SEVENOAKS SCHOOL

Policy reference	Policy – AO1
Policy Category	A. Student and Parent Facing
Name of policy	Online Safety Policy
Scope	Students, Staff and Parents
Purpose of policy	Online safety is an essential part of safeguarding and the School acknowledges its duty to ensure that all students and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out the whole school approach to online safety which will empower, protect and educate students and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.
Regulatory or legal requirement addressed by policy	Education Regulations 2014 (Independent School Standards) Working Together to Safeguard Children (December 2023) (WTSC), Keeping Children Safe in Education (September 2024) (KCSIE), Prevent Duty Guidance (March 2024)
Other policies referred to	Anti-bullying policy, Behaviour Policy, Communications Policy, Curriculum Policy, Data Protection Policy, Use of Student or Staff Images guidance, PSHE and RSE Policies, IT Terms of Use, Safeguarding Policy, Searching and Confiscation policy, Social media Policy, Staff Code of Conduct, Use of Technology in the Classroom
Policy owned by	Deputy Head Pastoral/Designated Safeguarding Lead
Published on website	Yes

1. Policy Aims and Scope

1.1. This policy has been written by Sevenoaks School involving staff, students and parents/carers, building on The Education People policy template, with specialist advice and input as required. It takes into account DfE statutory guidance local safeguarding children multi-agency partnership procedures.

1.2. We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all students and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out our whole school approach to online safety which will empower, protect and educate students and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.

1.3. Sevenoaks School understands that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: 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; for example, making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

1.4. Sevenoaks School recognises that children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online.

1.5. This policy applies to students, parents/carers and all staff, including the governing body, senior leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy).

1.6. Sevenoaks School identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, are an important part of everyday life, and present positive and exciting opportunities, as well as challenges and risks. This policy applies to all access to and use of technology, both on and off-site.

1.7. This policy links with several other policies, practices and action plans, including but not limited to:

- Behaviour Policy (including Anti-bullying Policy and Anti-cyberbullying Policy)
- Communications Policy
- Curriculum Policy
- Data Protection Policy
- IT Terms of Use
- PSHE and RSE Policies
- Safeguarding Policy
- Searching and Confiscation policy
- Social media Policy
- Staff Code of Conduct
- Use of Student or Staff Images guidance
- Use of Technology in the Classroom

2. Responding to Emerging Risks

Sevenoaks School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- carry out an annual review of our online safety approaches, including but not limited to our filtering and monitoring provision, considering the specific risks our students face and the potential for new or updated measures to mitigate these risks.
- regularly review the methods used to identify, assess and minimise online risks.
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted.
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet access is appropriate.
- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems, and as such identify clear procedures to follow if breaches or concerns arise.
- recognise that generative artificial intelligence (AI) tools may have uses which could benefit our school/college community, but equally can pose risks; this is including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material.
- make staff and students aware of the benefits and risks of using AI tools.
- respond to any misuse of AI in line with relevant policies, including but not limited to, anti-bullying, behaviour and child protection.
- respond in line with the relevant guidance where we believe that AI tools may have facilitated the creation of child sexual abuse material, including the sharing of nude/semi-nude images by children.

3. Monitoring and Review

- Sevenoaks School will review this policy at least annually. The policy will also be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure he has oversight of online safety, the Headmaster will be informed of online safety concerns, as appropriate.
- The Deputy Head Pastoral will report on online safety practice and incidents, including outcomes, on an annual basis to the wider governing body.
- Any issues identified will be incorporated into our action planning.

4. Roles and Responsibilities

The Designated Safeguarding Lead (DSL) is recognised as holding overall lead responsibility for online safety, however Sevenoaks School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The Senior Leadership Team will:

- Create a whole school culture that incorporates online safety throughout.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies which address the acceptable use of technology, child on child abuse, use of social media and mobile technology.
- Work with technical staff and IT support to ensure that appropriate filtering and monitoring systems are in place.

- Support the DSL and Deputy DSLs by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement. Ensure that staff, students and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole school curriculum which enables all students to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety as appropriate.
- Ensure referrals are made to relevant external partner agencies, as appropriate.
- Work alongside Deputy DSLs to ensure online safety is recognised as part of the school's safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep students safe online, including the additional risks that students with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents/carers and the wider community.
- Maintain records of online safety concerns as well as actions taken, as part of the school's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.
- Report online safety concerns, as appropriate, to the Senior Leadership Team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet the student online safety working group on a termly basis.

