



# SAXON WAY

---

PRIMARY SCHOOL

## Online Safety Policy

Date: January 2026

Review Due: January 2027

Reviewed Annually

## Introduction

Saxon Way's lead professional for Online Safety is Jen Vidler-Ironmonger (Head of School). This policy has been written for Saxon Way, in line with local and national guidance. This policy should be read in conjunction with the Safeguarding Policy (Child Protection) and the Anti-bullying Policy and includes protecting children from maltreatment online.

## Background

At Saxon Way we understand the benefits and the risks associated with using the internet. This policy sets out clear procedures to ensure our pupils are safe and that they can learn how to use the Internet and ever-changing technologies in a safe and discerning way.

Adults, as well as young people, can find themselves vulnerable to malicious use of the Internet both in their personal and professional lives. This policy highlights the importance of training and guidance in good practice in safer use of the Internet for staff. The policy also recognises that there are other safety issues associated with using technologies, such as over-exposure to LCD screens, privacy etc. Children with SEND or those who are otherwise vulnerable (e.g., victims of abuse) may face unique or heightened risks online.

The Internet and associated technology is a rapidly evolving environment where new opportunities and risks appear daily. Pupils learn to manage existing risks and understand the dynamic nature of technologies, so that they are able deal confidently with challenges in the future, whatever they might be.

The school recognizes that the digital landscape is rapidly evolving with the emergence of Generative Artificial Intelligence (AI). While AI offers educational benefits, it also introduces risks such as the creation of deepfakes (highly realistic but fake images, audio, or video) and the potential for biased or harmful content. We are committed to teaching pupils and staff how to navigate these technologies safely and critically.

## Roles and Responsibilities

Role	Key responsibilities
Head teacher	<ul style="list-style-type: none"> <li>• takes overall responsibility for online safety provision</li> <li>• take overall responsibility for data and data security (SIRO)</li> <li>• to ensure the school uses an approved, filtered Internet Service, which adheres to best practice and recommendations</li> <li>• to be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant</li> <li>• to be aware of procedures to be followed in the event of a serious online safety incident.</li> <li>• to receive regular monitoring reports from the Online Safety Co-ordinator</li> <li>• to ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager or IT support company)</li> </ul>
Online Safety Co-ordinator / Designated Safeguarding Lead	<ul style="list-style-type: none"> <li>• takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents</li> <li>• promotes an awareness and commitment to e-safeguarding throughout the school community</li> <li>• ensures that online safety education is embedded across the curriculum</li> </ul>

	<ul style="list-style-type: none"> <li>• liaises with school ICT technical staff</li> <li>• To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering, and school's change control processes and requests</li> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident</li> <li>• To ensure that an online safety incident log is kept up to date</li> <li>• facilitates training and advice for all staff</li> <li>• liaises with the Local Authority and relevant agencies, including making appropriate referrals to Children's Social Care and/or the police when necessary</li> <li>• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:             <ul style="list-style-type: none"> <li>○ sharing of personal data</li> <li>○ access to illegal / inappropriate materials</li> <li>○ inappropriate on-line contact with adults / strangers</li> <li>○ potential or actual incidents of grooming</li> <li>○ online bullying and use of social media</li> <li>○ extremism and radicalisation</li> </ul> </li> </ul>
Governors	<ul style="list-style-type: none"> <li>• To ensure that the school follows all current online safety advice to keep the children and staff safe</li> <li>• To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor</li> <li>• To support the school in encouraging parents and the wider community to become engaged in e-safety activities</li> <li>• The role of the E-Safety Governor will include:             <ul style="list-style-type: none"> <li>○ regular review with the E-Safety Co-ordinator / Officer (including: e-safety incident logs, filtering / change control logs )</li> </ul> </li> </ul>
Computing curriculum leader	<ul style="list-style-type: none"> <li>• To oversee the delivery of the e-safety element of the Computing curriculum</li> <li>• To liaise with the e-safety coordinator regularly</li> </ul>
Network Manager / Technician	<ul style="list-style-type: none"> <li>• To report any e-safety related issues that arise, to the e-safety coordinator.</li> <li>• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed</li> <li>• To ensure that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up to date</li> <li>• To ensure the security of the school ICT system</li> <li>• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices</li> <li>• the school's policy on web filtering is applied and updated on a regular basis</li> <li>• that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant</li> <li>• that the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any</li> </ul>

