Online safety and social media policy

Key statutory guidance	The DfE's latest 'Keeping Children Safe in Education' and 'Teaching online safety in schools' guidance
Independent school standards	Paragraphs 7 and 34.
Last updated by senior leaders	September 2025
Last reviewed by advisory board	September 2025
Next review due	September 2026

Aims

St. John's Prep and Senior School:

- believes that online safety (e-safety) is an essential element of safeguarding pupils and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

- has a duty to provide the school community with quality internet access to raise education standards, promote pupil achievement, support the professional work of staff and enhance the school's management functions.

- has robust processes in place to ensure the online safety of pupils, staff, volunteers and visitors.

- delivers an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.

- identifies that the internet and information communication technologies are an important part of everyday life so pupils must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Protecting children from radicalisation (the Prevent Duty)
- Generative artificial intelligence (AI) in education

Associated policies

This policy must be considered alongside and in conjunction with:

- Safeguarding and child protection policy
- Data protection (GDPR) policy
- Anti-bullying policy
- Behaviour policy
- Relationships and sex education policy
- Artificial Intelligence (AI) policy.

Roles and responsibilities

The principal

The principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead (DSL)

The DSL takes lead responsibility for online safety in school, including in the following ways.

- Supporting the Principal and Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on HUBmis and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour policy
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.

The ICT Manager

The ICT manager is responsible for the following.

- Putting in place appropriate filtering and monitoring systems (Smoothwall), which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems monthly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on HUBmis and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

Staff

All staff (including any contractors, agency staff and volunteers) are responsible for:

- maintaining an understanding of this policy
- implementing this policy consistently
- agreeing and adhering to the terms on acceptable use of the School's ICT systems and the internet (appendix 2), and ensuring that pupils follow the School's terms on acceptable use (appendix 1)
- working with the DSL to ensure that any online safety incidents are logged on HUBmis and dealt with appropriately in line with this policy.
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School Behaviour Policy.

Parents and carers

- Parents are expected to ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1).

- Parents may seek further guidance on keeping children safe online from the following organisations and websites:

  What are the issues? - UK Safer Internet Centre
  Hot topics - Childnet International
  Parent factsheet - Childnet International
  Healthy relationships – Disrespect Nobody

- Parents are expected to notify a member of staff or the Principal (Prep.) or headteacher (Senior) of any concerns or queries regarding this policy.

Visitors

- Visitors who use the School's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Educating pupils about online safety

Pupils are taught about online safety as part of the computing curriculum:

In Key Stage 1, pupils are taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 are taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact.

In Key Stage 3, pupils are taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in Key Stage 4 are taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

Teaching pupils about the safe use of technology is within the computing and PSHE education curriculum and pupils are taught about online safety and risks as part of our whole-school approach.

Managing and monitoring information systems

St. John's Prep and Senior school is responsible for ensuring the personal safety of staff and pupils when using the IT systems. The IT systems are reviewed regularly in order to ensure the security of the school's systems.

- All servers are secure and up to date (Operating Systems).
- All workstations are kept up to date and secured with the latest virus protection.
- All servers are secured, and access is restricted.
- All data held on the school system is regularly backed up.
- All software is checked and tested before installation.
- All software must be from legitimate sources and providers.
- All portable devices must be used in accordance with the IT acceptable use policy.
- All members of staff will have their own unique username and private passwords to access St. John's Prep and Senior School systems. Staff are responsible for keeping their password private and changing them regularly.
- From Year 1, all pupils are provided with their own unique username and private passwords to access St. John's Prep and Senior School systems. Pupils are responsible for keeping their password private.

- We require staff and pupils to use strong passwords for access into our system.

Filtering and monitoring the internet

- St. John's Prep and Senior school uses filtering software to safeguard the staff and pupils, monitoring the internet usage with a system called Smoothwall. Smoothwall sends daily and weekly reports to the IT team, showing internet usage and summarizing and identifying any activity that is in contradiction with this policy and the acceptable user agreement. This will allow the IT team to identify the user/s and act accordingly.

- All web traffic is monitored and suitable black/whitelists have been created without 'over blocking' the users. However, St. John's Prep and Senior School are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

- All network access points are password protected and the password is changed bi-annually.

Email

- We require staff and pupils to use strong passwords for access into our system.