4.3 It is the responsibility of all members of staff to:

- Read and adhere to our Online Safety Policy and IT Terms of Use.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with students.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the students in their care.
- Identify online safety concerns and take appropriate action by following our safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting students and parents/carers to appropriate support, internally and externally.

- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures to ensure that the school's IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL to enable them to take appropriate safeguarding action when required.

4.5 It is the responsibility of students (at a level that is appropriate to their individual age and ability) to:

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the IT Terms of Use and Behaviour Policy.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

4.6 It is the responsibility of parents and carers to:

- Read our IT Terms of Use and encourage their children to adhere to it.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media
- Seek help and support from the school or other appropriate agencies if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as learning platforms and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and Engagement Approaches

5.1 Education and engagement with students

- Sevenoaks School will establish and embed a whole school culture and will empower our students to acquire the knowledge needed to use the technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- We and will raise awareness and promote safe and responsible internet use amongst students by:
    - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) '[Education for a Connected World Framework]' and DfE '[Teaching online safety in school]' guidance.
    - ensuring online safety is addressed in PSHE (including RSE) and Technology lessons.
    - recognising that a one size fits all approach may not be appropriate, and a more personalised or contextualised approach for more vulnerable children e.g. victims of abuse and SEND, may be needed.

- reinforcing online safety principles in other curriculum subjects and whenever technology or the internet is used onsite.
- implementing appropriate peer education approaches, such as feedback to the student body from the student online safety working group.
- creating a safe environment in which all students feel comfortable to say what they feel, without fear of getting into trouble or being judged for talking about something which happened to them online.
- involving the DSL as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any students who may be impacted by the content.
- making informed decisions to ensure that any resources used are appropriate for our students.
- using external visitors, where appropriate, to complement and support our internal online safety education approaches, being mindful of the guidance found here: Using External Visitors to Support Online Safety Education: Guidance for Educational Schools
- rewarding positive use of technology.

- Sevenoaks School will support students to understand and follow our IT Terms of Use in a way which suits their age and ability by:
  - sharing our Terms of Use with them in accessible and appropriate ways.
  - informing students that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
  - seeking student voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Sevenoaks School will ensure students develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
  - ensuring age-appropriate education regarding safe and responsible use precedes internet access.
  - enabling them to understand what acceptable and unacceptable online behaviour looks like.
  - teaching students to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
  - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
  - preparing them to identify possible online risks and make informed decisions about how to act and respond.
  - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable students

- Sevenoaks School recognises that any student can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some students, for example looked after children and those with special educational needs or disabilities, who may be more susceptible or may have less support in staying safe online.
- Sevenoaks School will ensure that differentiated and appropriate online safety education, access and support is provided to all students who require additional or targeted support.
- Staff at Sevenoaks School will seek input from specialist staff as appropriate, including the DSL and SENCO, to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

- We will:
    - provide and discuss the online safety policy and procedures, including our IT Terms of Use, with all members of staff as part of induction.
    - provide up-to-date and appropriate training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach. Updates will be delivered at least annually.
    - ensure staff training covers the potential risks posed to students (content, contact and conduct) as well as our professional practice expectations.
    - build on existing expertise, by providing opportunities for staff to contribute to and shape our online safety approaches.
    - ensure staff are aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
    - ensure staff are aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
    - highlight useful educational resources and tools which staff could use with students.
    - ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving students, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- Sevenoaks School recognises that parents and carers have an essential role to play in enabling our students to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - providing information and guidance on online safety, specifically through The Wellbeing Hub, a free resource signposted and made available to all parents at the start of the academic year.
    - talking to them about students' access to online sites when away from school.
    - drawing their attention to our Online Safety Policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as on our website.
    - requiring them to read our IT Terms of Use and discuss the implications with their children.

6. Safer Use of Technology

6.1 Classroom use

- Sevenoaks School uses a wide range of technology. This includes access to:
    - Computers, laptops, tablets and other digital devices
    - Internet, which may include search engines and educational websites
    - Learning platforms, remote learning platform/tools and intranet
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras.
- All school owned devices will be used in accordance with our IT Terms of Use and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites (including search engines), tools and apps fully before use in the classroom or recommending for use at home.
- Teaching staff will ensure that emails and other potential sources of sensitive information are not visible to students at any stage in the classroom.
- Use of video sharing platforms will be in accordance with our IT Terms of Use, following an informed risk assessment and with appropriate safety and security measures in place.

