

Stanborough Primary School & Nursery

E-Safety Policy



Approved by:	Date:
Last reviewed on:	October 2025
Next review due by:	September 2026

1. Introduction

Our school aims to:

- Have robust processes in place to ensure the **online safety (digital safety)** of pupils, staff, volunteers and governors
- Identify and support groups of pupils potentially at greater risk of harm online
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology (including mobile, cloud, AI and smart technology)
- Establish clear mechanisms to identify, intervene in, and escalate an online safety incident, where appropriate

2. The 4 key categories of risk:

Our approach to online safety is based on addressing the following risk categories:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation / disinformation / conspiracy theories, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction, such as peer-to-peer pressure, commercial advertising, adults posing as children / young adults seeking to groom, exploit, coerce
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm (e.g. making/sending/receiving explicit images—including consensual/non-consensual sharing of nudes/semi-nudes—online bullying, harassment, trolling, doxing, influencing others)
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing, financial scams, or exploitation via in-app purchases or subscription traps

3. Legislation, statutory guidance and other references

This policy is based on, and should be read in conjunction with, the following (current as of 2025):

- **Keeping children safe in education 2025** (statutory guidance) [NSPCC Learning+3GOV.UK+3safecic.co.uk+3](#)
- DfE guidance on **meeting filtering and monitoring standards** for schools and colleges [GOV.UK+2GOV.UK+2](#)
- DfE / Government guidance on **teaching online safety in schools** (e.g. via the Education for a Connected World / UK Safer Internet Centre / Internet Matters)
- DfE advice on **Prevent duty / radicalisation / protecting children from extremist content**
- Legislation including, but not limited to: Education Act 1996 (as amended), Education and Inspections Act 2006, Education Act 2011 (on cyberbullying and search powers), Equality Act 2010, Data Protection Act 2018 / UK GDPR, Computer Misuse Act 1990, Communications Act 2003
- Relevant statutory guidance or departmental updates (e.g. changes under the Children's Wellbeing and Schools Bill, or in future versions of KCSIE) [Mondaq+1](#)

4. Roles and responsibilities

(Your original structure is good; here are some suggested updates / expansions.)

4.1 The Governing Board

- The board has overall responsibility for monitoring this policy, ensuring its implementation, and holding the headteacher to account
- It should ensure all staff receive online safety training as part of safeguarding training, and that there are regular updates and refreshers (at least annually)
- The board should coordinate meetings with relevant staff to review online safety, training needs, incident logs, filters/monitoring performance
- It must ensure the school has appropriate filtering and monitoring systems in place (meeting the DfE filtering/monitoring standards) and regularly review their effectiveness with IT staff and providers
- Specifically, the board should ensure the school:
 - Identifies roles and responsibilities for managing filtering/monitoring systems
 - Reviews filtering/monitoring provisions at least annually

- Blocks harmful/inappropriate content without unreasonably affecting teaching and learning
- Implements effective monitoring strategies meeting safeguarding needs

All governors will:

- Read, understand, and approve this policy
- Adhere to the school's acceptable use policy (AUP) for ICT
- Promote online safety as a continuous, integrated theme in the school's safeguarding strategy

4.2 Headteacher

- Ensure staff understand this policy and that it is implemented consistently
- Oversee strong communication and accountability for online safety across staff, pupils, parents
- Ensure that, where needed, safeguarding / online safety provision is adapted for vulnerable pupils, SEND pupils, or those who may need personalised support

4.3 Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for online safety, including:

- Supporting the headteacher in ensuring consistent implementation of this policy
- Leading the annual review of the policy, ensuring it is current and aligned with updated guidance
- Understanding filtering and monitoring systems in place, and working with ICT staff to maintain them
- Managing online safety incidents (in line with the safeguarding policy)
- Logging all e-safety / digital incidents, cyberbullying, etc., and reviewing trends / patterns
- Delivering staff training on online safety, ensuring updates in line with new risks (e.g. AI misuse, emerging platforms)
- Liaising with external agencies (e.g. police, CEOP, internet service providers, safeguarding partners) as needed
- Leading on risk assessments relating to online safety / digital technology
- Providing governance / senior leadership with regular reports on online safety

4.4 ICT / Network Manager / Technicians

- Implement and maintain filtering / monitoring systems according to DfE standards
- Review and update security (antivirus, firewall, patching) regularly
- Monitor network activity, run audits and reports, respond to alerts
- Block access to dangerous sites, prevent downloading or execution of harmful files where possible
- Support logging of incidents (e.g. via CPOMS or equivalent)
- Liaise with DSL / safeguarding team when suspicious or concerning activity is detected

