SEVENOAKS
PREPARATORY SCHOOL

Online and E Safety Policy

Status and Review Cycle	Statutory / Annual
Policy reviewed and amended	February 2025
Next review date	August 2025
Governor Lead	Mrs Jan Berry jan.berry@theprep.org.uk
Policy Holder	Mrs Helen Cook helen.cook@theprep.org.uk 01732 764829

1. Aims and Objectives

It is the duty of Sevenoaks Prep School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft. Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It is linked to the following school policies:

- Child Protection & Safeguarding Policy
- Prevent Strategy
- Staff Code of Conduct;
- Behaviour Policy;
- Anti-bullying Policy
- Data Protection Policy and Privacy Notice/s;
- PSHE Policy;
- RSE Policy
- Acceptable Use of AI

The policy aims to ensure that the school:

- follows the statutory guidance related to online safety in Keeping Children Safe in Education
- promotes a culture which incorporates the principles of online safety across all aspects of school life.
- pupils and staff are as clear about what is expected of them online as they are offline.
- pupils and staff, both in and out of school, are responsible users of technology for educational, personal and recreational use
- protects pupils from potential risks in their use of technology and educates them to understand risks online, including methods used to bully, groom, abuse or radicalise

- has technical provision and safeguards in place, to filter and monitor inappropriate content and which alert the school to safeguarding issues, that are fit for purpose and robust
- has IT systems which are protected from accidental or deliberate misuse that could put the security of the systems at risk
- adheres to Data Protection requirements.
- has clear reporting mechanisms available for all users to report issues and concerns to the school
- informs and provides guidance to parents/carers about use of digital technology and online safety

At Sevenoaks Prep, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

1. Scope

This policy applies to all members of the school community, including staff, pupils (including those in the EYFS), parents and visitors, who have access to and are users of the school IT systems. In this policy:

- “staff” includes teaching and non-teaching staff, governors, and volunteers;
- “parents” includes pupils' carers and guardians; and
- “visitors” includes anyone else who comes to the school.

Both this policy, and the Acceptable Use policies, cover all forms of technology and digital devices both fixed and mobile. This includes but is not limited to internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, wearable devices etc.).

The school will deal with any e-safety incidents in accordance with the procedures outlined in this policy and associated school policies.

Any data protection breaches will be dealt with in accordance with the procedures outlined in the Data Protection policy.

3. Risks

In designing this policy, the school has considered the “*4Cs*” outlined in KCSIE as the key areas of risk.

content: being exposed to illegal, inappropriate or harmful material; e.g. pornography, fake news, hate speech, racism, misogyny, self-harm, suicide or radical and extremist views.

contact: being subjected to harmful online interaction with other users e.g: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: personal online behaviour that increases the likelihood of, or causes, harm, e.g. making, sending and receiving explicit images, or online bullying (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography).

commerce: online gambling, inappropriate advertising, phishing and or financial scams

Adults are at similar risk to those for children.

Staff must also understand how to keep data safe by following the Data Protection Policy and be aware of the prevalence of phishing and malware websites and e-mails.

The school recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology.
The improper use of mobile technology by pupils, whether this occurs in or out of school, will be dealt with under the school's Behaviour Policy and / or Safeguarding and Child Protection Policy as is appropriate in the circumstances. The improper use of mobile technology by staff will be dealt with under staff disciplinary procedures and Part 4 of KCSIE, as appropriate.

4. Roles and responsibilities in relation to online safety

All staff, governors and visitors have a responsibility to follow the school's Safeguarding and Child Protection policy in order to protect children from all forms of abuse and make appropriate referrals. The following roles and responsibilities must be read in conjunction with the Safeguarding and Child Protection Policy.

4.1 The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy.
Governors will ensure that:

- the school keeps up to date with emerging risks and threats through technology use
- the school provides regular updates to the Board about risks and any incidents
- pupils are educated on all aspects of online safety appropriate to their age
- data protection awareness and training is provided so all staff are alert to the need to protect personal data processed by the school

- Staff training, both at induction and with updates at regular intervals, ensures that:
- all staff, in particular the DSL and Senior Leadership Team are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

The Governing Body ensures that that filtering and monitoring provision is reviewed at least once every academic year. The review is conducted by members of the SLT, the DSL, IT support and the Safeguarding Governor. The review is conducted in line with the requirements outlined in 'Meeting digital and technology standards in schools and colleges' (updated January 2025)
The Governing Body is responsible for the review and approval of this policy, at least annually.