- Pupils may only use St. John's Prep and Senior School provided email accounts for educational purposes.

- All staff are provided with a specific St. John's Prep and Senior School email address to use for any official communication.

- The use of personal email addresses by staff for any official St. John's Prep and Senior School business is not permitted.

- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and/or encrypted methods.

- Members of the St. John's Prep and Senior School community must immediately tell a senior leader if they receive an offensive communication.

- Sensitive or personal information will only be shared via email in accordance with Data Protection (GDPR) legislation.

- Access in St. John's Prep and Senior School to external personal email accounts may be blocked.

- St. John's Prep and Senior School email addresses and other official contact details will not be used for setting up personal social media accounts or subscribing to services.

Mobile devices including phones

- For guidance on pupils' use of mobile devices, please refer to our separate mobile devices policy.

- Members of staff are not permitted to use their own personal phones or devices for contacting pupils, young people and their families within or outside of St. John's Prep and Senior school in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with the Principal or Headteacher.

- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose, where consent has been given by parents.

Images and video

- St. John's Prep and Senior School will ensure that all images are used in accordance with St. John's Prep and Senior School's photographic image use policy.

- An up-to-date record of all permissions is checked before any digital images or video are captured.

- In line with St. John's Prep and Senior School's photographic image policy, written permission from parents will always be obtained before images/videos of pupils are electronically published.

Managing online incidents and concerns

- All members of the St. John's Prep and Senior School community will be informed about the procedure for reporting online safety (e-safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.). These will be logged on HUBmis.

- The DSL (or a Deputy) will be informed of any online safety (e-safety) incidents involving child protection concerns, which will then be recorded.

- The DSL (or a Deputy) will investigate the concern, and ensure that they are escalated and reported to relevant agencies in line with the Enfield Safeguarding Children Partnership thresholds and procedures, as appropriate.

- St. John's Prep and Senior School will manage online safety incidents in accordance with the School's behaviour and/or anti-bullying policies where appropriate.

- Where there is cause for concern or fear that illegal activity has taken place or is taking place then St. John's Prep and Senior School will contact the Enfield Education Safeguarding Team or the police via 999, if there is immediate danger or risk of harm.

- The use of computer systems without permission, or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the police.

- If St. John's Prep and Senior School is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Local Authority's Designated Officer (LADO).

Social media including safeguarding issues such as sexting, online harassment and the sending of nudes/semi-nudes

- For many years, online-safety messages have focused on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced.

- Examples of dangers include sexting (see below), the sharing of violent and sexual videos, self-harm materials, coerced nudity via live streaming, cyber bullying, peer-on-peer sexual exploitation, child criminal exploitation and radicalisation.

- Sexting is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. Any incidents that arise will be dealt with according to current school policies and UKCCIS: Sexting Guidance (March 2024)

- The seriousness of the dangers, including in light of the submissions to the *Everyone's Invited* website, was highlighted in Ofsted's review of sexual abuse. We ensure that consent, sexual harassment and the law, implications and dangers of sharing explicit imagery, all receive suitable curriculum coverage.

- Any incidents will be immediately reported to the DSL or a Deputy and will be managed in line with the school's safeguarding and child protection policy and the guidance above.

Pupils' use of social media

- Safe and responsible use of social media is outlined for pupils and their parents as part of St. John's Prep and Senior School's Acceptable User Agreement (Appendix 1).
- Any concerns regarding pupils' use of social networking, social media and/or personal publishing sites, both at home and at St. John's Prep and Senior School, will be dealt with in accordance with existing policies.
- Any concerns that arise must be reported to the DSL or a Deputy.

Official use of social media

- The school makes official use of Instagram and Facebook, with clear educational, parental and community engagement objectives in mind.

Appendix 1

Acceptable Use Agreement: Pupils – Online Safety Rules

When using the School's ICT facilities and accessing the internet:

- I will only use ICT in School for educational purposes.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible. I will be kind and respectful at all times.
- I will not deliberately look for, save, or send anything that could be unpleasant or nasty. If I accidently find anything like this, I will tell my teacher immediately.
- I will not give out my own details, such as my name, telephone number, or home address. I will not arrange to meet someone offline.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I understand that the School will monitor the websites I visit and my use of the School's ICT facilities and systems and that my parent/carer contacted if a member of School staff is concerned about my online safety.
- I will ensure that my online activity including the use of social media/networking sites, both in School and outside School, will adhere to the School rules.
- I will ensure that I do not use any electronic device to bully, take inappropriate images or send inappropriate images.
- I understand that the School can sanction me if I do certain unacceptable things online, even if I am not in School when I do them.
- I will only use Artificial Intelligence (AI) tools if my teacher gives permission, and I will never pass off AI work as my own.
- If I use AI to help with my work, I will make it clear what I have used and always check that it is correct.

