

Technology Acceptable Use Policy

1. Introduction

Al-Islamia is committed to integrating technology into education while ensuring its ethical and secure use. This policy outlines the acceptable use of technological resources by staff, pupils, and volunteers, aligning with our eSafety Policy and the school's ethos.

2. Scope

This policy applies to all users of the school's technological resources, including:

- School-owned devices: Laptops, Interactive Whiteboards, iPads.
- Personal devices: Smartphones, tablets, laptops used for school purposes.
- Network and internet access: Both wired and wireless connections provided by the school.

3. School-Owned Devices

- Access: Staff and pupils have access to school-owned laptops, Interactive Whiteboards, and iPads.
- Security Measures:
 - Monitoring and Filtering: All devices are protected by SENSO, a monitoring and filtering system, to prevent access to harmful content.
 - Password Protection:
 - iPads: Password-protected and designated for staff use only, primarily for assessment and photographing evidence of learning.
 - Laptops: Feature two user profiles—'Student' and 'Staff'. Staff profiles are password-protected to maintain confidentiality and security.

4. Personal Devices

- Usage: Personal devices may be used for work purposes under the following conditions:
 - Mobile Phones:
 - Classroom Restrictions: Mobile phones must not be present in classrooms, except for Senior Leadership Team (SLT) members or with explicit permission.
 - Tablets and Laptops:
 - Classroom Use: Personal tablets, iPads, or laptops can be used in the classroom.
 - Privacy Measures: Personal information must be concealed and not visible to students at any time.

5. Cybersecurity Measures

- Monitoring and Filtering: Implementation of SENSO to monitor and filter internet usage, ensuring compliance with the school's eSafety standards.
- Training: Provision of cybersecurity training for staff to promote safe and responsible use of technology.

6. Handling Inappropriate Use

- eSafety Education: Integration of eSafety learning into the Computing curriculum to educate pupils on responsible online behaviour.
- Incident Reporting:
 - Documentation: All incidents, including those reported by SENSO, are logged and addressed promptly.
 - Cyberbullying: Any instances of cyberbullying or inappropriate use of technology by staff or pupils are handled in accordance with the school's disciplinary procedures – see Disciplinary Procedure Policy and Behaviour Policy.

7. Faith-Based Considerations

- Content Alignment: All media accessed for teaching and learning must align with the school's ethos, values, and the eSafety Policy.
- Content Restrictions: Access to content that contradicts the school's faith-based values and ethos is prohibited.

8. User Responsibilities

- Compliance: All users must adhere to this policy and the eSafety Policy.
- Reporting: Users are required to report any breaches or concerns related to technology use to an appropriate staff member, e.g., the Computing Lead and/or the Safeguarding team.

9. Policy Review

This policy will be reviewed annually to ensure it remains effective and relevant to the evolving technological landscape.