4.2 Headteacher

The Headteacher has overall responsible for the safety of all members of the school community, and this includes responsibility for online safety. He is responsible for

- procuring appropriate filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of the filtering and monitoring provisions

- overseeing reports,
- ensuring e-safety and data protection training throughout the school is appropriate for the recipients, e.g. all staff, the SLT, the DSL and parents
- ensuring pupils are appropriately educated on online safety
- ensuring all e-safety and data protection incidents are reported promptly and dealt with appropriately
- reporting to the Board of Governors on all online safety matters
- ensuring this policy is reviewed at least annually, covers all aspects of current technology use and is effective in monitoring and managing any e-safety incidents

4.3 The Designated Safeguarding Lead (DSL)

The DSL for Sevenoaks Prep School is Helen Cook (helen.cook@theprep.org.uk).
The DSL takes the lead responsibility for Safeguarding and Child protection at Sevenoaks Prep School. This includes a responsibility for online safety as well as the school's filtering and monitoring system.
The DSL will:

- ensure that this policy is upheld at all times, working with the Headteacher and Senior Leadership Team and IT staff to achieve this.
- work closely with the school's IT manager and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced.
- review filtering and monitoring reports to ensure they are being triaged and responded to appropriately
- ensure that termly checks are made of the system
- report any breaches or inappropriate activity to the Headteacher without delay
- make the initial response to the receipt of any report that relates to inappropriate activity that has taken place online
- conduct a review of filtering and monitoring systems at least annually in conjunction with IT staff

4.4 Online Safety Coordinator

The DSL has delegated day to day responsibilities relating to online safety to two of the DDSL's, Kevin Eyres and Laura Young. They are required to keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures.
The Online Safety Coordinator shares any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the DSL immediately.
[Are they also responsible for approving/not approving content or is that the DSL? You have said the Head documents this but who makes the decisions?]

4.5 IT staff

The school's IT staff have a key role in maintaining a safe technical infrastructure at the school. They are responsible for:

- keeping abreast with the rapid succession of technical developments, including emerging risks and threats.
- the security of the school's hardware system which will include as a minimum:
  - anti-virus is fit-for-purpose, up to date and applied to all capable devices
  - system updates are regularly monitored and devices updated as appropriate
  - any e-safety technical solutions such as Internet filtering are operating correctly
  - filtering levels are applied appropriately and according to the age of the user
  - categories of use are discussed and agreed with the DSL and Head
  - passwords are applied correctly to all users regardless of age
  - ensuring that all devices taken off-site are sufficiently encrypted, and password protected

    - the security of data
- for training the school's teaching and administrative staff in the use of IT.
- monitoring the use of the internet and emails, maintaining content filters, and reporting inappropriate usage to the DDSLs for Online Safety. [How is this determined? It is likely that the IT staff get tens if not hundreds of alerts per day – how do they triage these? How are these monitored and what criteria are in place for them to decide what must be reported to the DSL/DDSLs? This aspect is a crucial part of monitoring the effectiveness of the systems.]

4.6 Teaching and support staff

As with all issues of safety at the school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise.

All staff are required to:

- sign and return the staff IT Acceptable Use Policy before accessing the school's systems
- read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL, the Headteacher and the Senior Leadership Team.
- understand and ensure pupils follow the Pupil's Acceptable Use Policy
- embed safe and responsible usage of digital technology in all aspects of the curriculum and other school activities
- act as good role models for the pupils in their use of digital technology
- report any suspected misuse, problem or e-safety incident to the school's Online Safety Officer or Designated Safeguarding Lead (DSL) immediately.
- report any data breach is immediately reported in accordance with the Data Protection Policy

4.7 Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy. This includes understanding the importance of reporting abuse, misuse or access to inappropriate materials and to know how to report concerns to any member of the teaching staff.