- We will ensure that the use of internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to students' age and ability.
    - Students will use age-appropriate search engines and online tools and will be appropriately supervised.

6.2 Managing internet access

- All users will read and agree to our IT Terms of Use before being given access to our computer system, IT resources or the internet.
- We will maintain a record of users who are granted access to our devices and systems.

6.3 Filtering and monitoring

Leaders and DSLs should access guidance about establishing 'appropriate levels' of filtering and monitoring to help inform their decision making: **www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring**

6.3.1 Decision making

- Sevenoaks School will do all we reasonably can to limit children's exposure to online risks through school provided IT systems/devices and will ensure that appropriate filtering and monitoring systems are in place.
- Our governors and senior leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit students' exposure to online risks.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- Governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

6.3.2 Appropriate filtering

- Sevenoaks School uses filtering systems which block 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.
- Our filtering system is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC); it also integrates 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.
- If students or staff discover unsuitable sites or material, they are required to turn off their screen, (in the case of a student) report the concern immediately to a member of staff and report the site/material in question to the IT Department via the helpdesk.
- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate in line with existing policies, including Safeguarding, IT Terms of Use and Behaviour.

- Parents/carers will be informed of filtering breaches involving students.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or NCA-Child Exploitation and Online Protection Command (CEOP).

6.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all school owned or provided internet enabled devices.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If a concern is identified via our monitoring approaches:
    - Where the concern relates to students, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as Safeguarding, IT Terms of Use and Behaviour.
    - Where the concern relates to staff, it will be reported to the Head (or Chair of Governors if the concern relates to the Head), in line with our Staff Code of Conduct and Safeguarding Policy.

6.4 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

6.5 Information security and access management

- We take appropriate steps to ensure necessary security protection procedures are in place, in order to safeguard our systems, staff and students. These include:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus/malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
    - Checking files held on our network, as required and when deemed necessary by leadership staff.
    - The appropriate use of user logins and passwords to access our network and user logins and passwords will be enforced for all users.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
- We will review the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies.

6.5.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- On arrival in the school, all students are provided with their own unique username and private passwords to access our systems; students are responsible for keeping their password private.
- We require all users to:
    - use strong passwords for access into our system.
    - change their passwords annually.

- not share passwords or login information with others or leave passwords/login details where others can find them.
- not to login as another user at any time.
- lock access to devices/systems when not in use.

6.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- We will ensure that our school website complies with guidelines for publications, including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or students' personal information will not be published on our website; any staff contact details will be their school address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

6.7 Publishing images and videos online

- We will ensure that all images and videos shared online are shared appropriately and in accordance with the guidelines set out elsewhere in this policy and in Use of Student or Staff Images.

6.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and the code of conduct/behaviour policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Emails containing sensitive or personal information will have suitable confidentiality settings in place and where necessary attachments will be password protected.
- School email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately report offensive communication to the DSL or other Deputy as appropriate.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.
- Wellbeing and pastoral issues will be directed to the relevant tutor or Divisional Head, but students are also made aware of the email address of the DSL/Deputy Head Pastoral, who can be contacted directly with safeguarding or pastoral concerns.

6.8.1 Staff email

- All members of staff:
  - are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
  - are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, students and parents.

- Will be reminded that they should use a personal, rather than school email account for the purpose of whistleblowing, in order to maximise the confidentiality of this process.

6.8.2 Student email

- Students will:
  - use a provided email account for educational purposes.
  - agree to our IT Terms of Use and receive education regarding safe and appropriate email etiquette before access is permitted.

6.9 Educational use of videoconferencing and/or webcams

- Sevenoaks School recognises that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
- All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
- Videoconferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publicly.
- Videoconferencing equipment will not be taken off the premises without prior permission of the DSL or Headmaster.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Videoconferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

6.9.1 Users

- Parental consent will be obtained prior to students taking part in videoconferencing activities.
- Videoconferencing will take place via official and approved communication channels following a robust risk assessment and will be supervised appropriately, according to the student's age and ability.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and will be kept securely, to prevent unauthorised access.

