INTERNATIONAL EUROPEAN UNIVERSITY

IT POLICY FOR INTERNATIONAL EUROPEAN UNIVERSITY

Approved by the Academic Council
of International European University
29.08. ___, 2024 (protocol No. 1)

Chair of the Academic Council
of International European University
________ Oleh PADALKA
29.08. ____, 2024

ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ «МІЖНАРОДНИЙ ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ» Ідентифікаційний код 42947833 УКРАЇНА * м. КИЇВ *

Became effective by Order
dd. 29.08.2024 No. 60-OD

Kyiv – 2024

CONTENT

I. GENERAL PROVISIONS

All users of computing, networking, and IT facilities at International European University (IEU), including students, teaching and non-teaching staff, management, visiting guests, and research fellows, are expected to adhere to the following guidelines. These rules are in place to maintain the efficient and secure operation of IT systems while safeguarding the privacy and work of the university community.

Authorized Use: Students, faculty, staff, management, guests, and research fellows are authorized to use the university's computing, networking, and IT facilities for academic, administrative, and personal purposes, provided such use complies with all relevant laws and university policies.

Unauthorized Access: The university strictly prohibits any attempt to gain unauthorized access to restricted IT resources. Any such activity is considered a violation of both university policy and applicable national and international laws, including GDPR and European cyber security regulations, potentially leading to civil or criminal liability. The university reserves the right to monitor and analyze IT resources for compliance with institutional and legal requirements.

Inappropriate Content: Users are prohibited from sending, viewing, or downloading fraudulent, harassing, obscene (e.g., pornographic), threatening, or otherwise inappropriate material that violates any law or university policy. Caution is advised when interacting with email or online content that may be questionable in nature. Any actions that disrupt the academic or work environment are strictly prohibited.

Copyright and Licensing: All users must respect intellectual property rights, copyright laws, and software licensing agreements. Engaging in illegal file-sharing or using unauthorized, pirated, or unlicensed software on university IT systems (including personal devices used within the university network) is a violation of this policy.

Open Source Software: The university encourages the use of open-source operating systems (e.g., Ubuntu, CentOS) and processing software (e.g., LibreOffice, OpenOffice). Users, particularly those using university-sponsored devices, are expected to transition to these recommended platforms unless they receive approval for an exemption due to technical limitations.

Privacy and Data Security: Users are expected to adhere to data privacy regulations, including the GDPR. Accessing or sharing unauthorized information without proper consent is strictly prohibited. All users are responsible for safeguarding personal and institutional data and following best practices for online privacy and security.

Data Integrity: Users must not engage in any actions that intentionally or accidentally damage or alter data. The integrity of information must be maintained by all users, and any disruption of the university's IT systems is a serious violation.

Availability of IT Resources: Users are not permitted to engage in activities that might affect the availability or performance of IT resources, whether intentionally or accidentally.

Departmental Policies: Individual departments, dormitories, or units may establish additional guidelines for IT resource usage, provided they are in line with this university-wide policy. Such guidelines should be publicized and enforced at the local level. Any use of external networks must also comply with university IT policies.

Third-Party Access: In certain circumstances, such as legal investigations, the university may be required to provide IT information or resources to external parties. Additionally, for purposes of monitoring and optimizing the use of IT resources, the university may audit or review IT usage without prior notice to users. The university may also engage third-party service providers to perform these tasks.

Equipment Care: Users are responsible for the proper care of university IT equipment. Any malfunctions should be reported immediately to the responsible staff or the facility supervisor. Users should not attempt to repair, move, or modify equipment or connect unauthorized devices without permission.

Laboratory Etiquette: No food or drinks are allowed in computer laboratories. Users are expected to maintain a quiet environment, refraining from disruptive activities such as playing games or music loudly, watching movies, or talking loudly.

Policy Violations: Any violation of this policy may result in disciplinary action, which could range from warnings to more severe consequences depending on the nature of the offense. University authorities will determine the appropriate response based on the severity of the violation.

Policy Updates: This policy may be updated as necessary. Any changes will take effect immediately and will be communicated via email, posted notices, or other means.

II. EMAIL ACCOUNT USE POLICY OF INTERNATIONAL EUROPEAN UNIVERSITY

In order to improve the effective distribution of important information to faculty, staff, students, and administrators, International European University encourages the use of its official email services for formal communication, academic activities, and other official purposes.

All students and staff of the university have their own official email addresses and Google Workspace for Education for academic-related work. Students are to abide with the Google Workspace Acceptable Use Policy when using any Google Workspace for Education service.

The use of email for formal communications ensures the timely delivery of messages and documents to the university community, including faculty, staff, students, and external stakeholders. Official communications may include administrative updates, human resources notifications, policy changes, university-wide announcements, and other important messages.

To ensure you receive these important communications, it is essential to keep your email account active by logging in and using it regularly. Faculty and staff can access their email by using their designated User ID and password. To request a university email account, individuals should contact the HR department by submitting a formal application in the required format.

By utilizing the university's email system, users agree to the following terms:

The email system should primarily be used for academic and official purposes, with limited use for personal communications.

Using the email facility for illegal or commercial purposes is strictly prohibited and constitutes a violation of the university's IT policy. Illegal activities include, but are not limited to, unauthorized distribution of software, sending unsolicited bulk emails (spam), and generating threatening, harassing, abusive, obscene, or fraudulent messages or content.

When sending large attachments, users must ensure the recipient's email system can accommodate such files.

Users are responsible for managing their mailbox and ensuring it stays below 80% capacity. A full mailbox may result in emails bouncing back, particularly if they contain large attachments.

Users should avoid opening emails or attachments from unknown or suspicious sources. Even emails from known contacts should be treated with caution if they include suspicious attachments. In such cases, users should confirm the authenticity of the email with the sender before opening it, to prevent the risk of viruses or malware.

