LAURUS

TRUST

# Online Safety Policy

|  |  |
|---|---|
| **Author:** | David Woolley |
| **Last reviewed:** | Oct 2021 |
| **Next Review Date:** | Oct 2022 |

The e-Safety Policy is part of the Trust and/or School Improvement Plan and relates to other policies including those for ICT, bullying and for safeguarding.

Our e-Safety Policy has been written by the Trust, building on government guidance. It has been agreed by the Senior Leadership Team and approved by the Trustees.

The internet is an essential element in 21st century life for education, business and social interaction. The Trust 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 pupils.

Each school within The Laurus Trust adopts a whole school approach to online safety which protects and educates students and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

This policy presents the four main areas of risk involved in using the internet; how we educate students to mitigate the risk of internet use; IT systems and procedures to ensure online safety for students and staff; support for parent/carers with online safety, protecting personal data and the implication of online safety for remote learning.

The breadth of issues classified within online safety are considerable but are categorised into four main areas of risk:

### 1. <u>Content</u>

Being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

### 2. <u>Contact</u>

Being subjected to harmful online interaction with other uses; for example: peer to peer pressure, commercial advertising and adults positing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

### 3. <u>Conduct</u>

Personal online behaviour that increases the likelihood of, or causes, harm; for example, 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.

### 4. <u>Commerce</u>

Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

In order to protect and educate students against these risks, the school does the following:

- Clear boundaries are set for the appropriate use of the internet and digital communications and are discussed with both staff and pupils.
- Students are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- 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.
- e-Safety rules will be posted in all rooms where computers are used and a summary of the rules will appear on each PC in school as a reminder to students before they log into the school's network.
- Students will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be included in the IT Induction lessons at KS3.

In order to provide a safe environment for students in which to learn, we have robust IT systems and security protection procedures in place to limit children's exposure to the four main areas of risk above. This includes the following:

- When joining a school within the Trust, all students and staff will be allocated a username and password for access to the school network/email system. It is each individual's responsibility to ensure that nobody else becomes aware of their password(s), as well as ensuring that they are changed on a regular basis.
- Trust and/or school ICT system security will be reviewed regularly by the Trust's Network Manager.
- Virus protection will be installed and updated regularly.
- Students may only use approved email accounts on the Trust/school system.
- The trust will regularly review how email from students to external bodies is presented and controlled
- The Trust internet access is designed expressly for pupil use and will include filtering appropriate to the age of students.
- 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.
- The Trust will ensure that systems to protect students are reviewed and improved if necessary.

- If staff or students discover an unsuitable site, it must be reported to the Network Manager.
- The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The Trust is committed to contributing to community cohesion and reducing the likelihood of students becoming radicalised. Our IT filters in our schools will be one of the strategies the Trust uses to help prevent this. Should any member of our IT Team become concerned about a student’s use of particular websites relating to terrorism, then this will be reported to the Designated Safeguarding Lead in the appropriate school who will investigate the matter further in line with the school’s Safeguarding policy.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile technology 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 messages is forbidden.
- The use by students of cameras on personal mobile technology will not be permitted in school.
- Student internet access via mobile phone networks (e.g. 3G, 4G, 5G) is not permitted in school unless under the direct supervision of a member of staff
- The Trust 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 Stockport/Tameside/Cheshire East/Manchester Education can accept liability for any material accessed, or any consequences of Internet access.
- The Trust will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

The following is in place to keep ICT systems and students safe when using emails:

- Students must immediately tell either a member of the IT support team or their teacher if they receive offensive email.
- In email communication, students must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known and the attachment is expected.
- If an incoming email appears suspicious, for instance looks like it might be a phishing email, it should be reported to the IT support team immediately.

We have a duty of care to staff to protect and educate them in their use of technology. The following measures are put in place across the Trust:

- All staff are expected to use their trust/school email account for any electronic communication relating to school matters and to follow protocols outlined in the Staff Acceptable Use Policy for ICT.
- Staff use of mobile technology will be in accordance with the protocols outlined in the Staff Acceptable Use Policy for ICT.

- All staff must read and sign the ‘Staff Acceptable Use Policy for ICT’ before using any Trust/school ICT resource. Staff must ensure that a signed copy of the agreement is in the possession of the Trust/school.
- The Trust will maintain a current record of all staff who are granted access to school ICT systems.
- All staff will be given the School e-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 who 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 school 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 pupils 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.
- Staff should not use Facebook or any other social networking site to communicate with students. They must ensure that the use of Facebook etc. is restricted so that pupils cannot gain access to their profile.
- In all aspects of digital communication and social networking, staff will be expected to comply with the protocols outlined in the Staff Acceptable Use Policy for ICT.

It is essential that parent/carers are also made aware of the risks surrounding internet use and how to keep their child safe online. All parent/carers are asked to sign a consent form for internet access in school.

Parent/carers attention is drawn to the Trusts Online Safety Policy in newsletters and on the Trust Website, which also contains online safety resources and advice for parent/carers.

In addition to the IT systems to reduce the risk of using the internet and educating around staying safe online we also have a legal responsibility to protect the personal data or staff, students and their parent/carers. The following processes/procedures ensure that personal data, students’ images and work are not shared online.

- Staff or student personal contact information will not generally be published. The contact details given online should be the school office.
- The Assistant Head of school responsible for marketing will take overall editorial responsibility and ensure that published content is accurate and appropriate.
- Photographs that include students will be selected carefully so that individual pupils 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.
- Work can only be published with the permission of the student and parents/carers.
- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018, please refer to the Data Protection Policy.
- No student/staff personal data must be stored on any removable device unless encrypted / passworded.

Since the COVID-19 pandemic began, the internet has been used widely for remote learning and video conferencing. The following measures are in place.

- Videoconferencing should use Trust approved platforms such as Microsoft Teams.
- When using videoconferencing efforts should be taken to limit unintended exposure of participants e.g. by blurring the background
- Within school setting videoconferencing should be supervised by staff at all times.
- Videoconferencing will be appropriately supervised for the students' age.
- During videoconferencing all other Trust policies continue to apply, for instance Safeguarding and Behaviour for Learning.

## 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 Head of School.
- Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- Complaints of a data protection nature must be dealt with in accordance with school data protection procedures.
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

# Equality Impact Statement

| | |
|---|---|
| Names and titles of people involved with this assessment<br>**Title of Policy – e-Safety** | **Emma Warrington SENDCO** |
| Impact assessment carried out with regard to identified characteristics | Race ☒<br>Disability ☒<br>Gender ☒<br>Age ☒<br>Religion & belief ☒<br>Sexual orientation ☒ |
| Summary of any issues/proposed changes | |
| Date | **Sept 21** |
| Date of next review | **July 2022** |