6.9.2 Content

- When recording a videoconference lesson or meeting, it should be made clear to all parties at the start of the conference; continued attendance in the lesson will be taken as consent to be part of the recording.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the students.

6.9.3 Management of learning platforms

- Sevenoaks School uses Firefly as its official learning platform and all access and use takes place in accordance with our IT Terms of Use.

- Leaders and staff will regularly monitor the usage of Firefly, including message/communication tools and publishing facilities.
- Only current members of staff and students will have access to Firefly. When staff/students leave the school, their account will be disabled or transferred to their new establishment.
- Any concerns about content on Firefly will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A student's parents may be informed.
    - If the content is illegal, we will respond in line with existing safeguarding procedures.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto Firefly by a member of the leadership as part of an agreed focus or a limited time slot.

6.9.4 Management of applications (apps) used to record progress

- We use isams to track student progress and share appropriate information with parents and carers.
- The Director of IT will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations and Data Protection legislation.
- To safeguard students' data, all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

6.9.5 Management of remote learning

Where children are asked to learn online at home in response to a full or partial closure:

- Sevenoaks School will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with students and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and via Teams.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and students will engage with remote teaching and learning in line with existing behaviour principles as set out in our Behaviour Policy and IT Terms of Use.
- Staff and students will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- Staff will follow the guidance in 'Safeguarding and Child Protection Policy Addendum – COVID-19', found here: https://sevenoaksschool.fireflycloud.net/resource.aspx?id=981164&officeint=on
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. Sevenoaks School will continue to be clear about who from the school their child is going to be interacting with online.

- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

7. Social Media

7.1 Expectations

- The expectations regarding safe and responsible use of social media apply to all members of the Sevenoaks School community. The policy applies to all use of social media; the term social media includes, but is not limited to, blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or other online communication services.
- All members of our community are expected to engage in social media in a positive and responsible manner and are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control student and staff access to social media whilst using school provided devices and systems onsite.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary action.
- The use of social media or apps, for example as a formal remote learning platform will be robustly risk assessed by the DSL, Senior Deputy Head and Deputy Head Academic prior to use.
- Concerns regarding the online conduct of any member of the Sevenoaks School community on social media will be taken seriously and managed in accordance with the appropriate policies.

7.2 Staff use of social media

- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our Code of Conduct and IT Terms of Use.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our Safeguarding Policy and Code of Conduct.

7.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the school.

- Members of staff are encouraged not to identify themselves as employees of Sevenoaks School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

7.2.2 Communicating with students and their families

- Staff will not use any personal social media accounts to contact students or their family members.
- All members of staff are advised not to communicate with or add any current or past students or their family members, as 'friends' on any personal social media accounts.
- Any communication from students and parents/carers received on personal social media accounts will be reported to the DSL or another Deputy.
- Any pre-existing relationships or situations, which mean staff cannot or need not comply with this requirement, will be discussed with the DSL. Decisions made and advice provided in these situations will be formally recorded to safeguard students, members of staff and the setting.
- If ongoing contact with students is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official communication tools provided by the school.

7.3 Official use of social media

- Sevenoaks School staff will use social media for official purposes in the line with the Social Media Policy.

7.4 Student use of social media

- Students in Years 7 - 11 are not permitted to use social media (or mobile phones more broadly) during the school day.
- Students in the Sixth Form may use social media during school hours for personal use, except when in lessons, activities, the café or dining hall at lunch time, or other situations where a teacher has deemed such use inappropriate.
- We will empower our students to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to students as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create or condone accounts for students under the required age as outlined in the service's terms and conditions.
- Mindful of the particular risks posed by group chats, we will actively discourage students from setting these up or joining them, whether for school purposes or otherwise.
- Students will be advised:
    - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.

- only to approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.
- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
- to use safe passwords.
- to use social media sites which are appropriate for their age and abilities.
- how to block and report unwanted communications.
- how to report concerns on social media, both within the setting and externally.

