NETWORK SECURITY AND PRIVACY AT UGMACERAK

This is a brief document covering our strategies and policies we employ in order to safeguard our IT Infrastructure, data and network.

WiFi

This Privacy Policy outlines how we collect, use, disclose, and protect the personal information of users accessing the Wi-Fi network provided by UGMACERAK on the campus premises. We are committed to respecting and safeguarding our users' privacy rights.

1. Information Collection and Usage

1.1 Information we collect

When accessing and using our Wi-Fi network, we may collect the following types of information:

a. **Device Information:** We may collect information about the devices used to connect to the Wi-Fi network, such as IP addresses, MAC addresses, device identifiers, and technical details necessary for network operation.

b. **Network Usage Data:** We may collect information about network usage, including but not limited to session duration, bandwidth usage, websites visited, and data transferred.

1.2 Usage of Information

We may use collected information for the following purposes:

a. **Network Management:** To ensure proper functioning and security of the Wi-Fi network, we may monitor network traffic, troubleshoot issues, and enforce network policies.

b. **Network Improvement:** Aggregated and anonymized data may be analysed to improve network performance, optimize resources, and enhance user experience.

2. Data sharing and disclosure

2.1 Third-Party Service Providers

We may engage trusted third-party service providers to assist us manage and operate the Wi-Fi network. These providers include:

a. UniFi AP: We utilize UniFi Access Points to provide wireless network connectivity across the campus. UniFi AP devices may collect device information, such as MAC addresses and signal strength, to ensure seamless connectivity and optimize network performance.

b. UniFi Firewall: Our network security is enhanced through the use of UniFi Firewalls. UniFi Firewalls help protect against unauthorized access, malicious activities, and potential security threats. These devices may collect network traffic data for the purpose of identifying and mitigating security risks.

c. Cisco Switches: We employ Cisco switches to enable reliable and efficient data transmission within the network infrastructure. Cisco switches may collect device information, such as MAC addresses and network port activity, to facilitate network management, troubleshooting, and performance optimization.
d. Etisalat: Our internet service provider (ISP). Etisalat facilitates the connectivity between our campus network and the wider internet. As part of their service, Etisalat may collect certain network data, such as IP addresses and bandwidth usage, to ensure the proper functioning and delivery of internet services.

2.2 Legal Requirements

We may disclose personal information if required to do so by law, or in good faith that such action is necessary to:

a. Comply with legal obligations, court orders, or governmental requests.
b. Protect the rights, safety, or property of UGMACERAK, its users, or the public.

3. Data Security

We implement industry-standard security measures to protect personal information from unauthorized access, loss, misuse, alteration, or destruction. However, no data transmission or storage method is entirely secure, and we cannot guarantee absolute security and data protection.

4. Data Retention

We will retain personal information for as long as necessary to fulfil the purposes outlined in this Privacy Policy, unless a longer retention period is required or permitted by law.

5. Cybersecurity Strategies

5.1 Physical Isolation:

We have implemented physical isolation measures to ensure the security of our staff network. This involves separating the staff network from the student network, thereby minimizing the potential for unauthorized access or security breaches.

5.2 Network Segmentation:

Our staff network contains all the servers and is designed to be separate from other networks. This segregation helps protect sensitive information and restricts access to authorized personnel only.

5.3 Active Directory and Protected Folders:

We utilize Active Directory to manage user accounts and access permissions within staff network. This centralized authentication system allows us to control user access and ensure that only authorized individuals can access sensitive files and folders.

Additionally, we have implemented appropriate permissions on these protected folders and files. Access rights are assigned based on the principle of least privilege, ensuring that users have access only to the information necessary for their roles and responsibilities. Access and permissions are audited for the purpose of tracking and trail.

5.4 MAC Address Authentication:

To further enhance security, we may implement MAC address-based authentication for staff devices. This means that only devices with pre-registered MAC addresses are allowed to connect to our network. By sharing these MAC addresses with the IT team, we ensure that only trusted devices can authenticate and gain access to our network resources.

5.5 Regular Security Assessments:

We conduct regular security assessments and audits to identify vulnerabilities and address them proactively. This includes penetration testing, vulnerability scanning and monitoring of network activities to detect any unusual behaviour or potential threats.

5.6 Staff/Faculty Awareness and Training:

We conduct regular employee awareness and training relating to cybersecurity best practices. Regular training sessions are offered to educate staff members about potential risks, phishing attacks, password hygiene, and safe online behaviour. We empower our staff to actively contribute to our overall cybersecurity posture by promoting a security-conscious culture.

5.7 Incident Response Plan:

In the event of a security incident, we have an established incident response plan. This plan outlines the necessary steps to mitigate and contain the incident, minimize the impact on our systems and data, and restore normal operations as quickly as possible. Regular drills and tabletop exercises are conducted to ensure the effectiveness of the plan.

5.8 Antivirus and Antimalware Protection:

We employ Total 360 Security as our antivirus and antimalware protection solution. This software is regularly updated to defend against known threats and provides real-time scanning and monitoring of our systems for any malicious activities. It helps safeguard our network and devices from malware, viruses, and other forms of cyber threats.

5.9 Automated OS Updates:

We have automated our systems to run weekly operating system (OS) updates. By ensuring that our systems are up-to-date with the latest security patches and bug fixes, we minimize vulnerabilities and protect against known exploits. This proactive approach helps maintain the integrity and security of our network infrastructure.

5.10 VPN for Remote Staff:

We provide a Virtual Private Network (VPN) to our staff members who work remotely. The VPN creates a secure encrypted tunnel between their devices and our network, ensuring that all data transmitted between them remains confidential and protected. This increased protection helps safeguard sensitive information and prevents unauthorized access, even when staff members are accessing our network from external locations.

Last Updated:	*November 2025*
Reviewed on	*November 2025*
Next review Date	*September 2026*