Onside Education

E-Safety Policy

2025/6

The E-Safety Policy aims to provide comprehensive development opportunities to all students, encompassing both curriculum-based and broader learning experiences. This includes access to the internet and email (limited to staff) for legitimate personal development and educational purposes. Internet access can be obtained through various devices beyond school networked computers, such as mobile phones and tablets, and the policy applies uniformly to all methods of access.

The E-Safety Policy is interconnected with and pertains to other policies, including those addressing Bullying and Harassment, Behaviour, Phone, Child Protection and Safeguarding, and Data, GDPR, Filtering, and Monitoring. The programme lead responsibility as the E-Safety Coordinator, with the Senior Leadership Team taking charge in their absence.

Teaching and Learning:

Highlighting the importance of internet use, the policy recognises the internet as an indispensable component of 21st-century life for education, business, and social interaction. The programme facilitates internet access as a vital element of the statutory curriculum and a necessary tool for both staff and students. Internet use is designed to enhance learning, with a focus on online learning supported by education providers.

Students are instructed in effective internet research, including skills like knowledge location, retrieval, and evaluation. The responsible use of materials downloaded from the internet, adhering to copyright law, is emphasised. Students are trained to critically assess the materials they encounter and validate information before incorporating it into lessons.

Inappropriate Internet Use:

Acknowledging the potential misuse of the internet, the policy encourages students to report any electronic bullying, treating it in line with the Bullying and Harassment Policy.

Managing Internet Access:

The policy outlines information system security measures, filtering, and monitoring responsibilities. The programme lead with the senior leadership team managing system procurement, decision-making, effectiveness reviews, and reporting. The DSL takes the lead in safeguarding and online safety, working closely with Smoothwall (IT service providers) to ensure effective filtering and monitoring systems. Smoothwall is tasked with maintaining systems, providing reports, and conducting reviews.

Security Measures:

Security measures include regular reviews of ICT systems' capacity and security, installation of updated virus protection, and checks on files stored on school premises. No information is locally stored on laptops, and any security breaches may lead to disciplinary action or investigation by the Directors.

E-mail:

Onside Education does not provide students with email addresses or laptops. Students are advised against using personal emails on computers, and Onside Education disclaims responsibility for offensive emails or bullying on personal accounts. Personal information disclosure online is addressed through communication with the Senior Leadership Team and, in alignment with the Bullying and Harassment Policy, any "cyberbullying" is dealt with through appropriate channels.

Published Content and School Website:

The Onside Education website contains only institutional contact details, and personal information of staff or students is not published. Published images and work are carefully selected, with no use of full names, and permission is sought from parents or carers before publication.

Social Networking and Personal Publishing:

Access to social networking sites is filtered. Students are educated on the dangers of using such sites, advised against disclosing personal details, and are made aware of the risks involved.

Managing Filtering:

Collaborating with the DfES and the Internet Service Provider, the provision works to improve systems protecting students. Unsuitable sites are reported to the schools management team, and regular checks ensure filtering methods remain appropriate and effective.

Policy Decisions:

Staff and students are required to read the 'Code of Conduct' and the Mobile Phone Policy.

Assessing Risks:

Onside Education takes reasonable precautions to prevent access to inappropriate material but acknowledges the inherent challenges in guaranteeing absolute protection due to the international scope of the internet. No Student will have access to WIFI or a laptop onsite and any mobile phone should be secured away due to the mobile phone policy.

Handling E-Safety Complaints:

Complaints of student internet misuse are addressed by the Leadership Team, while complaints about staff misuse are referred to the programme lead. Safeguarding complaints follow the Child Protection and Safeguarding Policy.

Introducing the E-Safety Policy to Students:

E-Safety rules are displayed in networked rooms, informing students of monitored network and internet use. Students are educated on internet safety through the PHSE program, with additional support provided to identified vulnerable students.

Staff and the E-Safety Policy:

All staff are provided with Onside Educations E-Safety Policy, emphasising the importance of discretion and professional conduct. Staff with designated laptops undergo regular spot checks, including history and download content examinations. Spot checks are also conducted on staff emails and mobile phones.