Acceptable User Policy

1. Introduction

An Acceptable User Policy (AUP) for IQRA College outlines the guidelines and rules for the responsible use of school-provided technology, such as computers, laptops, internet access, and other digital resources. It protects Users from potential harm or legal liability and establishes guidelines for the appropriate use of school-provided technology and internet access.

2. Scope

This policy applies to all students and users who use school-provided technology, personal devices and internet access.

3. School Provided Technology

IQRA College provides technology equipment to users including computers, headphones, mouse, keyboards, and iPads. Users are expected to adhere to the guidelines put in place to ensure their proper and responsible use, to promote digital citizenship, and maintain a safe and productive learning environment. Users are therefore required to comply with the following:

Care and Responsibility

- Handle all technology equipment with care, keeping it in good working condition
- Not remove or tamper with any labels, identification tags, software and hardware components
- Report any damage, malfunction, loss, or theft of school-provided technology immediately to a designated staff member or to the IT department.
- Not lend, borrow, or share the school-provided technology equipment without proper authorisation from the IT department.
- Use email and other communication tools provided by the school in a responsible, professional, and respectful manner.
- Users log into School shared devices at their own risk. They are responsible in logging out of their school account from any and all School shared devices. Users take full responsibility if their account has been misused due to the user's failure to take adequate measures to maintain their ICT credentials.

Hardware and Safety Protocols

- Users will not share personal information about them, with other users without prior consent
- Students will promptly disclose to a teacher any message received that is inappropriate or makes the student feel uncomfortable
- Users will take great care of all ICT equipment in the school. This can include computers (Desktops, Laptops), interactive data panels, projectors, digital cameras, IPads, printers, scanners, microphones and headphones
- Users will use the technology at school for learning education/work purposes, use the equipment properly and not interfere with the work or data of another user.

4. Electronic Devices – Mobile Phones and Personal Laptops

- Students may bring their phones or other devices to school, but they must be powered off and handed to the responsible coordinator at the beginning of the School day, and collected at the end of the School day.
- Students are not permitted to use their devices on the bus at all times.
- Students caught bringing their devices or phones to school and not handing it in to the responsible coordinator at the beginning of the day will have their devices temporarily confiscated for a period determined by the responsible coordinator or the disciplinary coordinator – further disciplinary actions may be imposed *(Refer to the Discipline Policy)*.
- There may be instances where a student is required to bring and use their personal devices during School hours for medical reasons. In such case, parents must provide written documentation to the administration noting the device that will be used, the frequency of usage, and the reason it will be used, and the student must only use their device for the given purpose.
- Students from year 10-12 are encouraged to bring their own laptops to School to assist in coursework. Refer to the Acceptable User Policy for more information.

Responsibility

- It is the responsibility of any user who is connecting to the IQRA College network via a personal device to ensure that all components of their connection remain as secure during their network access within the office.
- It is imperative that any wireless connection to the IQRA College network to be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's device

Personal Liability

Students bring their personal devices to school at their own risk; They are solely responsible for the care and use of their personal devices. In the event of any damage, loss, misuse, or theft that occurs to their devices while on School premises, without the negligence of the school, students assume full responsibility for any associated consequences.

5. Prohibited Activities

Activities that are prohibited when using the School's internet, School-provided technology, personal laptops or any other devices include, but not limited to:

- Do not attempt to bypass network security measures, install unauthorized software, or engage in hacking or any other form of unauthorised access
- Hacking, cyberbullying, or distribution of illegal materials
- Distributing pornographic or offensive materials
- Engaging in activities that may damage or disrupt the school's technology infrastructure
- Using technology to cheat or plagiarise
- Violating copyright or trademark laws
- Spamming or sending bulk emails, including electronic chain mail.
- Using another person's password, disclosing a password to someone or impersonating someone
- Disabling, interfering with or overloading any computer system or protective measure
- Downloading or transferring illegal file types or subscribing to inappropriate email lists
- Downloading or transferring games
- Using inappropriate language
- Not allowed to use school or personal devices to capture photos or videos of self or other

students within the school compound

6. Internet Access and Usage

The School uses a content management system called 'Linewize' to help manage their technology and maintain the safety of the students with a school filter. It provides managed network access and restricts students from accessing the following during School hours:

- Social media
- Streaming media
- Games
- Offensive content
- Dating websites
- VPN and Adult websites

Students from year 10-12 are encouraged to bring their own laptops to School to assist in coursework (see BYOD Policy). Users refusing to download and install any IT mandated software will not be granted internet access and may have their devices confiscated – Students are not permitted to connect to any personal hotspot for internet access.

7. Monitoring and Security

The school reserves the right to monitor and log all activity on school-provided technology and internet access, and to take appropriate action to ensure the security of the school's technology infrastructure. Users using the internet have the responsibility to report inappropriate behaviour and material to their teachers for e.g., the transmission or receipt of inappropriate internet material from other student or staff.

The school reserves the right to suspend this service without notice if the company's systems, data, users, and clients are at risk.

** Year 10-12 teachers and coordinators, head of school, the IT department, Discipline Coordinator and the Principal may log in at any time and monitor all student activities conducted within school hours.*

8. Investigation Process

In the event that the IT department suspects that Users are misusing ICT resources, the School will communicate transparently with the Users involved. As a precautionary measure, the School reserves the right to temporarily suspend the email address, school account, or confiscate any device associated with the suspected misuse, pending a thorough investigation into the matter.

During the suspension period, a comprehensive investigation will be conducted to determine the nature of the misuse and to gather relevant evidence. The investigation may involve examining email correspondence, device usage history, internet activity logs, and any other relevant information that pertains to the suspected misuse. The School will make every effort to maintain the privacy and confidentiality of the investigation while ensuring that the truth is established.

Should the investigation uncover evidence of criminal behaviour or behaviour that is in violation of this or any other School's policies and practices, appropriate actions will be considered. These actions may include but are not limited to the suspension of email accounts, device privileges, and any other measures deemed appropriate under the School's Discipline Policy.

The investigation process may take up to a week to ensure a thorough and accurate assessment of the situation. Throughout this period, the IT department, along with the discipline coordinators, any other external designated parties, reserves the right to closely monitor the student's email, account, and device usage. This monitoring is intended to ensure that the student complies with the terms of suspension and exhibits appropriate behaviour after the investigation has concluded.

9. Consequences for Violations

Violations of any provision of this policy will be dealt with in accordance with this policy and the Discipline Policy. Any offence identified by any staff member and/or inducted personnel to inform Homegroup/House teachers who will notify the Parents and house teachers will follow the steps in the discipline policy.

10. Enrolment Exit

- Students agree that all information belonging to IQRA College will be deleted from personal devices by the IT department upon an enrolment exit from the school.
- Students agree that they will not keep any information belonging to IQRA College in their possession after exit and understand that IQRA College may take legal action against them if they are in violation of this policy.