- Any concerns, sanctions or support regarding students' use of social media will be dealt with in accordance with appropriate existing policies, including Behaviour and Safeguarding.
- Civil or legal action may be taken if necessary.
- Concerns regarding students' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

8. Mobile and Smart Technology

8.1 Safe use of mobile and smart technology expectations

- Sevenoaks School recognises that use of mobile and smart technologies is part of everyday life for most students, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the school community are advised to:
  - take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our Behaviour and Safeguarding Policies.
- All members of the Sevenoaks School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our policies.

8.2 School provided mobile phones and devices

- School mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff – or, in the case of classroom devices, by students when supervised in class.
- School mobile phones and devices will always be used in accordance with the IT Terms of Use and other relevant policies.
- Where staff or students are using school-provided mobile phones or devices, they will be informed prior to use that activity may be monitored for safeguarding reasons and to ensure policy compliance.

8.3 Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant school policy and procedures.
- Staff will be advised to:

- Keep mobile phones/personal devices on their person or in a safe and secure place during lesson time.
- Not use personal devices during teaching periods unless required for safeguarding or other unavoidable procedural reasons.
- Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.

- Members of staff are not permitted to use personal email accounts or phone numbers for contacting students or parents/carers.
  - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL.
- Staff will only use a school account, mobile or SIM (rather than a personal one):
  - to take photos or videos of students in line with our image use policy.
  - to work directly with students during lessons/educational activities.
  - to communicate with parents/carers.
- If a member of staff breaches our policy, action will be taken in line with our Code of Conduct and Safeguarding Policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

8.4 Student use of mobile and smart technology

- Students in the Sixth Form are permitted to use mobile phones and personal devices on site.
  - Mobile phones or personal devices will not be used by students during lessons or formal educational time, unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
  - The use of personal mobile phones or devices for a specific educational purpose does not mean that blanket use is permitted.
  - Mobile phones or personal devices can be used during break or free time, but any use must be in accordance with our Behaviour Policy and IT Terms of Use.
- Sixth Form students will have a range of access to the internet via mobile phone networks (i.e. 3G, 4G and 5G); some will have unlimited and unrestricted access. This brings the potential for students to harass, bully, and control othersvia their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.
- Therefore, students will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
- Safe and appropriate use of mobile and smart technology will be taught to students as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our Curriculum, PSHE and RSE policies.
- Sevenoaks School expects students' personal devices and mobile phones to be kept safe and secure when on site. Students remain responsible for their devices, including the safe and appropriate usage thereof.
- If a student needs to contact their parents/carers whilst on site, they may use their own phone but may also use a school phone, for example in the main school office, if necessary.
- If a student requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with a staff member prior to use being permitted.
- Where students' mobile phones or personal devices are used when learning at home, this will be in accordance with all relevant school policies.

- Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- Any concerns regarding students' use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including Behaviour and Safeguarding.
    - Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our school policies, including but not limited to those listed above.
    - Searches of mobile phone or personal devices will be carried out in accordance with our policy and in line with the DfE **Searching, Screening and Confiscation** guidance.
    - Students' mobile phones or devices may be searched by a Divisional Head or member of the Senior Leadership Team, with the consent of the student or a parent/carer. Content may be deleted or requested to be deleted if it contravenes our policies.
    - Mobile phones and devices that have been confiscated will be held in a secure place and released to students at the end of the school day, or as soon as possible if immediate release is not possible or appropriate.
    - Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our Behaviour policy.
    - Concerns regarding policy breaches by students will be shared with parents/carers as appropriate.
    - Where there is a concern that a child is at risk of harm, we will respond in line with our Safeguarding Policy.
    - If there is suspicion that material on a student's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

8.5 Visitors' use of mobile and smart technology

- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our IT Terms of Use and other associated policies, including Safeguarding.
- If visitors require access to mobile and smart technology, for example when working with students as part of multi-agency activity, this will be discussed with the relevant lead staff member prior to use being permitted. Staff will never share their own login details or capability with outside parties.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or Head of any breaches of our policy.

9. Responding to Online Risks and/or Policy Breaches

- All members of the community:
    - are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content or comments which could cause harm, distress or offence.
    - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures.
    - will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
    - are expected to adopt a partnership with the school to resolve issues.
- If appropriate, after any investigations are completed, the DSL and leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

- If we are unsure how to proceed with an incident or concern, the DSL or Head will seek advice from the local authority or Education Service in accordance with our Safeguarding Policy.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local schools are involved or the wider public may be at risk, the DSL and/or Head will speak with the police and/or the Local Authority first, to ensure that potential criminal or child protection investigations are not compromised.