Dear Parents and Carers,

ICT including the internet, email and mobile technologies, etc. is an important part of learning in our School.

We expect all pupils to be safe and responsible when using any ICT.

The School is proud of its high standards and ethos. The internet and social media should not be used to share complaints about the School. When negative or inaccurate comments online are drawn to our attention, we will invite the person to discuss their concerns with the School by following our complaints procedure.

Please read and discuss these Online Safety rules with your child and sign the bottom of the page. If you have any concerns or would like some explanation, please contact the ICT Department.

We have discussed this and _____ (**your child's name**) agrees to follow the Online Safety rules and to support the safe use of ICT at St. John's School.

Parent/Carer Signature _____ **Date** _____

Appendix 2

Acceptable Use Agreement: Staff – Online Safety Rules

Name of staff member/volunteer/visitor:_____

When using the School's ICT facilities 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 a senior leader 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 Artificial Intelligence (AI) tools for educational or administrative purposes, and always in line with the School's AI Policy.
- I will check and take responsibility for any AI-generated content I use, ensuring it is accurate, appropriate, and clearly distinguished from my own professional work.

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 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

GDPR - Photograph Consent Form

Name of child:_____

Occasionally, we may take photographs of the pupils at our school. We may use these images as part of our school displays and sometimes in our school's prospectus or in other printed publications that we produce. We will also use them on our school website, Instagram and Facebook page. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption. If we name a pupil in the text, we will not use a photograph of that child to accompany the article. If a child has won an award and the parent would like the name of their child to accompany their picture, we will obtain permission from the parent before using the image.

From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high-profile event. Pupils will often appear in these images, which may appear in local or national newspapers, approved websites or on televised news programmes. To comply with the General Data Protection Regulations (GDPR), we need your permission before we can photograph or make any recordings of your child. Please answer the questions below, then sign and date the form where shown and return the completed form to the school office.

Please circle your answer

1. May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional and marketing purposes? Yes No
2. May we use your child's image on our School Website (In-house maintained)? Yes No
3. May we use your child's work on our School Website (In-house maintained)? Yes No
4. May we use your child's image on our Social Media accounts (In-house maintained)? Yes No
5. May we use your child's work on our Social Media accounts (In-house maintained)? Yes No
6. Do you consent to your child's image being published with a press photograph? Yes No

Please note:

Conditions for use of these photographs are on the back of this form. I have read and understood the conditions of use on the back of this form.

Signature: ……(**Parent/Carer) Date**: ……...

Parent/Carer Name……

Conditions of School Use:

This form is valid indefinitely from the date you sign it. It is your responsibility to let us know if you want to change or withdraw your agreement at any time.

- We will not re-use any photographs or recordings a year after your child leaves this school. Historic photographs will remain on our school website and social media feeds.

- We, the school, will not use the personal details or full names (which means first name and surname) of any child in a photographic image on video, on our website, in our school prospectus or in any of our printed publications.

- We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.

- If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption, unless we have your agreement.

- If we name a pupil in the text, we will not use a photograph of that child to accompany the article.

- We may include pictures of pupils and teachers that have been drawn by the pupils.

- We may include, if selected, work from pupils.

- We may use group or class photographs or footage with very general labels, such as “a Science lesson” or “making Christmas cakes”.

- We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

- Websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

- Parents’ consent will be recorded on the school’s Management Information System and will be retained no longer than is necessary for the purpose the data was obtained for. The paper copy will be retained on school file up to a year after your child leaves this school.

- As the child’s parents, you agree that if you take photographs or video recordings of your child/ren which include other pupils, you will use these for personal and family use only and you will not post on any personal social media accounts. You understand that where consent has not been obtained from the other parents for any other use, you would be in breach of the Data Protection Act 1998 if you used the recordings for any wider purpose.