Online Safety Policy

Date Accepted by YES Trust Board: Spring 2024

Reviewed by: Standards Committee

Date Reviewed: Spring 2024 – 18th April 2024

Date for Policy review: Spring 2025

Amendments to this version

- **(p1) – Inclusion of academies aims and 4 key categories of risk**
- **(p2) – Inclusion of roles and responsibilities descriptors**
- **(p4) – Inclusion of artificial intelligence awareness**

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).

All our academies aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Our Online Safety Policy has been written by the Trust and has been agreed by the Trust Standards Committee. This policy complies with our Funding Agreement and Articles of Association.

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.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

ROLES AND RESPONSIBILITIES

Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and reviewing its effectiveness. This policy has been agreed and approved by the Trust Standards Committee.

Local support boards

Key responsibilities of local support governors include:

- Ensuring our academies follow all current online safety advice to keep children and staff safe
- To hold headteachers to account for the implantation of online safety
- To make sure all staff undergo online safety training as part of child protection and safeguarding training
- To ensure all staff understand their expectations, roles and responsibilities around filtering and monitoring

The headteacher

Headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Trusts academies.

The designated safeguarding lead (DSL)

Details of the Trust academies designated safeguarding leads (DSL) [and deputy/deputies] are set out in the academies child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in the academy, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on academy devices and academy networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the academies' s child protection policy

- Ensuring that any online safety incidents are logged on CPOMS or school MIS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the academy to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on academy devices and academy networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at the academy, including terrorist and extremist material
- Ensuring that the academies ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the academies ICT systems on a [weekly/fortnightly/monthly] basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the academies ICT systems and the internet and ensuring that pupils follow the academies terms on acceptable use

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the academies ICT systems and internet. Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

Visitors and members of the community

Visitors and members of the community who use the academies ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

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 academy 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.
- Academies must ensure that 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 academies 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 academy in the Trust, students will be allocated a username and password for access to the academy 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 academy ICT system security will be reviewed regularly by the academies 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 academy 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 academy 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 academy web site

- Staff or student personal contact information will not generally be published. The contact details given online should be the academy 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 academy. 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 academy.

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 an academy 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 academy 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 academy 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 academy 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 academy via personal social media, nor post anything that could be interpreted as reflecting the academy 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 the academy is allowed.
- Mobile phones will not be used during lessons or formal academy 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 academies.
- No student-owned devices will be allowed on the academy network.

Artificial intelligence (AI)

- Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
- The Trust recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.
- The Trust will treat any use of AI to bully pupils in line with academies Behaviour Policy.
- Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the academy.

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 an academy 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 academy 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 academy 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 academy 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 academy network. Neither the academy 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 academy child protection procedures.
- Students and parents will be informed of the complaint's 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 the academy where the individual's specific use is necessary to enable them to carry out their work in the academy.
- 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 academy 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 academy purposes – e.g., for the submission of assignments, etc. This should only ever be done through academy 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 academy websites.
- Academies will maintain a list of online safety resources for parents/carers.