	<p>misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction</p> <ul style="list-style-type: none"> <li>• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a critical incident or system failure</li> <li>• To keep up-to-date documentation of the school’s e-security and technical procedures</li> </ul>
Data Manager	<ul style="list-style-type: none"> <li>• To ensure that all data held on pupils on the school office machines have appropriate access controls in place</li> </ul>
Teachers	<ul style="list-style-type: none"> <li>• To embed e-safety issues in all aspects of the curriculum and other school activities</li> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology ( including, extra-curricular and extended school activities if relevant)</li> <li>• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws</li> </ul>
All staff	<ul style="list-style-type: none"> <li>• To read, understand and help promote the school’s e-safety policies and guidance</li> <li>• To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy</li> <li>• To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices</li> <li>• To report any suspected misuse or problem to the e-safety coordinator</li> <li>• To maintain an awareness of current e-safety issues and guidance e.g. through CPD</li> <li>• To model safe, responsible and professional behaviours in their own use of technology</li> <li>• To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones, social networking sites, etc.</li> </ul>
Pupils (may not all be relevant to EYFS)	<ul style="list-style-type: none"> <li>• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at EYFS and KS1 it would be expected that parents / carers would sign on behalf of the pupils)</li> <li>• to understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>• to know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations</li> <li>• to know and understand school policy on the use of mobile phones, digital cameras and hand held devices.</li> <li>• To know and understand school policy on the taking / use of images and on cyber-bullying.</li> <li>• To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school</li> </ul>

	<ul style="list-style-type: none"> <li>To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home</li> <li>to help the school in the creation/ review of e-safety policies</li> </ul>
Parents/carers	<ul style="list-style-type: none"> <li>to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images</li> <li>to read, understand and promote the school Pupil Acceptable Use Agreement with their children</li> <li>to access the school website / on-line pupil records in accordance with the relevant school Acceptable Use Agreement.</li> <li>to consult with the school if they have any concerns about their children's use of technology</li> </ul>
External group	<ul style="list-style-type: none"> <li>Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school</li> </ul>

## 1. Teaching and learning

As we move towards a more digital curriculum, we will actively promote the use of 'real-world' technologies to enhance and support learning.

### 1.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils will be taught to recognize the risks of online radicalization, including how extremist groups use social media and gaming platforms to groom young people through 'grievance narratives' and misinformation

### 1.2 Media Literacy and AI

- Pupils will be taught to critically evaluate AI-generated outputs, recognizing that AI can 'hallucinate' (produce false information) or reproduce societal biases found in its training data.
- Education will include recognizing signs of manipulated media (deepfakes) and understanding the safeguarding risks associated with 'nudification' or the malicious creation of AI content to embarrass others

### 1.3 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught the differences between acceptable and unacceptable Internet use and given clear objectives for Internet use.
- The school is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

#### 1.4 Good Practice

- Teachers will update and check websites before accessing with the children to ensure that the content is appropriate. The curriculum is planned in context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. safe search kids or kiddle
- The school makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and the curriculum plans.
- A record is kept of any Cyberbullying or inappropriate behaviour in-line with the school behaviour management system. Parents/carers are informed of significant or repeated inappropriate behaviours
- The school ensures the Designated Safeguarding Lead Professional has appropriate training in Online Safety practice.
- The school provides advice and information on reporting offensive materials, abuse/ bullying etc and makes this available for pupils, staff and parents.
- Online Safety advice for pupils, staff and parents is provided.
- The school ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights.
- The school ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.
- The school makes training on the Online Safety education available to staff
- The school gives advice, guidance and training for parents, including Information leaflets; practical sessions; in school newsletter.

#### 1.5 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Saxon Way has a clear, progressive Online Safety education programme throughout all Key Stages, built on local and national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

- to STOP and THINK before they CLICK
- to discriminate between fact, fiction and opinion;
- to develop a range of strategies to validate and verify information before accepting its accuracy;
- to skim and scan information;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- [for older pupils] to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- [for older pupils] to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- [for older pupils] to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;

- [for older pupils] to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- [for older pupils] to understand why they must not post pictures or videos of others without their permission;
- [for older pupils] to know not to download any files – such as music files - without permission;
- [for older pupils] to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand online purchasing e.g. apps and within app purchases
- [for older pupils] to understand why and how some people will ‘groom’ others with inappropriate or illegal motives

## 2. Managing Internet Access

### 2.1 Information system security

- School ICT systems capacity and security are reviewed regularly.
- Virus protection is updated regularly.