9.1 Concerns about student online behaviour and/or welfare

- All concerns about students will be responded to and recorded in line with our Safeguarding Policy:
  - The DSL will be informed of all online safety concerns involving safeguarding or child protection risks.
  - The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Sanctions and/or pastoral support will be provided to students as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

9.2 Concerns about staff online behaviour and/or welfare

- Any complaint or allegation made about staff behaviour, whether online or otherwise will be handled as per the guidance in the Safeguarding Policy.
- Where appropriate, welfare support will be offered, and where necessary, disciplinary, civil and/or legal action will be taken in accordance with our Code of Conduct.

9.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents'/carers' behaviour and/or welfare online will be reported to the Head and/or DSL and dealt with in line with existing policies. Where appropriate, welfare support will be offered, and where necessary, civil and/or legal action may be taken.

10. Procedures for Responding to Specific Online Concerns

10.1 Online child on child abuse

- Sevenoaks School recognises that whilst risks can be posed by unknown individuals or adults online, students can also abuse their peers; all online child on child abuse concerns will be responded to in line with our child protection and behaviour policies.
- We recognise that online child on child abuse can take many forms, including but not limited to:
  - bullying, including cyberbullying, prejudice-based and discriminatory bullying
  - abuse in intimate personal relationships between peers
  - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
  - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
  - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
  - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party

- upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
- initiation/hazing type violence and rituals.

- Sevenoaks School believes that abuse is abuse, including when it takes place online and it will never be tolerated or dismissed as "banter", "just having a laugh", "part of growing up" or "boys being boys" as this can lead to a culture of unacceptable behaviours and an unsafe environment for children.
- All staff have a role to play in challenging inappropriate online behaviours between peers.
- Sevenoaks School recognises that, even if there are no reported cases of online child on child abuse, such abuse is still likely to be taking place.
- Concerns about students' behaviour, including child on child abuse taking place online offsite will be responded to as part of a partnership approach with students and parents/carers and in line with existing policies, for example IT Terms of Use, Behaviour and Safeguarding policies.
- We want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online child on child abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with associated policies. Students who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

10.1.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Sevenoaks School will follow the guidance outlined in Part Five of KCSIE 2023, as well as being mindful of Childnet's online sexual harassment guidance: **www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals**
- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.
- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.
- Sevenoaks School recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
  - consensual and non-consensual sharing of nude and semi-nude images and videos
  - sharing of unwanted explicit content
  - 'upskirting' (which is a criminal offence and typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
  - sexualised online bullying
  - unwanted sexual comments and messages, including, on social media
  - sexual exploitation, coercion and threats.
- Sevenoaks School recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms, and for things to move from platform to platform online.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment and the support available, by

implementing a range of age and ability appropriate educational methods as part of our curriculum.

- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator and any other children involved/impacted.
    - The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children and staff and any actions that are required to protect them.
    - Reports will initially be managed internally by the DSL, including where appropriate seeking advice from the Education Safeguarding Service, and where necessary will be referred to Children's Social Care and/or the Police.
    - The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
    - If content is contained on students' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Following an immediate risk assessment, the school will:
    - provide the necessary safeguards and support for all students involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
    - inform parents/carers for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
    - if the concern involves children and young people at a different educational school, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised.
    - review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- Sevenoaks School recognises that the internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. Sevenoaks School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

10.1.2 Nude or semi-nude image sharing

The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of 18. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex.

- Sevenoaks School recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") can be a safeguarding issue; all concerns will be reported to and dealt with by the DSL.
- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
    - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.

- shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
- possesses nude and/or semi-nude imagery created by another person (or AI created image) under the age of 18.

