# CROXBY PRIMARY SCHOOL

# E-SAFETY POLICY

**Effective Date:** -September 2025

**Date of minuted approval by the Board of Governors:** June 2025

**Review Committee:** Primary Local Board

**Review Date:** September 2026

## Rationale

The education of learners in online safety is an essential part of the school's online safety provision. Our approach is informed by the Department for Education's guidance *"Teaching Online Safety in Schools" (2019)* and the statutory safeguarding framework outlined in *Keeping Children Safe in Education (KCSIE)*. We are committed to not only meeting but exceeding the minimum expectations set out in this guidance, ensuring that online safety is fully embedded across all aspects of school life. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum, and staff should reinforce online safety messages consistently. The online safety curriculum should be broad, relevant, and provide clear progression, with opportunities for creative activities and real-world application, and will be provided in the following ways.

### Aims

- teach learners to become responsible, respectful and competent users of data, information and communication technology.
- teach learners to understand the importance of governance and legislation regarding how information is used, stored, created, retrieved, shared and manipulated.
- equip learners with skills, strategies and knowledge that will enable them to reap the benefits of the online world, whilst being able to minimise risk to themselves or others.
- exceed the minimum government recommended/statutory guidance for online safety.

### Guidelines

Online safety has a high profile at Croxby for all stakeholders. We ensure this profile is maintained and that pupil needs are met by the following:

- a relevant up-to-date online safety curriculum which is progressive from Early Years to the end of Year 6.
- a curriculum that is threaded throughout other curriculums and embedded in the day-to-day lives of our learners.
- training for staff and governors which is relevant to their needs and ultimately positively impacts on the learners.
- scheduled pupil voice sessions and learning walks steer changes and inform training needs.
- through our home/the school links and communication channels, parents are kept up to date with

relevant online safety matters, policies and agreements via newsletters, social media links, and the school website. They know who to contact at the school if they have concerns.

- staff have read the Trust ICT Acceptable Use Policy which are signed and copies freely available on the Trust website.
- our trust Safeguarding and Child Protection Policy clearly states how the monitoring of online safety is undertaken and the school's Behaviour Policy states how any incidents/infringements to it are dealt with.
- filtering and monitoring systems for all our online access

**We aim to provide online safety for all learners and our teachers will ensure that:**

- the online safety curriculum is delivered and links made to this whenever appropriate
- they stay up-to-date with current online safety information/vocabulary
- they complete staff online surveys and attend appropriate training sessions
- they read, understand and help promote the school's eSafeguarding policies and guidance
- they read, understand and adhere to the school staff Acceptable Use Policy
- they ensure that all online safety incidents are logged promptly and escalated following the school's safeguarding procedures
- they develop and maintain an awareness of current eSafeguarding issues and guidance
- they model safe and responsible behaviours in their own use of technology
- they embed eSafeguarding messages in learning activities across all areas of the curriculum.
- they supervise and guide learners carefully when engaged in learning activities involving technology
- they understand and are aware of incident-reporting mechanisms that exist within the school

**The designated online safety lead will ensure that:**

- pupil voice for online safety is completed annually and results used to inform planning and teaching
- internet safety days and visitors are planned to enhance the importance of online safety
- any up-to-date online safety information is shared with staff/parents/children as appropriate
- they promote an awareness and commitment to eSafeguarding throughout the school
- they are the first point of contact on all eSafeguarding matters
- they develop an understanding of current eSafeguarding issues, guidance and appropriate legislation
- they ensure that all members of staff receive an appropriate level of training in eSafeguarding issues through staff CPD
- eSafeguarding education is embedded across the curriculum
- eSafeguarding is promoted to parents and carers via newsletters, social media links, and the school website
- Safeguarding incidents are logged correctly using CPOMs.

**Implications for the whole school will be:**

- a series of specific eSafeguarding-related lessons will be provided in every year group/specific year groups as part of the Computing curriculum / PSHE curriculum / other lessons.
- we will celebrate and promote eSafeguarding through assemblies and whole- school activities, including promoting Safer Internet Day each year.
- we will discuss, remind or raise relevant eSafeguarding messages with learners routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- learners will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

At Croxby, we recognise that some learners, including those with Special Educational Needs and Disabilities (SEND) or other vulnerabilities, may require additional support to develop their understanding of online safety. We ensure that online safety education is adapted to meet individual needs where appropriate, providing targeted resources, scaffolded teaching, and additional adult support when necessary. Staff are aware of the specific risks that vulnerable learners may face online and are proactive in offering extra guidance and reassurance to help build their resilience and ability to navigate online environments safely.

