E-Safety Policy

1. Scope

1.1 The Indian Public School (TIPS) is committed to promoting and safeguarding the welfare of all students. Effective online safety and responsible use of technology are integral to this commitment.

1.2 The aims of this E-Safety Policy are to:

- Protect the School community from illegal, inappropriate, or harmful content, contact, or behavior online.
- Educate students, staff, and parents on the responsible use of technology, including laptops, mobile devices, and the internet.
- Establish clear procedures for identifying, intervening, and escalating incidents of online misuse or cyber harm.

1.3 The policy covers all technology, networks, and devices used for communication or learning, collectively referred to as **Technology**.

1.4 This policy applies to all members of the TIPS community, including students, staff, volunteers, parents, and visitors, whether on or off School premises, whenever their technology use affects student welfare or the School's reputation.

1.5 This policy should be read in conjunction with:

- Anti-Bullying Policy
- Staff Code of Conduct
- Safeguarding & Child Protection Policy
- Laptop Discipline & Usage Policy

---

2. Roles and Responsibilities

2.1 Proprietors

- Has overall responsibility for safeguarding, including E-Safety.
- Ensures leadership actively promotes student welfare and oversees the adoption and annual review of the E-Safety Policy.
- Reviews safeguarding procedures annually, including online safety measures, and evaluates their effectiveness.

2.2 Principal and Senior Leadership Team (SLT)

- Principal oversees safety, welfare, and online safety for all members of the School.
- Designated Safeguarding Leads (DSLs) are senior staff responsible for safeguarding, including technology-related incidents.

Responsibilities include:

- Ensuring all safeguarding and E-Safety policies are implemented and updated regularly.

- Responding promptly to incidents involving misuse of technology, cyberbullying, radicalization, or inappropriate content.
- Monitoring the **Technology Incident Log** on E360 for trends and areas for improvement.
- Liaising with parents, staff, and students on online safety incidents.
- Organizing staff and student training sessions on online safety.
- Organise digital awareness sessions for parents and guardians.
- Integrating online safety education into the curriculum and pastoral activities.
- Approving any exceptions for mobile devices or personal laptops.
- Reporting to the Proprietors on policy effectiveness and any incidents affecting reputation or student welfare.

2.3 IT Manager

Responsible for operational technology management and E-Safety.

Key responsibilities:

- **Security & Monitoring:** Maintaining network security, filtering harmful content, monitoring email, internet, and other technology usage.
- **Laptop Management:** Installing and maintaining school-approved operating systems on all laptops, managing warranty and repairs, ensuring compliance with Laptop Discipline Policy.
- **Support & Guidance:** Advising staff on safe technology use, reporting activity trends to SLT, supporting teaching staff with online safety tools.

- **Incident Response:** Investigating technical breaches, collaborating with DSL/SLT to ensure incidents follow safeguarding and disciplinary procedures.

2.4 Staff

Staff act as role models and enforce safe technology use.

Responsibilities include:

- Demonstrating appropriate professional use of technology.
- Teaching students safe and responsible technology use.
- Reinforcing online safety messages in lessons, assemblies, and pastoral activities.
- Reporting misuse or suspicious behavior immediately to DSL or IT Manager.
- Participating in mandatory E-Safety and data protection training.
- Supporting periodic Laptop audits and ensuring compliance with school policies.

2.5 Parents

Parents support safe technology use outside School.

Responsibilities include:

- Encouraging adherence to School technology policies.
- Discussing responsible use of laptops, mobile devices, and social media.
- Monitoring children's online activity and reporting concerns promptly.
- Ensuring students follow Laptop Discipline & Usage Policy.
- Participating in parent workshops and utilizing online safety resources.

- Encouraging children to seek help from staff if cyberbullying, radical content, or unsafe situations occur.