- When made aware of concerns regarding nude and/or semi-nude imagery, we will follow the advice as set out in the non-statutory UKCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.
- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
  - Report any concerns to the DSL immediately.
  - Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, this will be immediately reported to the DSL.
  - Not delete the imagery or ask the child to delete it.
  - Not say or do anything to blame or shame any children involved.
  - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
  - Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.
- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
  - act in accordance with our Safeguarding Policy and the relevant local procedures and in line with the UKCIS guidance.
  - carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of students involved, including the possibility of carrying out relevant checks with other agencies.
  - make a referral to Children's Social Care and/or the police immediately if:
    - the incident involves an adult (over 18).
    - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
    - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
    - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
  - consider whether to involve other agencies at any time if further information/concerns are disclosed at a later date .
  - seek advice from the Education Safeguarding Service if unsure how to proceed.
  - store any devices securely:
    - If content is contained on students' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - inform parents/carers about the incident and how it is being managed and provide support and

signposting, as appropriate, unless to do so would place a child at risk of significant harm.
    - provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
    - implement sanctions where necessary and appropriate in accordance with our Behaviour Policy but taking care not to further traumatise victims where possible.
    - consider the deletion of images in accordance with the UKCIS guidance.
        - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
        - Students will be supported in accessing the Childline Report Remove tool for nude images where necessary
    - review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- We will not:
    - view any imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. If it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child and will not allow or request students to do so.

10.1.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Sevenoaks School. Any incidents of cyberbullying will be responded to in line with our Anti-bullying and Anti-cyberbullying Policies (found within the Behaviour Policy).

10.2 Online child abuse and exploitation

- Sevenoaks School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL, in line with our Safeguarding Policy.
- We will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target students, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for students, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our Safeguarding Policy and the relevant local safeguarding children partnership procedures.
    - store any devices containing evidence securely:
        - If content is contained on students' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Care and inform the police via 101, or 999 if a student is at immediate risk.
    - If involving a staff member, make a referral to the LADO and take immediate steps to safeguard the

community.
    - carry out a risk assessment which considers any vulnerabilities of student(s) involved, including carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - provide the necessary safeguards and support for students, such as, offering counselling or pastoral support.
    - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using school provided or personal equipment.
    - Where possible and appropriate, students will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via the National Crime Agency CEOP Command (NCA-CEOP): www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Service, Local Authority and/or police.
- We will ensure that the NCA-CEOP reporting tools are visible and available to students and other members of our community, on Firefly.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL.
- If members of the public or students at other schools are believed to have been targeted, the DSL will seek advice from the police and/or the Local Authority before sharing specific information to ensure that potential investigations are not compromised.

10.3 Indecent Images of Children (IIOC)

- Sevenoaks School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - act in accordance with our Safeguarding Policy and the relevant local safeguarding children partnership procedures.
    - store any devices involved securely, until advice has been sought. If content is contained on students' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a student has been exposed to indecent images of children, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk and/or police.
    - inform the police as appropriate, for example if images have been deliberately sent to or shared by

students.
    - report concerns as appropriate to parents and carers.
- If made aware that indecent images of children have been found on school provided devices, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and any other agencies, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children, we will:
    - ensure that the Head is informed in line with our policy on managing allegations against staff.
    - inform the LADO and other relevant organisations, such as the police.
    - quarantine any involved school provided devices until police advice has been sought.

10.4 Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Sevenoaks School and will be responded to in line with existing policies, including Safeguarding and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Local Authority and/or the police.

10.5 Online radicalisation and extremism

- We will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a student may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Safeguarding Policy.

10.6 Cybercrime

- Sevenoaks School recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.
- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the Cyber Choices programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

11. Useful Links

Links for Schools

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- SWGfL: 360 Safe Self-Review tool for schools www.360safe.org.uk
- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- PSHE Association: www.pshe-association.org.uk
- National Education Network (NEN): www.nen.gov.uk
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk
- Educate against hate: https://educateagainsthate.com
- NCA-CEOP Education Resources: www.thinkuknow.co.uk
- Safer Recruitment Consortium: www.saferrecruitmentconsortium.org/

Reporting Helplines

- NCA-CEOP Safety Centre: www.ceop.police.uk/Safety-Centre
- Internet Watch Foundation (IWF): www.iwf.org.uk
- ChildLine: www.childline.org.uk
  - Report Remove Tool for nude images: www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online
- Stop it now! www.stopitnow.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Report Harmful Content: https://reportharmfulcontent.com
- Revenge Porn Helpline: https://revengepornhelpline.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Support for children and parents/carers

- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Parent Zone: https://parentzone.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
  - Net Aware: www.net-aware.org.uk
- Parents Protect: www.parentsprotect.co.uk
- Get Safe Online: www.getsafeonline.org
- NCA-CEOP Child and Parent Resources: www.thinkuknow.co.uk