



## PL6 Learning Hub Safer Internet & IT Usage Policy

### 1. Purpose

This policy aims to ensure the safe and responsible use of internet and IT resources within [Your Tutoring Business Name], protecting both the business and its users from potential risks.

### 2. Scope

This policy applies to all staff, students, and visitors who use the IT resources of [Your Tutoring Business Name].

### 3. Acceptable Use

- **Work-Related Activities:** Internet and IT resources should primarily be used for educational and business-related activities.
- **Personal Use:** Limited personal use is permitted, provided it does not interfere with work performance or violate any part of this policy.

### 4. Prohibited Activities

- **Illegal Activities:** Accessing, downloading, or sharing illegal content.
- **Inappropriate Content:** Viewing or distributing obscene, offensive, or discriminatory material.
- **Security Risks:** Engaging in activities that compromise the security of the IT systems, such as hacking or spreading malware.

### 5. Data Protection

- **Confidentiality:** Ensure that all personal and sensitive information is handled in accordance with GDPR and other relevant data protection laws.
- **Encryption:** Use encryption for sensitive data to prevent unauthorized access.

### 6. Security Measures

- **Passwords:** Use strong, unique passwords and change them regularly.
- **Software Updates:** Keep all software and systems updated to protect against vulnerabilities.
- **Antivirus:** Install and maintain antivirus software on all devices.

### 7. Monitoring and Privacy

- **Monitoring:** [Your Tutoring Business Name] reserves the right to monitor internet and IT usage to ensure compliance with this policy.
- **Privacy:** Monitoring will be conducted in a manner that respects the privacy of users as much as possible.

## 8. Training and Awareness

- **Training:** Provide regular training to staff on safe internet and IT usage practices.
- **Awareness:** Promote awareness of potential cyber threats and safe online behavior.

## 9. Incident Reporting

- **Reporting:** Encourage users to report any security incidents or breaches immediately to the designated IT administrator.
- **Response:** Respond promptly to any reported incidents to mitigate potential damage.

## 10. Policy Review

This policy will be reviewed annually and updated as necessary to ensure it remains effective and relevant.