### 2.2 E-mail

- Pupils may only use approved school e-mail accounts on the school system.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- 

### 2.3 Published content and the school web site

- The contact details on the Web site are the school address, e-mail and telephone number. Staff, pupils’ or governors’ personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

### 2.4 Publishing pupil’s images and work

- Photographs that include pupils will not refer to the pupil by full name. Digital images /video of pupils stored in a teacher’s documents or shared images folder on the network are deleted at the end of the year – unless specifically required for a key school publication or assessment information.
- Images of children and staff are not to be taken on or away from school premises by parents or visitors, unless prior permission is sought and given by the school or at scheduled school events such as assemblies or festivals.
- Pupils are not identified by their full name in online photographic materials in the credits of any published school produced video materials / DVDs.
- Parental agreement is obtained, through the consent form signed at point of admission, before pupil’s images are published on the school’s website, social media accounts or other publications e.g. local newspapers.
- Staff should ensure that pictures are removed from mobile phones / personal equipment before they leave the school premises.
- Pupils are taught about how images can be manipulated in their Online Safety education programme and also taught to consider how to publish for a wide range of audiences, which might include governors, parents or younger children.

### 2.5 Social networking and personal publishing (further details available in our Social Networking Policy)

- The school blocks/filters access to social networking sites or newsgroups unless there is a specific, approved educational purpose.

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents are advised that the use of some social network spaces, for example Facebook, Twitter, Instagram, TikTok, Whatsapp outside school is inappropriate for primary aged pupils and that some of these sites have minimum age requirements.
- Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. They are taught the need to keep their data secure and what to do if they are subject to bullying or abuse.

### 2.6 Managing filtering

- The school will work with relevant providers to ensure systems which protect pupils are regularly reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Leader. Concerns are escalated to the Technical service provider as necessary.
- The school will immediately refer any material we suspect is illegal to the appropriate authorities e.g Police, and the local authority.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### 2.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

### 2.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

## 3. Policy Decisions

### 3.1 Authorising Internet access

- The school reserves the right to withdraw Internet access from a pupil or member of staff in the event of misuse or infringement of policy.

### 3.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor GST can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish whether the Online Safety policy is adequate and that its implementation is effective.

### 3.3 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 Head of School.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

### 3.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to Online Safety.

## 4. Communications Policy

### 4.1 Introducing the Online Safety policy to pupils

- Online Safety rules are displayed and are discussed with the pupils on a regular basis.
- Pupils are informed that network and Internet use will be monitored.
- Pupils are not allowed to use mobile phones in school.

### 4.2 Staff and the Online Safety policy

- All staff (including governors) must receive online safety training at induction that covers the expectations and their responsibilities regarding filtering and monitoring.
- The Online Safety Policy is distributed to all staff and is included in child protection training sessions.
- Internet usage is able to be monitored and can be traced to the individual user.
- Discretion and professional conduct is essential.
- Staff may use school-approved AI tools to assist with planning or admin, but must maintain human oversight. All AI-generated content must be fact-checked and reviewed for accuracy and bias before being used in teaching or communications.'
- Staff must not input personal data (pupil names, emails, or sensitive details) into any Generative AI tool. Only anonymized or placeholder data should be used to protect privacy.
- Staff training includes identifying the signs of online radicalization and understanding that extremist content can often be subtle, appearing as memes or 'alternative' news sources.

### 4.3 Enlisting parents' support

Parents/carers' attention will be drawn to the school Online Safety Policy in a variety of ways including: newsletters, open evening events and on the school Web site.

A range of resources and activities are available through:

- CEOP – Child Exploitation and Online Protection
- [http://www.thinkuknow.co.uk/5\\_7/](http://www.thinkuknow.co.uk/5_7/)
- <https://www.thinkuknow.co.uk/Teachers/Lee-And-Kim/>
- [http://www.thinkuknow.co.uk/8\\_10/](http://www.thinkuknow.co.uk/8_10/)
- <https://www.thinkuknow.co.uk/teachers/resources/?tabID=2>
- <https://www.internetmatters.org/>