International Balkan University (IBU)
Fair Use Policy (FUP)

The Fair Use Policy (AUP) outlines the appropriate use of the university’s IT resources, including, but not limited to, computers, networks, internet services, email systems, and software. This policy ensures that all users act responsibly, ethically, and in compliance with applicable laws and university regulations while using these resources.

This policy applies to all users of the university’s IT resources, including students, faculty, staff, contractors, and visitors. It covers the use of all university-owned devices, networks, accounts, and personal devices connected to the university network.

1. General Principles

- **Responsible Use**: All IT resources support the university’s academic, research, and administrative activities. Users are expected to use these resources responsibly and for legitimate university-related purposes.
- **Legal and Ethical Behavior**: Users must comply with all applicable laws, regulations, and university policies when using IT resources. This includes respecting intellectual property rights, protecting the privacy of others, and refraining from any behavior that is illegal, unethical, or harmful to the university.

2. Authorized Use

- **Access Rights**: Access to the university’s IT resources is a privilege granted to authorized users. Users must only access systems and data that they are authorized to use. Unauthorized access, including hacking or attempting to bypass security measures, is strictly prohibited.
- **Account Security**: Users are responsible for the security of their accounts. Login credentials (e.g., usernames, passwords, PINs) must not be shared with others. Users should take precautions to protect their accounts, including using strong passwords and enabling multi-factor authentication (MFA) where available.

3. Use of Network and Internet Resources

- **Academic and Administrative Use**: The university’s network and internet resources support educational, research, and administrative activities. Personal Internet use should be limited and not interfere with academic or administrative priorities.
- **Content Restrictions**: The university reserves the right to restrict access to certain websites or content deemed inappropriate or non-academic. This includes, but is not limited to, websites related to pornography, illegal file sharing, and other content that violates university policies.
- **Bandwidth Usage**: The IT department monitors network traffic to ensure equitable access for all users. Excessive bandwidth usage that negatively impacts the network may result in restrictions or service throttling.

4. Prohibited Activities

- **Illegal Activities**: Users are prohibited from engaging in unlawful activities using university IT resources. These include, but are not limited to, copyright infringement, distributing or accessing illegal content, and unauthorized access to systems or data.

- **Harassment and Discrimination**: Using IT resources to harass, discriminate against, or bully others is strictly prohibited. This includes sending threatening, obscene, or offensive messages via email, social media, or other electronic communications.
- **Security Violations**: Users must not attempt to compromise the security of IT resources, including spreading malware, phishing, or engaging in activities that disrupt the university's IT infrastructure.
- **Unauthorized Software**: Installing or using unauthorized software on university devices or networks is prohibited. Users must not download or use software that could harm the university's IT environment or violate licensing agreements.

5. Email and Communication Systems

- **University Email**: The university provides email accounts for official communications. Users are expected to use their university email for academic and administrative purposes. Personal use of university email accounts should be minimal and must not violate university policies.
- **Spam and Mass Emails**: Users are prohibited from sending unsolicited mass emails, spam, or chain messages using university systems. Email communication should be professional and per the university's communication guidelines.

6. **Data Privacy and Protection**

- **Confidential Data**: Users who handle confidential or sensitive data (e.g., student records and financial information) must take appropriate measures to protect it. This includes using secure systems, encrypting data, and following the university's Data Protection Policy.
- **Data Sharing**: Users must not share university data with unauthorized individuals or third parties. Data sharing should be conducted through approved channels and under university policies and applicable laws, such as GDPR or HIPAA.

7. Personal Devices and BYOD

- **BYOD Policy**: Users who connect personal devices to the university's network must comply with the university's BYOD (Bring Your Own Device) policy. Personal devices must meet the university's security standards, including using up-to-date antivirus software and secure login credentials.
- **Personal Data**: The university is not responsible for the security or privacy of personal data stored on devices connected to the university's network. Users are encouraged to back up their data and avoid storing sensitive personal information on university systems.

8. Monitoring and Enforcement

- **Network Monitoring**: The university reserves the right to monitor network traffic, email communications, and other activities on its IT systems to ensure compliance with this policy. Monitoring is conducted under applicable laws and university regulations.

- **Policy Violations**: Violations of this policy may result in disciplinary action, including but not limited to loss of access to IT resources, suspension, or termination of employment or enrollment. Severe violations like illegal activities may be reported to law enforcement authorities.

9. Reporting Security Incidents

- **Incident Reporting**: Users must report any security incidents, such as unauthorized access, data breaches, or suspicious activity, to the IT department immediately. Prompt reporting helps protect the university’s IT resources and minimize damage.

10. Policy Review and Updates

- The IT department will review this policy regularly and update it as necessary to reflect changes in technology, legal requirements, or university operations. Users will be notified of any significant changes to the policy.