EDSTART SCHOOLS

E-Safety Policy

SAFEGUARDING & WELFARE

Policy owner	EdStart Specialist Education Ltd
Applies to	EdStart Schools – All Sites
Category	Safeguarding & welfare
Approval and validity	September 2026 to September 2027
Review trigger	Annual review, or earlier following statutory, regulatory or operational change

Status: This 2026 version supersedes all previous versions.

The E-Safety Policy relates to other policies including Curriculum, Behaviour and Safeguarding.

EdStart's appointed E-Safety coordinator is Kevin Buchanan, Director of Education

1. TEACHING AND LEARNING

Why the internet is and digital communications are important:

- The internet is an essential element in 21st century life for education life for education, business and social interaction. EdStart has a duty to provide students with high-quality internet access as part of their learning experience.

Internet use will enhance and extend learning:

- EdStart's Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students.

Students will be taught how to evaluate Internet content:

- Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law.

2. MANAGING INTERNET ACCESS

Information system security:

- EdStart's ICT system security will be reviewed regularly. Virus protection will be installed and update regularly. Security strategies will be discussed with the Local Authority.

E-mail:

- Students may only use approved e-mail accounts on EdStart system. Students must immediately tell a teacher if they receive offensive e-mail. In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Published content and EdStart website:

- Staff or student personal contract information will not generally be published. The contact details given online should be EdStart office.

Publishing student's images and work:

- Photographs that include students will be selected carefully so that individual students cannot be identified, or their image misused. Student's full names will not be used anywhere on an EdStart website or other online spaces, particularly in association with photographs.
- Written permission from parents/carers will be obtained before photographs of students are published on the EdStart website.

Social networking and personal publishing:

- EdStart will control access to social networking sites, and consider how to educate students in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- 'Sexting' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated. However, EdStart takes a pro- active approach to help students to understand, assess, manage and avoid the risks associated with 'online activity'. The school recognises its duty of care to its young people who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed. Sexting disclosures should follow the normal safeguarding practices and protocols (see Safeguarding Policy).

Managing filtering:

- If staff or students discover an unsuitable site, it must be reported to the e-safety coordinator or the Network Manager.

Managing videoconferencing:

- IP videoconferencing should use the education broadband network to ensure quality of service and security rather than the internet.
- Student should ask permission from the supervising teacher before making or answering a videoconference call.

Managing emerging technologies:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the centre is allowed.
- The senior management team should note that technologies such as mobile phones with wireless Internet access can bypass EdStart's filtering systems and present a new route to undesirable material and communications.

Protecting personal data:

- Personal data will be recorded, processed, and transferred and made available according to the Data Protection Act 2018.

3. POLICY DECISIONS

Authorising Internet access:

- EdStart will maintain a current record of all staff and students who are granted access to EdStart's ICT systems.

Assessing risks:

- EdStart will take all reasonable precautions to prevent access to inappropriate materials. However, due to the international scale and lined nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to EdStart's network. EdStart cannot accept liability for any material accessed, or any consequences of Internet access.

3 Handling e-safety complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Director.

4. COMMUNICATING E-SAFETY

Introducing the e-safety policy to pupils:

- Students will be informed that network and internet use will be monitored.

Staff and the e-safety policy:

- All staff will be given EdStart e-safety Policy and its importance explained.

Enlisting parents and carers support:

- Parents and carers attention will be drawn to EdStart e-safety Policy in newsletters, EdStart brochure and on EdStart website.

Version: September 2026