4.5 All Staff, Volunteers, Contractors

- Be aware of and comply with this policy
- Support pupils in acceptable use of technology
- Report any filtering / monitoring failures or suspicious digital behaviour to DSL / IT
- If needing to bypass filtering for education purposes, follow a documented process / get approval
- Collaborate with DSL to log and respond to e-safety incidents appropriately
- Respond to reports of online harassment / sexual violence / harassment (both online and offline) in line with safeguarding procedures

4.6 Parents / Carers

- Raise any concerns about online safety to the school
- Be aware of the SMART / safe usage rules and strategies taught at the school
- Seek further guidance from reputable sources (e.g. Safer Internet Centre, Childnet)

4.7 Visitors / Community Users

- If they use school ICT or network, they must comply with this policy (or a tailored acceptable use statement)
- Be informed (via signage or briefing) about acceptable use rules

5. Why Internet (and Digital Technology) Use is Important

(This section is broadly fine; you may wish to add that digital technology is essential for remote learning, cloud-based platforms, AI-assisted learning, hybrid / blended learning, etc.)

6. Benefits & Enhancements from Internet / Technology Use

- Use of online collaboration tools, safe cloud services, remote access (within controlled and secure environments)
- Use of AI-supported tools (within approved boundaries)
- Secure storage and sharing of curriculum resources
- Enabling pupils to learn about digital citizenship, media literacy, critical thinking

7. Authorised Internet Access / Access Management

- Internet filtering is provided by the school's IT infrastructure / firewall / filtering provider
- Breaches to security must be reported immediately to Headteacher / SLT / Computing Lead
- Keep an up-to-date record of all staff, pupils (and their access levels)
- Remove access for staff / pupils who leave (ideally immediately or within a defined period)
- All staff and pupils must read and sign the Acceptable Use Agreement (AUP) before using school ICT resources
- Pupils should comply with a "Responsible Internet Use" statement
- For remote access / home use, ensure that acceptable use and security requirements apply (e.g. VPN, device security, same filtering rules where feasible)

8. World Wide Web / Browsing

- If staff / pupils discover unsuitable sites (or content), they must report the URL, time, content, to e-safety leads / IT
- Pupils should be taught to critically evaluate sources, cross-check accuracy, detect bias, misinformation, etc.
- Use safe search settings on search engines / browsers

9. Email / Messaging / Communication

- Pupils may only use approved school email accounts / internal systems
- Personal details (addresses, phone numbers, etc.) must not be shared
- Offensive / suspicious emails must be reported immediately
- External email access may be restricted / filtered
- Staff should use their school email for all school communication; their personal emails should not be used or disclosed without permission
- Be cautious with forwarding, attachments, phishing-style messages

10. Acceptable Use of the Internet / Devices

- All users (pupils, staff, volunteers, governors, visitors) sign an AUP
- Use of the school's network / internet must be for education / role-related purposes
- Monitoring of usage will be in place and users should expect their activity to be visible
- For staff devices used off-site:
 - Devices should be password-protected with strong passwords / passphrases
 - Hard drives or storage should be encrypted (using supported, current encryption)
 - Devices should lock automatically after inactivity

- Do not share work devices with others
- Anti-virus and anti-malware should be installed and routinely updated
- Operating systems, applications, firmware, security patches to be kept up to date
- Work devices are for professional use; excessive personal use should be avoided
- If a staff member suspects a breach or compromise, they must inform the ICT manager / DSL immediately

11. Social Networking / Web 2.0 / Apps

- The school should block or filter access to social networking / newsgroups unless explicitly approved for educational purposes
- Pupils should not share identifying personal information or location details
- Pupils should be taught safe use of social networks (privacy settings, nicknames, avatars)
- Staff must not “friend” or follow pupils via personal social media accounts
- Any school-business communications via social media should be on official school accounts, with appropriate oversight
- Guidance should be given to parents / carers about safe social media practices

12. Filtering / Monitoring

- The network / IT manager must ensure filtering systems are effective, in line with DfE filtering and monitoring standards [GOV.UK+1](#)
- Downloaded files, email attachments, removable media should be virus-checked before opening
- If a virus or suspicious file is suspected, stop use and notify the IT manager
- If users discover unsuitable content, they must report it to the e-safety lead or network manager
- Monitoring should include both manual supervision and technical monitoring (alerts, logs)
- Monitoring systems should provide alerts/reports for high-risk behaviour (e.g. searches for extremist material, self-harm, harassment)
- The monitoring plan should define thresholds for alerts, investigation, escalation
- Monitoring systems should not technically restrict all content but should enable review and action (i.e. be reactive as well as preventative)
- A **Data Protection Impact Assessment (DPIA)** should be conducted for the monitoring/filtering tools, and privacy notices reviewed (e.g. in line with ICO guidance) [GOV.UK+1](#)

