WEST THAMES COLLEGE

E-Safety and IT Acceptable Usage Policy

Lead	Approved By:	Date Approved:	Next Review Date:	Where Published:
Amine Lallali	Lindsey Stewart Interim Executive Director	25 June 2025	25th June 2026	Staff Intranet/

E-Safety and IT Acceptable Usage Policy

1. Purpose and Scope

This policy outlines the acceptable use of IT resources at West Thames College, ensuring a safe, secure, and productive digital environment for staff, students, and authorised visitors. It addresses the effective use of technology while mitigating risks related to e-safety and cybersecurity. The College recognises the powerful potential of digital learning technologies to enhance skills and promote achievement while being aware of the associated risks.

2. General Principles

The College is committed to:

- Promoting safe and responsible use of technology.
- Enhancing learning experiences through digital tools.
- Safeguarding users against risks such as cyberbullying, grooming, and radicalisation.
- Complying with relevant laws, including GDPR (2018), Prevent Duty, and the Computer Misuse Act (1990).
- Implementing e-Safety measures to satisfy our duty of care.

This policy applies to all students, staff, visitors, and contractors who access the College's IT services, whether through College-provided equipment or BYOD (Bring Your Own Device).

3. Key Policy Updates

A. Password and Authentication Management

- Encourage passphrase-based passwords (e.g., "SummerBreeze2025!").
- Require Multi-Factor Authentication (MFA) for accessing sensitive college systems.
- Discourage routine password changes unless prompted by security concerns.
- Mandate secure storage and non-sharing of IT credentials.

B. Incident Reporting

- All incidents (e.g., breaches, lost/stolen equipment, unauthorised access) must be reported immediately via:
  - IT Service Desk: ITHelpdesk@west-thames.ac.uk
  - Online Incident Reporting Form https://ishelpdesk.west-thames.ac.uk/
  - Phone: **020 8326 2326**.
- Reports will remain confidential and handled per GDPR guidelines.

C. BYOD and Personal Device Use

- Personal devices must:
    - Use college-provided wi-fi network.
    - Adhere to the same security and acceptable use standards as college-owned devices.
    - Be registered with IT Services if accessing college networks regularly.

- Users are responsible for ensuring their devices run up-to-date operating systems and software.

4. Acceptable Use Guidelines

Unacceptable Usage: The following activities are prohibited:

- Accessing or sharing illegal, harmful, or inappropriate material.
- Bypassing college security measures (e.g., VPNs, proxies).
- Engaging in cyberbullying, harassment, or discrimination.
- Unauthorised sharing of sensitive or personal information.
- Using college systems for personal financial gain or unrelated business activities.
- Accessing the "Dark Web" or using anonymising tools without explicit permission.
- Wasting staff effort or resources through unnecessary IT tasks.
- Violating intellectual property laws (e.g., pirating software, music, or videos).

Professional Communication

- All student-staff communication must occur via college-approved platforms (e.g., Microsoft Teams, Email).
- Personal social media or messaging apps must not be used for official communication.

5. Training and Awareness

- **Regular Training:** Staff and students must complete e-safety training annually, including simulated phishing campaigns to improve cybersecurity awareness.

- **Resources:** Training materials include:
    - Data Protection
    - Cyber security

6. Cybersecurity and Safeguarding

Prevent Duty Compliance

The College will:

- Monitor internet activity to identify and address risks of radicalisation.
- Provide training on identifying extremist content and behaviours.

Incident Escalation

- Escalate significant breaches to senior management and external authorities (if necessary).
- Notify affected users promptly in case of data breaches.

7. Monitoring and Compliance

- IT activity is subject to monitoring to ensure compliance with this policy.
- Breaches may result in disciplinary action under staff or student codes of conduct.

8. Policy Review

This policy will be reviewed annually. Feedback from users is encouraged to improve clarity and effectiveness. Submit suggestions via [feedback portal link].

Policy Review Information

- **Last Reviewed**: June 2025
- **Review Period**: Annually
- **Next Review Due**: June 2026
- **Policy Owner**: Head of IT Services
- **Approval Authority**: College Governance Board
- **Contact for Queries**: IT Services ITHelpdesk@west-thames.ac.uk