IT and E-Safety Policy

Purpose of the Policy
At Next Steps Ed, we recognise the importance of technology in supporting learning, communication, and personal development. However, we are equally committed to ensuring the safe, responsible, and appropriate use of technology and the internet. This policy outlines our approach to IT use and e-safety to safeguard students, staff, and the wider school community.

Aims
- To ensure all students and staff use IT and online resources responsibly and safely.
- To educate students about online risks, digital wellbeing, and responsible behaviour.
- To provide clear procedures for identifying and responding to IT misuse or e-safety incidents.
- To promote a culture of safe and effective use of technology within the provision.

Scope
This policy applies to all staff, students, parents/carers, and visitors using the school's IT systems, devices, and networks. It covers all forms of digital communication, including email, the internet, social media, mobile devices, and cloud-based platforms.

Roles and Responsibilities

Senior Leadership Team
- Ensure e-safety is a priority within the provision and embedded in the curriculum.
- Review and update the IT and e-safety policy annually.
- Ensure staff receive regular training on IT use, safeguarding, and e-safety.

IT Manager/Coordinator
- Maintain the safety, security, and functionality of IT systems, including appropriate filtering and monitoring.
- Report any breaches of IT security or misuse to senior leaders.
- Support staff and students in the use of IT systems and resources.

Staff
- Model safe and appropriate use of IT systems and devices.
- Monitor students' use of IT in lessons and address inappropriate behaviour.
- Educate students about e-safety, digital responsibility, and online risks.

Students
- Use IT systems responsibly and in line with this policy.
- Report any concerns about e-safety, online bullying, or IT misuse to staff.
- Respect others online and follow the school's rules for safe internet use.

Parents/Carers

- Support the school's approach to IT and e-safety.
- Monitor and promote safe and responsible internet use at home.
- Communicate any concerns about their child's use of technology with the school.

Safe Use of IT and Online Systems

Filtering and Monitoring
- The provision uses filtering and monitoring systems to protect students from accessing harmful content.
- Staff and students are required to log into secure networks, and all activity is monitored to ensure safe use.
- Deliberate attempts to bypass security systems will result in disciplinary action.

Acceptable Use Agreements
- All students and staff must sign an **Acceptable Use Agreement** before accessing school IT systems.
- The agreement outlines expected behaviour, including rules for email, internet, and social media use.
- Failure to comply will result in appropriate sanctions.

Use of Personal Devices
- Personal devices (e.g., mobile phones, tablets) must be used in accordance with school rules.
- Students are not permitted to use personal devices during lessons unless directed by staff.
- Staff must ensure the secure and appropriate use of personal devices for school purposes.

E-Safety Education

- E-safety is embedded in the curriculum through **PSHE lessons**, workshops, and enrichment activities.
- Topics covered include online bullying, digital footprints, online privacy, and risks related to social media and gaming.
- Students are taught strategies to stay safe online, including recognising risks and reporting concerns.
- Staff receive regular training on online safeguarding, emerging risks, and supporting students effectively.

Responding to E-Safety Incidents

Reporting
- Students, staff, and parents/carers must report any e-safety concerns (e.g., online bullying, inappropriate content, security breaches) immediately to the Designated Safeguarding Lead (DSL).
- Concerns can also be raised via worry boxes or confidential reporting systems.

Investigating Incidents
- All reports of e-safety incidents will be taken seriously and investigated promptly.
- The DSL will involve external agencies, such as police or local safeguarding teams, where necessary.

Consequences
- Misuse of IT systems or breaches of this policy will result in appropriate sanctions in line with the Behaviour Policy.
- This may include restricted access to IT systems, loss of privileges, or further disciplinary action.
- Support and education will be provided to ensure students understand the consequences of unsafe online behaviour.

Online Bullying
Next Steps Ed has a **zero-tolerance approach to online bullying**. Students will be supported to:
- Recognise online bullying behaviours.
- Report incidents safely and confidentially.
- Access restorative approaches to repair harm caused.

The provision will work with families, external agencies, and support services to address and resolve incidents effectively.

Safeguarding and Online Risks*
The provision is committed to safeguarding students from specific online risks, including:
- Exposure to inappropriate or harmful content.
- Online exploitation, grooming, and radicalisation.
- Risks associated with social media and gaming.

The provision will provide clear guidance on identifying these risks and promoting safe practices both within and outside the provision.

Monitoring and Review
This policy will be reviewed annually to ensure it remains up to date with changes in technology, statutory requirements, and emerging e-safety risks. Feedback from staff, students, and parents/carers will inform updates to the policy.

Policy Review Date: 10th December 2025
Policy Approved By: Mica Smith - Director