13. Managing Emerging Technologies

- Emerging technologies (e.g. new apps, VR, AR, chatbots, AI, IoT devices) should be risk assessed by senior management before introduction
- Mobile phones / devices: pupils may be required to hand in personal phones during the school day (or follow a set policy)
- Pupils must not use phones for inappropriate purposes (e.g. bullying, harassment)
- School devices (laptops, Chromebooks) are for educational use; pupils should not install unauthorized software or apps
- Staff / pupils discovering unusual or concerning apps / content should report to e-safety lead / IT
- **AI / generative tools:**
 - Recognise that AI has educational potential but also risks (e.g. deepfakes, plagiarism, misinformation, misuse to bully)
 - The school will define a policy for acceptable AI use (which tools, for what purposes, approval process)
 - Staff should carry out risk assessments for new AI tools, and training should be provided
 - Misuse of AI in bullying, impersonation, generation of harmful content will be treated under behaviour / safeguarding policies

14. Published Content / School Website

- Published contact details should be limited to school address, generic email, telephone
- Staff / pupils’ personal data will not be published

- The IT manager or a nominated staff member takes overall responsibility for the website content, ensuring it is accurate and appropriate.

15. Publishing Pupils' Work / Images

- On pupil admission, parents / carers are asked for consent for use of images / work (with clear explanation of purpose)
- Parents must give explicit consent for use in newspapers, blogs or external media
- Consent may be withdrawn in writing at any time
- Pupils' full names should not be used alongside photographs on websites / blogs
- Permission is required for any pupil image publication
- For events (sports day, concerts) parents may take photographs strictly for personal use; publishing on social media / web should follow school policy

16. Information Systems Security

- ICT systems capacity and security should be reviewed regularly
- Anti-virus, firewalls, intrusion detection, patches, backups, controls must be maintained
- All devices (school-owned and brought-in) are subject to the school's security policy
- Bring-your-own devices (BYOD) must meet minimum security standards and will be subject to the same acceptable use / filtering rules while connected

17. Protecting Personal Data

- All personal data must be handled in accordance with **Data Protection Act 2018 / UK GDPR** (not DPA 1998)
- Data should be encrypted in transit and at rest, particularly on removable media / portable devices
- Use approved, secure systems for data storage / transfer
- Memory sticks / removable media must be encrypted (using supported tools) and used only when necessary
- The school should maintain a data protection / privacy policy, privacy notices, and ensure compliance with ICO guidance

18. Assessing Risks / Risk Assessment

- The school should take all reasonable precautions to prevent access to inappropriate content
- The ICT / network manager will audit usage / logs to assess whether the e-safety policy is adequate
- The school will educate pupils about cyberbullying, online harassment, and how to report it
- Staff, governors, volunteers should receive training on cyberbullying and supporting pupils
- In incidents of cyberbullying, follow the school's behaviour / safeguarding policies
- If illegal or harmful material is spread, the school should act to contain it, escalate, and provide evidence to the police / safeguarding partners as required
- The DSL should maintain and review a digital / online safety risk assessment annually (or more often), responding to new threats or changes in technology

19. Handling E-Safety / Online Complaints

- Complaints about Internet misuse should be referred to a senior staff member
- Complaints about staff misuse go to the headteacher
- Complaints of a safeguarding nature must follow the school's child protection policy
- Pupils, parents should know how to lodge complaints, and the consequences for misuse should be clearly stated

20. Communication of Policy

20.1 Pupils

- Internet / digital rules should be displayed in classrooms / shared widely
- All pupils (Years 1–6) sign an acceptable use agreement
- Pupils should be informed that use will be monitored
- Pupils should be taught the **SMART / safe usage rules** (safe, meeting, accepting, reliable, tell)
- Report online abuse via appropriate routes (e.g. smooth wall, CPOMs)

20.2 Staff

- All staff receive this policy and its implications explained
- All staff sign an acceptable use agreement
- Staff should be aware their Internet / device usage may be monitored

20.3 Parents / Carers

- The policy is shared via newsletters, blogs, school website, induction packs
- The E-Safety Lead shares updates / tips (for example via National Online Safety or similar)
- Parents are informed of the SMART rules taught to pupils
- Provide parents with 10 or more safety rules / guidance

