icecampus

March 2025

IT Policy

v1.1

Table of Contents

1. Purpose 2

2. Scope 2

3. Acceptable Use 2

4. Data Protection and Confidentiality 3

5. Cybersecurity 3

6. Remote Work and Device Security 4

7. Use of Email and Communication Tools 4

8. Intellectual Property and Lecture Recording 4

9. Monitoring and Enforcement 5

10. Review and Updates 5

1. Purpose

The purpose of this IT Policy is to ensure the responsible, secure, and efficient use of all ICE Campus information systems, infrastructure, software, and digital assets. The policy provides staff with clear expectations and requirements relating to technology access, data handling, cybersecurity, and digital conduct. This policy forms part of ICE Campus's overall commitment to operational integrity, data protection, and compliance with applicable laws, including the EU General Data Protection Regulation (GDPR).

2. Scope

This policy applies to:

- All ICE Campus personnel with access to institutional IT systems or data
- All institutional devices (desktops, laptops, tablets, mobile phones)
- All use of ICE Campus email, learning management system (LMS), storage, and communications platforms
- Personal devices used to access ICE systems or data under BYOD agreements

This policy covers both physical and cloud-based infrastructure, on-premise and remote work settings.

3. Acceptable Use

All users of ICE Campus IT systems must:

- Use institutional tools (email, LMS, cloud drives, CRM) only for authorised work-related activities
- Keep login credentials secure, and never share access with others
- Avoid storing, accessing, or distributing inappropriate, offensive, or illegal content
- Ensure that all communications conducted via institutional systems are professional and respectful
- Refrain from using ICE systems for unauthorised personal business, social media promotions, or political activity

4. Data Protection and Confidentiality

ICE Campus is committed to full compliance with EU GDPR and equivalent data privacy regulations.

All staff must:

- Access and process personal data (e.g. student records, staff files) only when necessary for work duties
- Store sensitive data only in approved platforms or encrypted formats
- Not transfer ICE data to personal devices or private storage systems without express permission
- Report any suspected data breach immediately to the designated Data Protection Officer or line manager

Training on data protection responsibilities is mandatory for all staff and will be refreshed periodically.

5. Cybersecurity

To mitigate cybersecurity risks, all staff must:

- Use strong, unique passwords for all ICE systems and update them regularly
- Ensure institutional and personal devices used for ICE work have updated anti-virus and firewall protection
- Avoid clicking on suspicious links, attachments, or unknown software downloads
- Log out of shared systems or devices when not in use
- Report phishing attempts, suspicious system activity, or potential breaches without delay

ICE Campus reserves the right to audit system use and perform vulnerability testing on institutional infrastructure.

6. Remote Work and Device Security

For remote or hybrid work arrangements:

- Work must be performed in a secure and quiet environment
- All devices used for work (institutional or personal) must be protected by passwords, screen locks, and antivirus tools
- Staff must use ICE-approved communication platforms only
- Sensitive materials must not be printed, shared over public Wi-Fi, or left unattended

7. Use of Email and Communication Tools

All institutional communication tools are to be used professionally and ethically:

- Emails should be courteous, relevant, and aligned with institutional tone and guidelines
- Mass or marketing emails require prior approval from management
- Staff may not use ICE emails or platforms to promote personal businesses or solicitations

8. Intellectual Property and Lecture Recording

Content created using ICE systems or during working hours — including slides, assessments, lecture recordings — remains the intellectual property of ICE Campus unless otherwise agreed in writing.

Staff must:

- Only record sessions when instructed or approved
- Not use recorded materials for personal or external use without authorisation
- Ensure student privacy is respected during any recordings

9. Monitoring and Enforcement

ICE Campus reserves the right to monitor the use of its IT systems where necessary for:

- Investigating policy violations
- Ensuring operational continuity and security
- Complying with legal and regulatory requirements

Non-compliance with this policy may result in disciplinary action, including suspension of IT access or formal sanctions in line with the Disciplinary Policy.

10. Review and Updates

This policy is reviewed annually or when significant changes to IT infrastructure, cybersecurity standards, or legal obligations occur. Staff will be notified of major updates and are responsible for familiarising themselves with the latest version.