Pupils are also expected to follow the policy in their online behaviour outside school.

4.8 Parents and carers

Sevenoaks Prep School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges discussion evenings for parents with either our own designated member of online safety staff or an outside specialist. These sessions advise about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

Parents will be encouraged to support the school by

- promoting good online safety practice
- following the guidelines on safe and appropriate use of technology
- attending information events on IT
- supporting and endorsing the guidance set out in the pupils' acceptable use policy.

5. Filtering and Monitoring

Sevenoaks Prep School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements, and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video. Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The DDSLs with responsibility for Online Safety will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. At least annually, the Safeguarding governor, the DSL and Online Safety DDSLs will review the filtering and monitoring system, looking at the records of the checks. The review will usually occur before the beginning of every new academic year, however such reviews will also take place if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult content.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals be identified. In line with the school's Data Protection Policy, IT Staff and the DDSLs will monitor the logs.

Any incidents will be acted upon and recorded. If there is a safeguarding concern, this must be reported to the DSL immediately. Teaching staff must notify the Safeguarding Team, their respective Assistant Head of Key Stage and the Head if they are teaching material which might generate unusual internet traffic activity.

Sevenoaks Prep's education broadband connectivity is provided through Tecwork Ltd using Gamma leased line and Gigaclear for backup FTTP connectivity. Sevenoaks Prep uses Fortinet, Lightspeed and Senso.Cloud for filtering and monitoring.

- Gamma, Fortinet, Lightspeed, Senso are all members of Internet Watch Foundation (IWF).
- Lightspeed has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)

- Lightspeed and Fortinet is blocking access to illegal content including child sexual abuse material (CSAM).

- Lightspeed and Fortinet blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.

We filter internet use on all school owned, or provided, internet enabled devices and networks. This is achieved by:

- On device filtering using Lightspeed Filter to filter all internet traffic on the device as it is accessed, including whilst off site.

- Network level filtering using Fortinet filtering.

- Our filtering system is operational, up to date and is applied to all users, including guest accounts, all school owned devices and networks, and all devices using the school broadband connection.

- We work with Lightspeed and Fortinet and our IT service providers/staff to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

- If there is failure in the software or abuse of the system, for example if pupils or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to:

- Report the concern immediately to a member of staff and turn off the monitor.

Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and behaviour policies.

Parents/carers will be informed of filtering breaches involving their child.

Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), Kent Police, NCA-CEOP or Kent Integrated Children’s Services via the Kent Integrated Children’s Services Portal.

If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or leadership team.

5.1 Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify their respective Assistant Head of Key Stage and the DSL if they believe that appropriate teaching materials are being blocked.

5.2 Pupils:

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the appropriate teacher. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.
Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact the relevant member of teaching staff, who will then contact the DSL to discuss if unblocking the site is appropriate or not.

6. Education and training

6.1 Staff: awareness and training
As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This includes training on this Online Safety Policy.
All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school.

All teaching staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff and contractors receive information about Online Safety as part of their safeguarding briefing on arrival at school.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding and Child Protection Policy, any concerns relating to online safety must be made by staff as soon as possible to the DSL and recorded on CPOMS.

If staff find inappropriate images stored on any device they should follow the procedures below

- the device involved should be confiscated and set to flight mode or, if this is not possible, it should be turned off.
- Staff must not view images, look for further images, copy or print any images or forward images by email or any other electronic means. This is particularly important if images involving 'nudes' or 'semi-nudes' are found, as to do so is a criminal offence.
- If the imagery has already been viewed by accident (e.g. if a pupil has shown it to a member of staff before he/she could ask them not to), this must be reported to the DSL immediately.
- Do not delete the imagery or ask the pupil to delete it.

- Do not ask the pupil(s) involved in the incident to disclose information regarding the imagery. Do not share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any pupil(s) involved.
- Do explain that you need to report it and reassure them that they will receive support and help. Report the matter to the DSL immediately

6.2 Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis. The school continually looks for new opportunities to promote online safety and regularly monitors and assesses pupils' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school is also be carried out via PSHE and RSE lessons, by presentations in assemblies, as well as informally when opportunities arise.