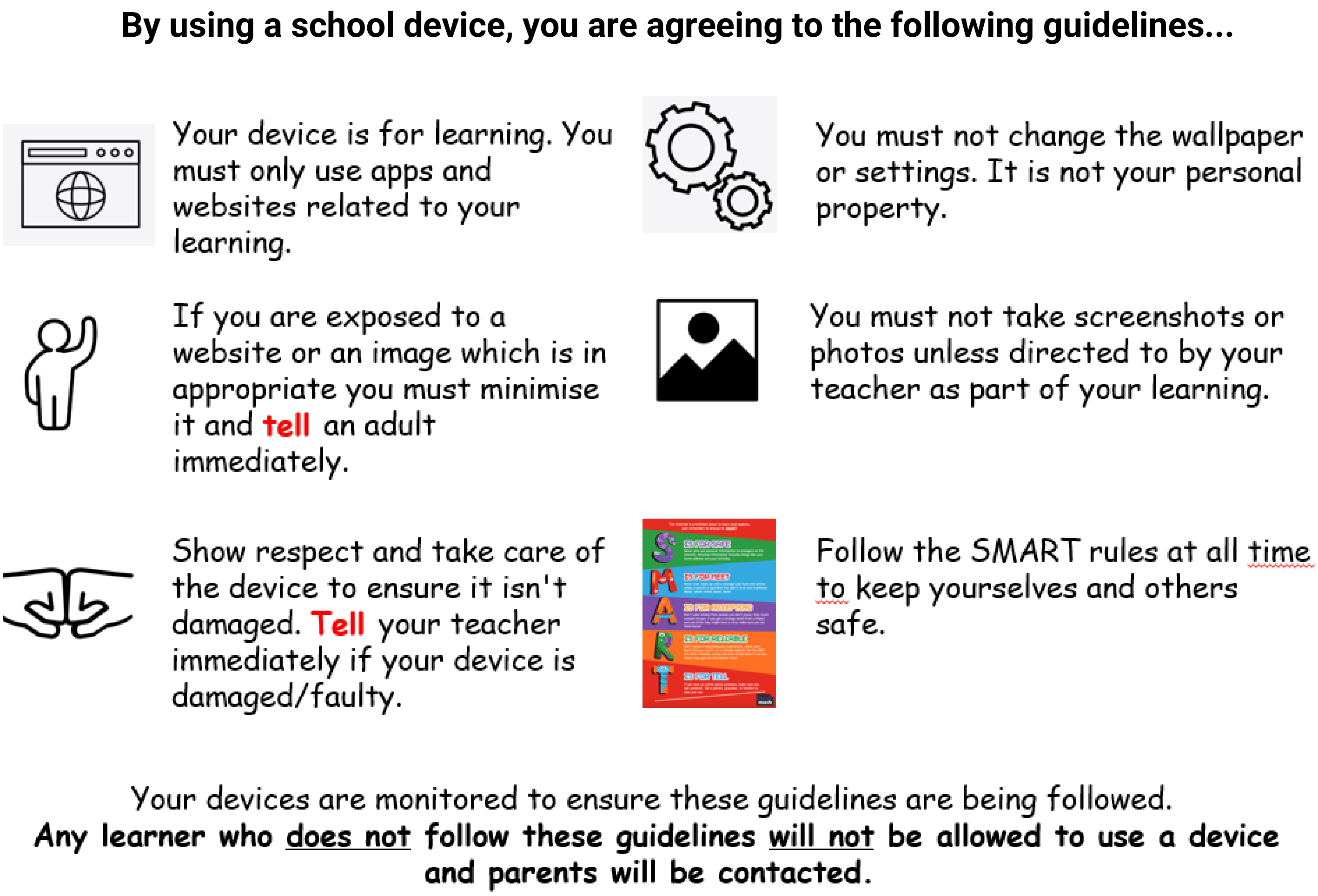
The school uses Smoothwall filtering and monitoring systems to help safeguard learners online. These systems automatically detect, block, and log any attempts to access inappropriate or harmful material, as well as monitor online behaviour for signs of potential safeguarding concerns. Any detected infringements are reviewed by the safeguarding team and appropriate action is taken in line with school policy.

