this policy.

8. Ethical considerations and academic freedom

8.1 Monitoring and moderation will be necessary and proportionate and must not unlawfully restrict freedom of speech or academic freedom. Legitimate academic inquiry including critical engagement with controversial or extremist material should be facilitated. Confidential information encountered in administrative duties must not be acted upon or disclosed except through authorised incident procedures.

9. Definitions

VLE: The virtual learning environment and integrated tools used for teaching, assessment and community interaction.
Sensitive/extremism-related research: Legitimate teaching or research that requires access to extremist materials.
Online event: Any ECT activity with external speakers or public components delivered via online platforms.
BYOD: Personally owned devices used to access ECT services; use requires authentication so activity is attributable to individuals.

10. Student-facing terms (for VLE/handbook)

10.1 Using ECT systems online:

- Keep it respectful and lawful; do not promote or support terrorism/extremism (unless expressly authorised for approved study).
- Use only your own account; protect your login; enable multi-factor authentication where offered.
- Follow forum and class etiquette; no harassment, hate speech or intimidation.
- Record live sessions only where permitted (reasonable adjustment or explicit approval) and never share recordings without permission.
- For sensitive/extremism-related study, get approval first.
- Worried about someone or something you've seen? Tell us via Report-and-Support/Prevent Lead (Head of Academics and Operations).

10.2 These terms reflect sector practice used by UK distance-learning universities and specialist IT training providers.

11. Enforcement, reporting and sanctions

Moderation and removals

11.1 ECT may hide, delete, block or quarantine posts, files or messages that threaten network security or breach conduct rules. Staff may remove participants from sessions where necessary.

Disciplinary responses

11.2 Breaches of this policy by students may be treated as misconduct under student disciplinary regulations and may lead to sanctions including warnings, access restrictions or further action. Staff breaches will be managed under HR policies and may lead to disciplinary action.

11.3 File sharing by students is a breach of copyright law and ECT's intellectual property rights. As a result, the following disciplinary actions will be taken against any student, including ECT graduates, who have been found engaging in file sharing activities.

	Frequency of offence:	**Disciplinary action typically resulting in:**
ECT students	First time offence	Educative response (reprimand, repeat the assessment, resubmission, alternate assessment, failure of unit/module etc.)
	Repeated offence	Suspension of up to a year or termination of enrolment (based on severity)
ECT graduates	First time offence	Written warning
	Repeated offence	Revocation of qualification

Reporting and ADR support

11.3 Suspected Prevent-related serious incidents are escalated to the Prevent Lead (Head of Academics and Operations). Records will support any OfS Prevent ADR (accountability and data return) requirements for the relevant academic year.

12. Related policies and documents

12.1 Prevent Duty Policy; Safeguarding Policy; Freedom of Speech & Academic Freedom Policy; Student Disciplinary Regulations; Data Protection Policy; Records Management Policy; Cyber Security Standards; External Speakers and Events Policy.

13. Good-practice sources reflected in this policy

Office for Students: Web filtering and monitoring – technical guidance note (2017).
Office for Students: Prevent monitoring – ADR guidance (most recent notice).
Office for Students: How we monitor (Prevent monitoring framework).
Home Office: Prevent duty guidance (England and Wales).
University of London: VLE Code of Conduct; Acceptable Use Policy (ISP-002).
The Open University: Prevent Principles; Code of Practice for Student Discipline.

Document Control		
Document title		Digital Teaching and IT Acceptable Use Policy
Version no.		1
Date Approved		21 November 2025
Approving Body		Governance Board
Policy Custodian		Head of Academics and Operations
Policy Contact		Compliance and Risk Manager
Commencement Date		November 2025
Review Period		Annually
Next Review Date		November 2026
Related documents		See 12.1
Revision History		
Version	**Date**	**Description of key changes**