ELMLEA SCHOOLS TRUST

Online Safety Policy

Document History Record of recent Policy changes

Date	Version	Author/Owner	Change	Origin of
September 2023	1.0	Jo Sloper	New policy	Judicium Policies template incorporating KCSIE 2023 changes personalised for Elmlea by JS

Trustees 'Committee	Trustees
Policy Adopted	December 2023
Review cycle	Annual
Review date	September 2024

The latest version of this policy is available on the school website and upon request.

Governors have had oversight of this policy and review and approve it annually.

Contents

Commented [HK1]: Fill in the correct page numbers after school adaptations have been made.

1. Introduction

Elmlea Schools Trust is committed to a whole-school approach to online safety and safeguarding that protects and educates students and staff in their technology use. We aim to ensure the online safety of pupils, staff, volunteers, and governors. We use training, education, and effective procedures to both educate and protect the whole school community when they are online. We recognise that the use of technology has become a significant component of many safeguarding issues, including child-on-child abuse. We take any concerns seriously and escalate these where appropriate.

In line with Keeping Children Safe in Education, we aim to address the following four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: 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; 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.
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

We strive to consistently create a culture that incorporates the principles of online safety across all elements of school life. This helps to support our safeguarding culture.

The purpose of this policy is to ensure the safety and wellbeing of children when online and provide our staff and volunteers with the guidance and means to do this.

When safeguarding issues arrise this policy will need to be used in conjunction with the safeguarding policy and anti-bullying policy.

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

The policy also takes into account the National Curriculum computing programmes of study.

2. Roles and responsibilities

2.1 The governing body:

- Take overall responsibility for this policy and its implementation
- Read, and understand this policy
- Ensure the policy is reviewed and updated annually
- Ensure students are taught about online safety
- Ensure staff and governors receive safeguarding training that includes online safety at induction, and that this is regularly updated
- Ensure online safety is a running and interrelated theme whilst devising and implementing the whole school approach to safeguarding and related policies and procedures
- Ensure there are appropriate filtering and monitoring systems in place and regularly review the effectiveness of these systems

2.2. Executive Head/DSL

- Ensure staff understand this policy
- Ensure the implementation of this policy is consistent across the school
- Ensure any new members of staff learn about our approach to online safety at induction and regularly thereafter
- Manage any referrals via CPOMS effectively and understand how to escalate concerns
- Oversee the annual review of the school's approach to online safety, supported by the annual risk assessment that considers and reflects the risks that children face online.
- Take the lead responsibility for online safety as part of their duties as safeguarding lead and ensure that all incidents are logged using CPOMS
- Work with other Safeguarding Leads to address any online safety concerns or incidents, in line with our child protection and safeguarding policy
- Liaise with external safeguarding partners as necessary, including children's social care and the police and make referrals with the support of relevant colleagues and their expertise
- Ensure any online safety incidents are recorded appropriately and that staff are aware of how to record online incidents
- Deliver staff training on online safety
- Provide regular updates regarding online safety incidents to other DSLs
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received

2.3 Director of Finance and Operations – Bristol City Council/Computeam/Computing Lead

- Undertake an annual review of the Trust approach to online safety, supported by an annual risk assessment that considers the risks children face.
- Ensure appropriate filtering and monitoring systems are put in place
- Regularly review the filtering and monitoring systems to ensure students are safe from harm online
- Ensure that the school's IT systems are secure and protected against viruses and malware
- Ensure that the school has an appropriate level of security protection and that this is reviewed periodically to keep up with evolving cyber-crime technologies.
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received

Commented [HK2]: Please note that paragraph 145 of KCSIE says, "Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face."

Ensure that with this being in the policy, you have these procedures in place. We have a risk assessment pro forma you can request.

Commented [HK3]: Likely to include: IT lead, SENCO, IT technicians etc.

- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Updating and delivering staff training on online safety
- Liaise with school technical staff
- Report regularly to SLT
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

2.4 All staff and volunteers

Staff need to be confident with online safety to be able to implement this policy and support the education of all pupils with Elmlea Schools' Trust. They must:

- Read and understand this policy
- Assist with the consistent implementation of this policy
- Agree with and follow our acceptable use of IT agreement
- Agree with and follow the EST Code of Conduct for All Adults which outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.
- Refer any online safety safeguarding concerns to the DSL or a Deputy DSL and update CPOMS
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, maintaining an attitude of 'it could happen here' and not dismissing any reports.
- Update parents around what their children are being asked to do online, including the sites they may be asked to access and who, if anyone, their child should be interacting with from the school online.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- Follow the guidance of the 'Education for a connected world'. And 'Keeping children safe in education' when planning our online safety curriculum
- Be updated through the Computing Leads on any relevant information or changes that would further their understanding of online safety.

