Online Safety Policy

Context

Wise and compassionate citizens understand the power of the internet. We want St. Ebbe's children to embrace and make the most of the countless opportunities to connect with others and to acquire new knowledge and learn new skills, whilst being able to be curious about where content has originated and to make wise decisions about how much of their time to spend online. We want them to develop an online presence which reflects compassionate citizenship whilst clearly understanding how to keep themselves and others safe when online.

We have clear processes in place to keep children safe online whilst in our care, a systematic approach to educating children in online safety as well as clear mechanisms to identify and report potential threats where appropriate.

The Designated Safeguarding Lead (DSL) has overall responsibility for online safeguarding within the school.

We identify that the issues can be broadly categorised into three 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
- **conduct:** 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: r**isks such as online gambling, inappropriate advertising, phishing and/or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

This policy should also be read in conjunction with our Relationships and Sex Education Policy and Behaviour Policy.

Policy

Teachers will:

- Refer to the SMART poster at the start of every lesson
- Deliver the aims of the Computing National Curriculum (see below)
- Deliver the online safety curriculum via Purple Mash
- Focus especially on the positive use of messaging apps such as WhatsApp whilst emphasising age restrictions (Year 4-6)
- Encourage children to report online abuse including in messaging apps ASAP
- Inform parents as soon as a child discloses online abuse or they suspect may not be using the internet safely
- Take every opportunity to teach Online Safety within other areas of the curriculum or when issues arise
- Report any online safety issues to the DSL in line with safeguarding procedures
- Review the Acceptable Use Agreement with pupils termly
- Begin each lesson by remembering the SMART acronym
- Discuss the safe use of social media including cyber-bullying, during PHSRE lessons and in line with our RSE policy
- Report concerns to the DSL

- Ensure mobile phones are handed in and stored safely
- Check children's Smart Watches are disabled

Children will:

- Read and adhere to the school's Acceptable Use Agreement
- Only access the internet on school devices during the school day
- Disable Smart Watches during the school day

Parents are requested to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Regularly check websites which give parental guidance on keeping children safe (See below)
- Ensure children have a healthy balance of screen time and other activities
- Activate parental controls and locks where available – e.g. YouTube
- Observe recommended ages for websites and apps (E.g. WhatsApp is 16+)
- Regularly check children's use of the internet and Apps (including messaging Apps) to check what they are searching and sharing is appropriate
- Regularly discuss online safety with children
- Contact their child's teacher if they have any concerns about online behaviour/cyber-bullying
- Inform their child's class teacher if their child is bringing a mobile phone to school and the reasons for this (e.g. travelling to and from school alone)
- Disable internet connection from all Smart Watches
- Keep up to date with Online Safety via, for example the NSPCC (see below)

The ICT Lead, in conjunction with the DSL (Designated Safeguarding Lead) will:

- Ensure a comprehensive whole school curriculum response is in place to enable all pupils to learn about and manage online risks effectively
- Support parents and the wider school community (including all members of staff) to become aware and alert to the need to keep children safe online.
- Keep staff updated with new safety threats/relevant teaching material
- Organise and communicate Online Safety Day (annually February)
- Host an annual internet safety event for parents
- Provide relevant training to staff
- Carry out annual online safety surveys of staff, parents and children

The DSL (or Deputy DSL) (Designated Safeguarding Lead) will:

Work with staff to address and log any online safety issues or incidents in line with the school behaviour policy

- Provide internet safety training as part of induction training
- Train staff in cyber-bullying as part of safeguarding training
- Keep staff and parents updated with new safety threats via email/weekly newsletter
- Keep the school website updated with useful websites
- Report to the Governing Body and provide training updates as part of safeguarding training
- Search pupils' electronic devices where they believe there is a 'good reason to do so' and in line with DfE Guidance

- Monitor internet searching in school via Securus screenshot alerts and record incidents of concern on CPOMS

The ICT Support Team (123ICT) will:

- Put in place appropriate filtering and monitoring systems - Securus
- Ensure the school's ICT systems are secure and protected against viruses and malware
- Conduct a full security check and monitor the school's ICT systems
- Block access to potentially dangerous sites
- Send all requests for unblocking to the Headteacher for approval
- Keep school updated with new threats

How will we know it's working?

- Fortnightly tracking of cyber-bulling/internet safety issues to governors
- Monitoring of reports from EXA regarding inappropriate searches online
- What pupils say about how to stay safe online
- Pupil surveys
- Parent surveys
- Staff surveys

For more information

DfE Publications

Keeping Children Safe in Education

DfE Teaching Online Safety in School

DfE Searching, screening and confiscation at school

Education for a Connected World

UK Council for Internet Safety

DfE Preventing and Tackling Bullying (including Cyber Bullying)

DfE Relationships, Sex and Health Education

National Curriculum Computing Programme of Study

Advice and Information

Apps, games and social media sites reviews for parents (net-aware.org.uk)

Think U Know

UK Safer Internet Centre

Childnet International

Internet Matters

ParentZone

Online Safety Policy

Netaware

National Online Safety Guides for Parents

NSPCC Keeping children safe online

Reviewed by	Approved
Operational Management Team	Jan 22
Operational Management Team	TBA November 2023