From Year 3 pupils are formally taught - at an age-appropriate level - about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. This is repeated yearly and adapted to be age appropriate. Pupils can report concerns to the DSL or to any member of staff at the school.

From Year 3, pupils are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils are made aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding and Child Protection / Anti Bullying / Behaviour Policies, which describe the preventative measures and the procedures that are followed when the school discovers cases of bullying or other unacceptable online behaviour). Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

In the Pre-Prep there are internet safety posters around the school as well as posters of the safeguarding team. Children in the Pre-Prep are encouraged to talk to their class teacher if they have any concerns or any other adult on duty if it is not their class teacher.

In Prep (Years 3-8), there is a page dedicated to online safety in each bi-weekly school newsletter and there are posters of the safeguarding team in each classroom.

7. Use of school and personal devices

7.1 Staff (also see Safeguarding and Child Protection Policy, Acceptable Use Policy, Mobile and Devices Policy and the Staff Code of Conduct.)

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are referred to the Staff Code of Conduct and Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Sevenoaks Prep are permitted to bring in personal devices for their own use. They may use such devices in designated areas, away from children and pupils, and only during break-times and lunchtimes or at times when they are not teaching and there are no children present.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on their personal devices.

7.2 Pupils

If pupils bring in mobile devices (e.g. for use during the journey to and from school), they must be handed in to Reception at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology. Parents/guardians are advised to install filtering and monitoring software on their child's devices.

School mobile technologies made available for pupil use by the school including laptops, tablets, cameras, etc. are stored in a locked cupboard. Access is available via members of staff only. Members of staff should sign devices out and in before and after each use by a pupil. In Years 3-5, pupils are assigned devices where possible, where this is not possible, staff will create a list of which child uses which device for tracking and monitoring purposes. Years 6, 7 and 8 have devices that are assigned to them.

Pupils are responsible for their conduct when using school issued or their own devices. Any misuse of devices by pupils will be dealt with under the School's Behaviour Policy.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers must arrange a meeting with their child's Assistant Head of Key Stage and the IT manager to agree how the school can appropriately support such use. The Assistant Head of Key Stage will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

8. Online Communications

8.1 Staff

Any digital communication between members of staff and between staff and pupils or parents / carers must be professional in tone and content. Staff must not engage in any email correspondence which could be viewed as offensive or makes unsubstantiated claims or gossip about other staff, parents or pupils.

Staff are permitted to check their personal email accounts but should do so at lunch and break time only; access at other points during the working day should be avoided. Staff should be aware that, if the Head believes that traffic generated by or sent to a member of staff may has been inappropriate or in contravention of any other school policies, the school reserves the right without notice to inspect and review email traffic that has passed through or on the school's system.

Staff must also be careful to avoid any email traffic being displayed inadvertently on a whiteboard or a computer screen such that it could be seen by a child or other member of staff to whom the data on display is not relevant and may be confidential.

The school's email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Staff must understand that the emails they send and receive are official records that can be disclosed to relevant parents, staff, other third parties or to the Information Commissioner's Office (ICO) if a subject access request (SAR) is made. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Under no circumstances may staff contact a pupil or parent or carer / recent alumni (i.e. pupils over the age of 18 who have left the school within the past 12 months) or parents of recent alumni using any personal email address or SMS / WhatsApp. The only circumstance where staff may contact recent alumni is if they become a member of staff working at the school. The alumni would have then completed our Child Protection and Safeguarding training as well as an induction period. The alumni would also then be subject to our Staff Code of Conduct.

Personal telephone numbers, email addresses, or other contact details, must not be shared with pupils or parents / carers and recent alumni, unless those parents / carers / alumni are members of staff. Under no circumstances may staff contact a pupil using a personal telephone number, email address or other messaging system nor should pupils, parents and recent alumni / their parents / carers be added as social network 'friends' or similar unless those parents / carers / alumni are members of staff.

Staff must immediately report to the DSL or the Headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT Staff.

8.2 Pupils

All pupils are issued with their own personal school email addresses for use on our network from Year 3, but they do not have access to them until Year 5. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work, research or projects. Pupils should be aware that email communications through the school network and school email addresses are monitored.