Commented [HK4]: Change to the term you use locally if this is different from Code of Conduct

2.5 Parents

- Understand the importance of children being safe online
- Read, understand and comply with this policy

- Read the information shared with parents regarding acceptable use, what the school asks the child to be doing online, including the sites they will be asked to access and who from the school (if anyone) will be interacting with their child
- Notify a member of staff regarding any questions regarding this policy and its implementation
- Ensure their child has read, understood and agreed to the acceptable use of IT agreement
- Support their child to behave safely and appropriately online
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
-

2.6 Pupils

- are responsible for following the Pupil Acceptable Use Policy
- need to have a good understanding of safe searching, research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online Safety Policy covers their actions out of school, if related to their membership of the school trust
- must demonstrate their understanding of how to be a good digital citizen when using home learning platforms

3. **Teaching online safety**

Commented [HK5]: Specify in which lessons/activities online safety is taught

In line with 'Teaching online safety in school,' published by the Department for Education in June 2019, we teach pupils about online safety and harms. Our teaching covers the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. These skills are covered in Computing, PHSE (Jigsaw), school assemblies and across the whole trust during Internet Safety Week/Safer Internet Day.

Throughout this, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives, including:

- how to evaluate what they see online
- the risks posed by social media platforms
- be taught about keeping personal information private, use of passwords and online messaging.
- how to recognise techniques used for persuasion
- unacceptable online behaviour
- how to identify online risks
- how and when to seek support
- how elements of online activity could adversely affect a pupil's personal safety or the personal safety of others online
- how elements of online activity can adversely affect a pupil's wellbeing
- being asked for their views when writing and developing online safety policies and practices, including curriculum development and implementation.

We recognise that there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Such groups may also face additional risks, for example from bullying, grooming and radicalisation. We will ensure these pupils receive the information and support they need through information provided from the school through online safety evenings for parents, support from the Inclusion Lead and information offered in the school newsletter and provided links.

In addition, our school completes an annual risk assessment for online safety. We consider the updated non-statutory guidance (Jan 2023) from the DfE on teaching online safety and how we teach these elements.

Commented [HK6]: We have guidance documents to support with this, including one to help you map key curriculum content which is closely tied to this guidance. See Appendix A of our Online Safety Risk Assessment for this

4. Filtering and monitoring

Appropriate security measures are in place to protect the firewalls, routers, wireless systems, work stations and mobile devices from accidental or malicious attempts which might threaten the security of the school trust's systems and data. The school trust's infrastructure and individual workstations are protected by up-to-date virus software.

Elmlea Schools Trust uses Netsweeper as a filtering and monitoring system provided through our local authority Bristol City Council. This filters and monitors for inappropriate content to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering. Furthermore, to ensure appropriate filters and appropriate monitoring systems are in place and we regularly review their effectiveness. Netsweeper limits children's exposure to the above risks from the Trust's IT system. This covers our school network including all devices across the trust.

The DSL has lead responsibility for understanding the filtering and monitoring systems and processes in place. The DSL and deputies monitor the effectiveness of this system through information provided by its monitoring and filtering provider.

The school takes care to not 'over block; content so that there are not unreasonable restrictions on what students can be taught regarding online safety.

The processes we have in place have been informed by our risk assessment as required by the Prevent Duty.

Commented [HK7]: Check to ensure you have this in place. We have documents to support with this.

The DfE has published filtering and monitoring standards which set out that schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without reasonable impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs

At Elmlea Schools Trust have done the following in relation to this:

When the filtering and monitoring system detects concerning usage, we will record this uisng CPOMS, contact our monitoring and filtering provider to block any harmful content found and take appropriate action, including making any relevant referrals to outside agencies if necessary.

Commented [HK8]: Outline how this record would be kept in your school.

5. Security

Elmlea Schools Trust has appropriate levels of security protection, and this is reviewed periodically to keep up with evolving cyber-crime technologies.

6. Educating parents about online safety

We recognise that parents can play a significant role in keeping their children safe online. To raise parents' awareness of online safety we provide training for parents on online safety. Digital Parenting magazine is a great parental resource which provides information on keeping their children safe online at home and includes the latest tips and news. The school sends this home when new editions are published. Information can also be sent out to parents via the school weekly newsletter when needed.

