2024

Policy and Procedure

European College of Polytechnics

EUROPEAN
COLLEGE OF
POLYTECHNICS

SKILL FOR PURPOSEFUL LIFE

Contents

European College of Polytechnics

IT policy

I. Scope

(1) The European College of Polytechnics recognises its computing resources as essential assets for educational and administrative functions. This IT policy outlines the expectations for all staff and students when using these resources. It encompasses all hardware, software, network access, and electronic communications managed by the college. Adherence to this policy is essential to maintaining the integrity and security of these systems. Each member of the community is entrusted to use these resources responsibly and exclusively for professional and academic activities, ensuring a collaborative and secure technological environment.

II. Hardware Use Guidelines

Authorisation Procedures

(2) Movement, connection to the network, or modifications of hardware devices must receive approval from the administrator. This protocol ensures network security and system integrity.

Care and Maintenance

(3) All electronic equipment must be handled with care. Any damage, malfunction, or loss should be promptly reported to the administrator. Regular maintenance checks are recommended to ensure optimal performance.

Security Compliance

(4) Portable devices, such as laptops, must be secured when off-campus to protect against data theft and hardware loss.

III. Software Management

System Configuration

(5) Initial setups and configurations are handled by the systems administrator to ensure consistency across the network. Unauthorised changes are not permitted.

Access Control

(6) Access to applications and data should align with individual role requirements. Unauthorised exploration of the network is not permitted and could impact system security.

Installation and Licensing

(7) Installation of any software, from applications to screensavers, requires prior approval from the systems administrator. Compliance with licensing laws is mandatory, ensuring all software is authorised and legally compliant.

IV. Email Usage and Security

Usage Expectations

(8) The primary aim of college email should be for professional communication. Personal communications using ECP's email should be restricted and carried out during personal time using personal channels. Upon joining the European College of Polytechnics (ECP), each employee may be assigned an official ECP email address. This email account serves as the primary communication method within the institution and is essential for accessing various institutional resources, receiving internal communications, and managing day-to-day administrative tasks

Monitoring and Privacy

(9) The college has right to monitor and access email and network systems when necessary for operational reasons. Monitoring is conducted respectfully and minimally intrusively.

Email Attachments and Safety

(10) Email attachments should only be opened from known and trusted sources. Suspect emails should be forwarded to the systems administrator for verification.

Password Security

(11) Passwords are critical for protecting identity and access within the system. Keeping them secret and secure is imperative to prevent unauthorised access. Individuals are accountable for any activity conducted under their credentials. Regularly updating passwords and ensuring their complexity is strongly supported.

V. Internet Use

Purpose and Restrictions

(12) Internet access is provided primarily for educational and administrative functions. The use of this resource should be prudent. Accessing non-business-related sites, especially inappropriate ones, is strictly prohibited and could result in serious consequences.

VI. Access to Learning Management Systems

(13) ECP utilises two main learning management systems (LMS): Canvas and eSkooly. These platforms are crucial for academic management, course delivery, and resource sharing. Login details for both Canvas and eSkooly are provided to each new employee by the IT department during the initial setup phase. Familiarity with these systems is

important, as they are regularly used to access teaching materials, submit academic content, and collaborate with students and colleagues. To ensure all staff are proficient in using the provided technological tools and understand the institutional policies related to their roles, ECP mandates attendance at specific training sessions for all newly hired employees. These sessions cover a range of topics, including effective use of the LMS platforms (Canvas and eSkooly), best practices for digital communication and data management using the ECP email system, overview of other institutional technologies and resources that are vital to daily operations. The training is designed to equip new staff with the necessary skills and knowledge to perform their roles effectively. It also provides an opportunity to ask questions and interact with various departmental leads, which can be invaluable for building internal relationships and understanding the institution's operational ethos. Employees are expected to complete these training sessions shortly after their induction. Department heads or responsible authority communicates details regarding the schedule and format of the training. Attendance is not only a requirement but also a beneficial part of the onboarding process, ensuring that staff members are well-prepared to start their journey at ECP successfully.

(14) Upon enrolment in the course, students will gain access to a comprehensive suite of study resources through the Learning Management Systems, specifically Canvas and eSkooly. After successful enrolment, students will receive an email invitation to register on these platforms. They must follow the instructions to set up their accounts, which typically involves creating a username and password. Once the account setup is complete, students can log in to access all necessary course materials, including textbooks, articles, video tutorials, and additional learning aids, regularly updated with the latest information relevant to the course modules. A mandatory induction session is designed to familiarise students with the LMS interface, course layout, and available resources. Details about the induction, including its date and time, will be communicated shortly after account activation. The purpose of this induction is to ensure that students understand how to navigate the LMS effectively and utilise the provided resources to maximise their learning experience. Should students encounter any technical issues with the LMS, support is available through the helpdesk feature on the platforms or directly from the IT support team. For academic inquiries related to course content or study resources, students can contact their instructors via the LMS messaging system or participate in scheduled Q&A sessions.

VII. Data Handling

Protection of Sensitive Information

(15) Extreme caution is required when handling or transporting sensitive data on portable storage devices. The security of intellectual property is a shared responsibility.

Data Storage and Clean-up

(16) Regular review and clean-up of storage areas are necessary to prevent unnecessary data accumulation, optimise system performance, and ensure data privacy.

VIII. Adherence to IT Policy

Prohibited Activities

(17) Engaging with offensive content, disseminating unauthorised materials, or misusing the IT environment is unacceptable and will be addressed with the utmost seriousness.

Enforcement and Monitoring

(18) Continuous monitoring helps maintain system security and operational integrity. Cooperation in following these guidelines is essential and highly valued.

IX. Communication Standards

Email Correspondence

(19) A professional tone in all email communications is encouraged, reflecting the decorum expected in the academic and professional community. Ensuring confidentiality and precision in communications reflects well on the entire institution.

X. Monitoring and Reviewing

(20) This policy is subject to periodic review and may be amended to reflect changes in legislation or best practices. This policy must be read in conjunction with all other relevant policies of ECP and its LMS partner organisations.