The school ensures that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work or research purposes, pupils should contact the IT Manager for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to the DSL.

9. Use of social media

9.1 Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices whilst teaching or in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room or staff-only areas of school.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Sevenoaks Prep into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual; or
  - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Code of Conduct or Safeguarding and Child Protection Policy.

9.2 School

The school uses the following social networking sites: Facebook and Instagram as broadcast services to engage and collaborate with the parents of current and prospective pupils. A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services and as such no two-way communication will take place.

Posts on the school’s networking sites may only be made by the Marketing Officer.

In addition,

- parents must have given written permission for the school to use their child’s image;
- no pupils are identified by name;
- where services are “comment enabled”, comments must be set to ‘moderated’;
- all posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted.

9.3 Pupils

The school expects pupils to think carefully before they post any information online or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by pupils vary seriously and incidents will be dealt with under the Behaviour, Safeguarding and Child Protection and Anti-Bullying policies as appropriate.

9.4 Parents

Parents are reminded to use social media platforms, including WhatsApp and other messaging apps, responsibly and respectfully when discussing school-related matters. To protect the reputation of the school, pupils, staff, and other parents, the school requests that any concerns or complaints be raised directly with the school through the appropriate channels rather than being discussed in online forums. Negative, defamatory, or misleading comments about the school community on social media can cause unnecessary distress and may be subject to further action. The school encourages all parents to set a positive example for pupils by fostering a respectful and constructive online environment.

10. Data protection

The Data Protection Act 2018 provides considerable protection of pupils’ personal data, and the UK data protection watchdog, the Information Commissioner’s Office (ICO), has fined educational establishments and individual teachers found to be failing in the duty to keep such data secure.

Please refer to the Data Protection policy and the Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.
Staff and pupils are expected to save all data relating to their work to the school's central server, as per the Acceptable Use Policy.
Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.
Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the school.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the IT Manager in accordance with the Data Protection Policy and Acceptable Use Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Manager.

11. Password Security

Pupils and staff have individual school network logins, staff also have school email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every 6 months;
- not write passwords down; and
- not share passwords with other pupils or staff.

12. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites) and follow the School's policy on official social media posting.

Staff are allowed to take digital/video images to support educational, promotional or marketing purposes, but must follow school policies concerning the sharing, distribution and publication of those images. Images should be taken only on school equipment: the personal equipment of staff should not be used for such purposes wherever possible, unless the Head has given specific prior permission.

The school's contract with parents indicates that photographs of their child(ren) may be used in school publications, on the school website or in other materials created or promoted by the schools in the public domain. Parents can complete a consent form to opt-out of all or some of these uses of their child(ren)'s photographs.

13. Artificial Intelligence

Please see the school's Acceptable Use of AI policy for all information, policy and procedures on AI usage.

14. Misuse

Sevenoaks Prep School will not tolerate illegal activities or activities that are in breach of any of the school's policies. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnership. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they must report it to the DSL immediately in accordance with the school's Safeguarding & Child Protection Policy. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Safeguarding and Child Protection and Behaviour policies.

15. Complaints

As with all issues of safety at Sevenoaks Prep School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the DSL in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection policy and reported to the school's DSL, Helen Cook, in accordance with the school's Safeguarding and Child Protection Policy.

16. Legislation and Guidance

This policy pays due regard to the following statutory and non-statutory guidance.

Keeping Children Safe in Education (September 2024)
Meeting Digital and Technology Standards in Schools and Colleges (updated 2025)
Teaching Online Safety in Schools (January 2023)
Safeguarding Children and Protecting Professionals in Early Years Settings (February 2019) advice for managers and practitioners
Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)
The UK Safer Internet Centre (www.saferInternet.org.uk)
CEOP's Thinkuknow website (www.thinkuknow.co.uk)
UK Council for Child Internet Safety (UKCCIS)
The Data Protection Act 2018
The GDPR, and relevant guidance from the Information Commissioner's Office (ICO)

Date last reviewed by the Governing Body: September 2024
Date of next review by the Governing Body: September 2025