Appendix 1: Overview of progression of e-safety learning through the school.

| | |
|---|---|
| Year 1 | • To be introduced to the concept of using computers safely, within the context of a school setting.<br>• To explore why we have rules in school and how those rules help us and then apply this understanding to rules needed for using computer technology safely.<br>• To understand how passwords and PINs keep devices and information secure.<br>• To recognise some examples of strong and poor password practice.<br>• To demonstrate the types of data that may be personal to you.<br>• To be able to articulate under what conditions I would ask an adult for help.<br>• To recognise that certain behaviours online can upset others and give examples of these<br>• To give examples of behaviours that can make others feel more pleasant emotions. |
| Year 2 | • To identify the features of effective passwords and identify why we need these.<br>• To consider how to use different forms of information technology safely, in a range of different environments.<br>• To list different uses of IT and talk about the different rules that might be associated with using them.<br>• To describe the difference between information shared on public platforms (YouTube) and privately (WhatsApp/Direct message), and what is appropriate for these platforms.<br>• To identify some characteristics that are typical of online bullying behaviour, considering the motives of these and how they may make someone feel.<br>• To recognise the difference between accidental and intentional behaviours that may affect others.<br>• To identify who they can turn to for help and support in different settings. |
| Year 3 | • To recognise that passwords protect my reputation and the information that I consider important.<br>• To be able to suggest methods for keeping password safe and secure.<br>• To demonstrate an awareness of the people that can be trusted.<br>• To make decisions about what information is appropriate to be shared and with whom.<br>• To recognise that smart devices often collect and share personal information and other information about people.<br>• To describe methods people may use to bully others including online and offline methods, and what this may look like.<br>• To identify the appropriate types of content that can be shared online and suggest ways to protect this.<br>• To explain why it is important to be kind online. |
| Year 4 | • To gain an appreciation of the fact that not everything they see on the internet is true, honest, or accurate.<br>• To identify the risks posed by over-sharing information online and suggest appropriate strategies for keeping personal information private in different contexts.<br>• To understand how monitoring services are used to keep children and users safe online.<br>• To structure an argument from one perspective and convey this with effective and clear contributions.<br>• To describe how some online services may seek consent to store information about me and know how to seek support if unsure about this.<br>• To understand bullying behaviour can make someone feel upset, hurt or angry.<br>• To explain the different features of different media.<br>• To simply describe what bullying online may look like on these different forms of media and how this can affect the feelings of others.<br>• To understand that what I do online can influence how someone feels about me.<br>• To understand I should not be mean online. |
| Year 5 | • To identify risks posed by not protecting accounts and information online.<br>• To implement appropriate strategies for creating strong passwords. |

| | |
|---|---|
| | • To understand how and why apps request permission to access data.<br>• To explain some differences between online and offline bullying.<br>• To know how to be an ‘upstander’ online and recognise when banter becomes harmful.<br>• To know who to speak to and how to seek support if someone I know was being bullied online.<br>• To understand if someone is at risk of harm I need to tell a responsible adult.<br>• To know how to block abusive users on the different platforms, apps and games that they use.<br>• To understand how to report posts, images, videos and photos on the different platforms, apps and games that they use. |
| Year 6 | • To recognise and select effective strategies for managing passwords<br>• To suggest methods for managing situations where passwords are lost or stolen.<br>• To compare different methods of communicating on the internet.<br>• To decide when I should and should not share information online.<br>• To explain that communication on the internet may not be private.<br>• To distinguish between genuine and fake content/sites.<br>• To understand some tactics employed by scammers.<br>• To identify the features of scam communications.<br>• To know there are different ways to gather evidence of bullying behaviour online.<br>• To know some different ways to use technology to protect myself from bullying behaviour.<br>• To identify routes for reporting bullying and harmful behaviours they witness or experience online.<br>• To make decisions about the suitability of different reporting routes based on context.<br>• To consider strategies for safely and positively intervening. |

Appendix 2: Copy of the e-safety slide shared with all learners at the start of each lesson which includes the use of IT.



**By using a school device, you are agreeing to the following guidelines...**

Your device is for learning. You must only use apps and websites related to your learning.

You must not change the wallpaper or settings. It is not your personal property.

If you are exposed to a website or an image which is in appropriate you must minimise it and **tell** an adult immediately.

You must not take screenshots or photos unless directed to by your teacher as part of your learning.

Show respect and take care of the device to ensure it isn't damaged. **Tell** your teacher immediately if your device is damaged/faulty.

Follow the SMART rules at all time to keep yourselves and others safe.

Your devices are monitored to ensure these guidelines are being followed.

**Any learner who does not follow these guidelines will not be allowed to use a device and parents will be contacted.**