---

3. Education and Training

3.1 Students

- Online safety education is part of the ICT curriculum and reinforced across subjects.
- **Focus Areas:**
    - Risks of technology use (scams, cyberbullying, radical content).
    - Evaluating online information and privacy management.
    - Reporting suspicious or harmful behavior.
    - Understanding cyberbullying and consequences of negative online behavior.
    - Safe use of laptops, mobile devices, and external devices.
    - Reporting channels for incidents.
- **Early years and Primary:** Guided exploration of technology, understanding safe resources, and recognizing appropriate use.

3.2 Staff

- Induction and ongoing training covering:
    - E-Safety principles and safeguarding students online.
    - Cyberbullying, radicalization, and data protection.
    - Laptop management and monitoring of student compliance.
- Scenario-based workshops for handling online incidents.

- Updates on emerging risks, social media trends, and remote learning safety.

3.3 Parents

- Guidance via TIPS portal and annual workshops.
- Topics include cyberbullying, social media, parental controls, and monitoring laptops.
- Encouraged to report concerns to DSL or IT Manager promptly.

---

4. Access to School Technology and Laptops

4.1 Compliance with **Acceptable Use Policy** is mandatory for all users.

4.2 **User Access & Authentication:**

- Individual usernames and passwords required; sharing prohibited.
- Lost credentials reported immediately to IT department.

4.3 **Laptop Policy (Grades 6–12):**

- Students may use school-issued or registered personal laptops with school-approved OS.
- Warranty: 3 years (laptops), 1 year (chargers). Post-warranty repairs chargeable.
- **Usage Restrictions:** Academic purposes only; gaming, social media, streaming, or unauthorized OS/software prohibited.
- **Audits:** IT department conducts periodic laptop audits.
    - First offense: warning and award of demerit points, followed by counselling.

- Subsequent offenses: fines, suspension, or confiscation
- Severe misuse: permanent loss of laptop privileges.

- Students responsible for repair costs for intentional or accidental damage.

4.4 **Staff Use:** Governed by Staff Code of Conduct; personal devices for school use only in emergencies.

4.5 **Mobile Devices:** Students cannot bypass safeguards using mobile data. Exceptions require SLT or IT Manager approval.

---

5. Procedures for Misuse

5.1 **Reporting:** All incidents or suspicions must be reported to DSL, IT Manager, or Principal.

5.2 **Student Misuse:**

- Minor: Handled by tutors or teachers; warnings issued.
- Repeated: Reported to Discipline Committee; possible fines, suspension, or laptop confiscation.
- Severe: Hacking, offensive content, circumventing security; may result in permanent loss of privileges.

5.3 **Staff Misuse:**

- Reported via **Whistleblowing Policy**; serious cases handled via Safeguarding & Child Protection procedures.

5.4 **Other Users:**

- Parents, visitors, or other users' misuse reported immediately to Principal or IT Manager.
- School may withdraw access or report illegal activity to authorities.

5.5 **Investigation & Follow-up:**

- IT Manager and DSL investigate and document incidents.
- SLT determines disciplinary action based on severity.
- Education and corrective measures applied to prevent recurrence.

---

6. Monitoring and Review

6.1 **Monitoring:**

- IT Manager logs serious incidents in **Technology Incident Log**: internet/email misuse, unauthorized software/content, Laptop Policy breaches.
- Logs reviewed regularly by DSL and SLT to identify trends.

6.2 **Review:**

- DSL and SLT review policies and procedures annually for effectiveness.

- Stakeholders consider online safety, technology usage, and laptop compliance during safeguarding review.

6.3 **Audit & Improvement:**

- Periodic audits of laptops, network activity, and device usage.
- Findings inform updates to policies, staff training, and student education programs.
- Emerging risks (new platforms, cybersecurity threats) assessed and mitigations implemented.

6.4 **Reporting to Stakeholders:**

- SLT reports to Proprietors on policy effectiveness, incidents, and technology use trends.
- Updates shared with staff, parents, and students to reinforce online safety.

7 Resources

- ThinkUKnow
- Disrespect Nobody
- Safer Internet
- Internet Matters
- Educate Against Hate
- KidSmart
- SafeNetKids
- ParentInfo