Users are encouraged to configure their email software to periodically download messages to their computer, freeing up server space. It is the user's responsibility to back up both incoming and outgoing emails.

Email accounts should not be shared with others. Account holders are personally responsible for any misuse of their email account.

Attempting to access or intercept another user's email is a violation of their privacy and is strictly prohibited.

When using shared computers, users should immediately log out of any email account that was left open by a previous user, without viewing its contents.

Impersonating another user by accessing their email account is considered a serious breach of the university's IT security policy and will result in disciplinary action.

It is ultimately each individual's responsibility to keep their e-mail account free from violations of the university's email usage policy.

III SOCIAL MEDIA POLICY OF INTERNATIONAL EUROPEAN UNIVERSITY

This policy provides guidance on the appropriate use of social media by employees. For the purposes of this policy, social media includes, but is not limited to, platforms such as WhatsApp, online forums, message boards, chat rooms, electronic newsletters, social networking sites, and other services where users can share information publicly.

The following principles apply to both professional use of social media on behalf of International European University (IEU) and personal use when referencing the university.

Employees must be aware of and follow these guidelines when engaging in social media activities that reference or reflect upon the university.

Employees should understand that their actions on social media can affect their personal reputation and the public image of International European University. Content shared or posted online may remain accessible to the public for an extended period.

The university may review content shared by employees on social media. Therefore, employees are expected to use good judgment when posting any material and ensure that it does not reflect poorly on IEU, its employees, or stakeholders.

While not exhaustive, some prohibited behaviors on social media include posting content, commentary, or images that are defamatory, harassing, pornographic, proprietary, or libelous, or that could create a hostile work environment or offend religious or cultural sentiments.

Employees are prohibited from sharing or publishing confidential information or any material not intended for public release. If there are any uncertainties about what constitutes confidential information, employees should consult with the Human Resources Department.

Social media interactions may sometimes attract media or legal attention. Employees should direct all press or legal inquiries to the designated university spokesperson.

If an employee encounters a potentially antagonistic or escalating situation on social media, they should politely disengage and seek advice from the Human Resources Department.

Employees must obtain appropriate permission before referencing or sharing images of current or former employees, students, members, vendors, or suppliers. Additionally, employees should ensure they have the legal right to use third-party content, including copyrighted materials, trademarks, or other intellectual property.

Social media use must not interfere with employees' responsibilities at the university. The university’s computer systems are intended for business purposes only. Use of social media for professional purposes is permitted only for those whose roles require it (e.g., managing the university's Facebook, Twitter, LinkedIn, or blogs). Personal use of social media on university systems is discouraged and may result in disciplinary action.

Employees should not use any type of offensive /abusive language or make any comment/post any photo which is not in line with their image as a member of the academic community.

IV. RULES FOR THE USAGE OF INTERNATIONAL EUROPEAN UNIVERSITY (IEU) COMPUTER LABS

Access to computer labs is limited to authorized students, faculty, and staff of the university. Visitors may use the facilities only with prior permission from the lab supervisor.

Users must present valid university identification upon request.

Computer labs are open during the designated hours as determined by the university. Users are required to vacate the labs at closing time unless special arrangements have been made.

Extended hours may be available during exam periods; any changes will be communicated in advance.

The lab's computers and equipment should be used solely for academic and research purposes. Personal use is allowed only to the extent that it does not interfere with academic activities.

Users are prohibited from tampering with, modifying, or moving any hardware or software configurations.

Installing unauthorized software, games, or other programs is strictly forbidden.

The university's internet connection must be used responsibly and in accordance with the IEU IT policy. Users should refrain from visiting inappropriate, illegal, or non-academic websites.

Downloading or sharing copyrighted material without proper authorization is prohibited.

Use of peer-to-peer (P2P) file-sharing applications is not allowed unless specifically required for academic purposes.

Silence must be maintained in the computer labs to create a conducive learning environment. Mobile phones should be set to silent mode, and phone conversations are not allowed.

Eating, drinking, or bringing food and beverages into the labs is strictly prohibited.

Respectful and professional behavior is expected from all users. Any form of harassment or inappropriate conduct will not be tolerated.

Users are responsible for backing up their own data. Files saved on lab computers are not guaranteed to be secure or retained after logout.

Users must log off their accounts after using the computers to protect their personal data and prevent unauthorized access.

Users should not monopolize lab resources. Computers should not be reserved or left unattended for extended periods.

When demand is high, users are encouraged to limit their sessions to reasonable timeframes to allow others access to the resources.

Printing services are available in the computer labs but should be used responsibly. Academic-related printing takes priority.

Large print jobs or unnecessary printing is discouraged to minimize waste and environmental impact.

Any malfunctioning equipment or technical issues should be reported immediately to the lab staff or IT support.

Users should not attempt to repair or fix any computer problems themselves.

Violations of these rules may result in suspension of computer lab privileges. Depending on the severity of the violation, disciplinary action may be taken by university authorities.

Serious offenses, such as damage to equipment or misuse of university resources, may result in legal action.

Users are expected to comply with all university policies, including the IT policy, email use policy, and code of conduct, while using the computer labs.

The university reserves the right to amend or update these rules as necessary. Any changes will be communicated to users via email or posted notices.

Although the IT Department at International European University strives to provide efficient and reliable services, it cannot be held responsible for data loss or any related liabilities resulting from issues within the IT infrastructure.

Users are strongly encouraged to maintain independent backups of any data stored in their user accounts, utilizing personal storage devices such as USB drives, external hard drives, DVDs, or other media.

The IT Department also reserves the right to temporarily or permanently suspend access to any or all IT services, for any reason deemed necessary.