21. Monitoring, Incident Logging, Review

- The DSL or Headteacher logs all safeguarding / online safety related incidents
- Maintain an “incident log” (e.g. Appendix) including date, nature, action, outcome
- The policy is reviewed annually (or sooner if needed), and shared with governors
- The review should include an updated risk assessment reflecting evolving technology and threats

22. Links with other policies

This online safety policy is linked to / should be consistent with:

- Child protection & safeguarding policy
- Behaviour / anti-bullying policy
- Staff disciplinary procedures
- Data protection / privacy policy / privacy notices
- Complaints procedure
- Acceptable use agreements (pupils, staff, visitors)
- Artificial Intelligence / Use of AI policy

Appendices

1. KS1 Acceptable Use Agreement
2. KS2 Acceptable Use Agreement
3. Staff / Governors / Volunteers / Visitors Acceptable Use Agreement
4. E-Safety Rules / SMART rules (updated for 2025)
5. Think then Click / other pupil guidance
6. Respecting / caring for the school community when taking photos / video
7. Guide to Use of Images (privacy, consent, cropping, storage)
8. Incident Log Template
9. AI / Generative Tools Use Guidance (if needed)
10. Filtering / Monitoring Roles & Checklist (aligned to DfE standards)

Appendix 1: EYFS and KS1 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 I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I select a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carers
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carers agreement: I agree that my child can use the school'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 will make sure my child understands these.

Signed (parent/carers):

Date:

Appendix 2: KS2 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:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers/laptops) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, clubs or other activities organised by the school, 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 agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school'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 3: Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school'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, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

- I will only use the school's 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 will monitor the websites I visit and my use of the school's ICT facilities and systems.
- 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:

Key Stage 1

Think then Click	
These rules help us to stay safe on the Internet	
	We only use the internet when an adult is with us
	We can click on the buttons or links when we know what they do.
	We can search the Internet with an adult.
	We always ask if we get lost on the Internet.
	We can send and open emails together.
	We can write polite and friendly emails to people that we know.
B. Stoneham & J. Barrett	

Key Stage 2

Think then Click
e-Safety Rules for Key Stage 2
• We ask permission before using the Internet. • We only use websites that an adult has chosen. • We tell an adult if we see anything we are uncomfortable with. • We immediately close any webpage we are not sure about. • We only e-mail people a teacher has approved. • We send e-mails that are polite and friendly. • We never give out personal information or passwords. • We do not open e-mails sent by anyone we don't know. • We do not use Internet chat rooms.

E-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any unauthorised person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.



Stanborough Primary School



Respecting and Caring for the Whole School Community when taking Photos and Video

online. This is to protect all members of the school community

We are happy for
parents and carers to
take photos and video
of the school
production for
personal use on
condition that these
images are not
distributed or put



Thank you for your support





Stanborough Primary and Nursery School

Guide to the use of

Images

**Respecting and Caring
for the
Whole School Community**



Using Images Safely and Responsibly

We all enjoy and treasure images of our family and friends.
Our new born baby, first steps, family events, holidays and

school events are moments we all like to capture in photos or on video.

We then have the added and exciting dimension of adding our images and video to our social network, such as Facebook, YouTube and many other online websites. This means that we can easily share our photos and video with family and friends.

Whilst this is naturally useful, in schools and educational settings we do need to protect and safeguard all children and staff in our school, including those who do not want to have their images stored online.

Online Images and Video

What should we think about before adding online any images or video? Are there any risks?

Facts

- Once online any image or video can be copied and stay online forever.
- Some children are at risk and MUST NOT have their image put online. Not all members of the school community will know who they are.
- Some people do not want their images online for personal or religious reasons.
- Some children and staff may have a complex family background which means that image sharing online can have unforeseen consequences.

We must all **'Think Before We Post' Online**

At Stanborough Primary and Nursery School we are happy for parents and carers to take photos and video of the school production for personal use on condition that these images are not distributed or put online. This is to protect all members of the school community

Thank you for your support

Further Information on the Use of Images and video can be found:

☺ **Be Safe Online**

<http://tinyurl.com/ye24kxe>

☺ **Information Commissioner's Office**

<http://tinyurl.com/yc7nmnv>

☺ **ThinkUknow**

<http://www.thinkuknow.co.uk/parents/safeuse/>

Developed by the
Hertfordshire Schools' eSafety Team

**CLICK CLEVER
CLICK SAFE**