Online Safety Policy

Date Accepted by YES Trust Board: Spring 2024

Reviewed by: Standards Committee

Date Reviewed: Spring 2024 – 18th March 2024

Date for Policy review: Spring 2025

Summary of changes in this version

None

GENERAL INTRODUCTIONS

The Online Safety Policy works in conjunction with the Trust's other policies including those for bullying and for child protection.

All academies in the Trust will appoint a designated safeguarding lead officer, who works in conjunction with an online safety coordinator (to be appointed by senior leaders).

Our Online Safety Policy has been written by the Trust and has been agreed by the Trust Standards Committee.

The Trust will ensure it meets the minimum requirements set out by the DfE RPA (Risk Pooling Agreement) in regards to cyber security standards. This is overseen by the Trusts ICT contractor.

TEACHING AND LEARNING

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business, and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

Internet use will enhance and extend learning

- Internet access across the Trust is designed for student and staff use and will include filtering appropriate to the age of students. This is controlled by the Trust's ICT support contractor, and the Trust's broadband and filtering provider – Schools Broadband.
- Clear boundaries are set for the appropriate use of the Internet and digital communications and discussed with both staff and students.
- Schools must ensure than students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.

Students will be taught how to evaluate Internet content

- All schools must have an online safety coordinator/lead.
- The online safety co-ordinator will ensure that the use of Internet derived materials by both staff and by students complies with copyright law.
- Students are to be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Usernames and passwords

- When joining any school in the Trust, students will be allocated a username and password for access to the school network. It is each student's responsibility to ensure that nobody else becomes aware of their password.

MANAGING INTERNET ACCESS

Information system security

- Trust and school ICT system security will be reviewed regularly by the school's IT support contractors.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed, where necessary, with the Trust Standards Committee and Risk/Audit Committee if required.

E-mail

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell either a member of the IT department, online safety co-ordinator or their 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.
- Incoming e-mail should be treated as suspicious, and attachments not opened unless the author is known, and the attachment is expected.
- The school will regularly review how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff or student personal contact information will not generally be published. The contact details given online should be the school office.
- The online safety coordinator responsible for ICT will take overall editorial responsibility and ensure that published content is accurate and appropriate.
- Staff are expected and required to ensure that any material posted only reflects the outstandingly positive nature of the school. This includes (but is not limited to) photos of the learning environment, and any online comments or communications. This also applies to any personal social media accounts while the member of staff is employed by the school.

Publishing students' images and work

- Where possible, photographs that include students will be selected carefully so that individual students cannot be identified, or their image misused.
- Students' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website or other online platforms.
- Work can only be published with the permission of the student and parents/carers, which is sought in the Home - School Agreement.

Social networking and personal publishing

- The school will control access to social networking sites and will 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.
- Students should not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.
- No employee of the school may have contact with a student on social media, or any personal device or account, unless specifically required by their role and ratified by the headteacher in writing.
- Staff members should take reasonable steps obscure their identity online to make it harder for students to locate their profiles.
- Staff may not post any references to any students of the school via personal social media, nor post anything that could be interpreted as reflecting the school negatively.

Managing filtering

- If staff or students discover an unsuitable site, it must be reported to the online safety coordinator or a member of SLT immediately.
- The online safety coordinator responsible for ICT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.

Managing video-conferencing

- Students should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the students' age.

MANAGING EMERGING TECHNOLOGIES

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time unless under the direct supervision of a member of staff. The sending of abusive or inappropriate text messages is forbidden.
- The use by students of cameras in mobile phones will not be permitted in school.
- No student-owned devices will be allowed on the school network.

PROTECTING PERSONAL DATA

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018, and the General Data Protection Regulations 2018.
- No student/staff personal data must be stored on any removable device unless encrypted or uses a strong password.
- Printing to a public area of a school will be PIN-locked to ensure confidentiality of produced documents.

POLICY DECISIONS

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. Staff must ensure that a signed copy of the agreement is in the possession of the online safety co-ordinator, or that the online safety co-ordinator can obtain a copy of this from the staff member's personnel file.
- The Trust's ICT contractor will maintain a current record of all staff and students who are granted access to school ICT systems.
- All students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- All staff must complete Cyber Security training which is to be updated in line with industry/DfE guidance.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the YES Trust can accept liability for any material accessed, or any consequences of Internet access.
- The Trust's ICT contractor will informally audit ICT use on a regular basis to establish if the online safety policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

Handling online 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 headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

COMMUNICATING ONLINE SAFETY

Introducing the online safety policy to students

- Students will be informed that network and Internet use will be monitored.
- A programme of training in online safety will be included in all IT lessons

Staff and the Online Safety Policy

- All staff will be given the Trust Online Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user. The internet should only be used in school where the individual's specific use is necessary to enable them to carry out their work in school.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff should ensure that any IT equipment provided by the school remains the property of the Trust at all times and should only be used for the purpose(s) it is intended for.
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship and should not communicate online with students in any way other than for school purposes – e.g., for the submission of assignments, etc. This should only ever be done through school email accounts or other approved communication methods. E.g., Arbor; class Dojo.
- Staff must not use Facebook or any other social networking site to communicate with students. They should ensure that the use of Facebook, etc. is restricted so that students cannot gain access to their profile.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the Trusts Online Safety Policy in newsletters and on the individual school websites.
- Schools will maintain a list of online safety resources for parents/carers.