7. Acceptable use agreement

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

8. Use of mobile and smart technology

Some upper KS2 children use their phones to communicate with parents when walking home alone but these are switched off and unused when within the school grounds. If an inappropriate incident occurs, then the school will work in conjunction with children and parents to implement suitable measures in response to the incident.

We recognise that many children have unlimited and unrestricted access to the internet via mobile phone networks. This access means some children can sexually harass, abuse, bully or control their peers via their mobile and smart technology, share indecent images consensually and non-consensually and view and share pornography and other harmful content. Any incidents will be dealt with using guidelines outlined in Elmlea Schools' Trust Good Behaviour and Anti-Bullying policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Our EST Code of Conduct for All Adults outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.

Commented [HK9]: Change to the term you use locally if this is different from Code of Conduct

Where a staff member misuses the school trust's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school trust will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. Training and staff knowledge

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. This will also include training on the filtering and monitoring system used by the school and an understanding of expectations, applicable roles and responsibilities in relation to this.

All staff members will receive refresher training at least annually as part of our safeguarding training programme, as well as relevant updates (for example through emails, e-bulletins and staff meetings and INSET days). E-safety training is also available for staff via the National College.

Commented [HK10]: Don't forget we have an e-learning on this topic which staff could also complete

The DSL and Deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

All staff should be aware and know:

- The indicators of abuse and neglect understanding that children can be at risk of harm inside and outside of the school/college, inside and outside of the home and online.
- To take reports of online harmful behaviour seriously and report them according to the school procedures.

- That technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline.
- That children can abuse other children online; this can take the form of:
    - Online abuse, including sexual
    - Online harassment, including sexual
    - Cyberbullying
    - Misogynistic/ misandrist messages,
    - the non-consensual sharing of incident images, especially around chat groups,
    - and the sharing of abusive images and pornography to those who do not want to receive such content.
    - That child-on-child abuse could be happening in the school setting and that this could be taking place online. All incidents of child-on-child abuse should be reported in line with our reporting systems.

More information about safeguarding training is set out in our child protection and safeguarding policy.

10. Further information to support you

We work with our local safeguarding partners, Bristol Safeguarding in education team to ensure our students are safeguarding. We will liaise with these partners where there are safeguarding concerns and will follow their policies and procedures when needing their support. This may include referrals or seeking advice from Children's Social Care, our local Prevent team and/ or the police.

Commented [HK11]: Add any specific information related to your local safeguarding partners here

For **parents** the following websites could be of use:

- Samaritans: Talking to your child about self-harm and suicide content online
- NSPCC Online Safety Guides for parents
- Report harmful content at https://reportharmfulcontent.com/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/
- Thinkuknow- how to help your children get the most out of the internet
- Further guidance shared by the DfE can be accessed here

For **students** the following websites could be of use:

- Mind- mental health support
- Togetherall- online community accessible 24/7
- Shout- a free text service available 24 hours a day. You can start a conversation by texting Shout to 85258
- Samaritans' self-help app

- Kooth is an online mental wellbeing community for young person
- Report harmful content at https://reportharmfulcontent.com/child/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/

For **all staff and volunteers,** it is useful to be aware of the resources available to staff and students so that you can signpost them as required. In addition, the following resources could be of use:

- UK Safer Internet Safety- teacher guides and resources
- https://www.internetmatters.org/schools-esafety/
- https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

Policies/ guidance to be read and understood alongside our online safety policy:

- Safeguarding/ Child Protection policy.
- Behaviour policy.
- EST Code of Conduct for All Adults inc. acceptable use of technology in the staff behaviour policy/ code of conduct.
- Anti-bullying procedures including cyberbullying
- The Prevent Duty and The Prevent duty: an introduction for those with safeguarding responsibilities
- Meeting digital and technology in schools and colleges (DfE)

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school trust's ICT systems and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • I will not look at, move or delete other people's files. • I will not alter any settings or rename desktop items. • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer If I bring a personal mobile phone or other personal electronic device within the school trust: • I will not use it during lessons, clubs or other activities organised by the school trust, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online • I will not take any photographs or videos when on the school trust premises without permission of the Headteacher. • I agree that Elmlea Schools' Trust will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that if I deliberately break these rules, I could be stopped from using the internet, computers or iPads.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school trust's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using	

the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors
Name of staff member/governor/volunteer/visitor:
When using the school trust's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school trust's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details
I will only use the Elmlea Schools' Trust ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school trust will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person(s) who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	