

Online Safety Policy

Applies to:

- The whole school along with all activities provided by the school, including those outside of the normal school hours;
- All members of the Radnor House Sevenoaks school community, including staff, pupils, volunteers, parents, carers and visitors, who have access to and are users of the school ICT systems;
- All staff (teaching and support), the Directors and volunteers working in the school.

In our school the term 'staff', in the context of safeguarding, is inclusive of all staff and is also inclusive of students on placement, contractors, agency staff, volunteers and the Proprietor.

Both this Online Safety Policy and our requirements for Acceptable Use of IT, cover both fixed and mobile 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 and staff brought onto school premises (personal laptops, tablets, wearable technology e.g. smart phones and watches, etc.). They also cover when pupils are going online in the home environment, for example when completing homework and coursework at home.

We aim to ensure that every pupil in our care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle 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 identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

Related Documents:

- | | |
|---|---|
| • Anti-bullying Policy | • Safeguarding Policy |
| • Behaviour Policy | • Staff Code of Conduct |
| • Health and Safety, Risk Assessment and Welfare Policy | • Acceptable Use of IT Policies (Pupils, and Staff and Directors) |
| • Data Protection Policy | • PSHEE, and RSE Policies |

This policy takes into account:

- DfE statutory guidance "Keeping Children Safe in Education" 2023,
- DfE advice for schools: "teaching online safety in schools" June 2019; which outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements: [Teaching online safety in schools - GOV.UK \(www.gov.uk\)](https://www.gov.uk/teaching-online-safety-in-schools)
- UKCIS 'Education for a Connected World' Framework, June 2020 : [Education for a Connected World - GOV.UK \(www.gov.uk\)](https://www.gov.uk/education-for-a-connected-world)
- DfE advice for schools: "sharing nudes and semi-nudes, advice for education settings working with children and young people": [Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK \(www.gov.uk\)](https://www.gov.uk/sharing-nudes-and-semi-nudes)
- Early Years and Foundation Stage 2021, and
- The Kent Safeguarding Children Partnership procedures

Availability:

- This policy is made available to parents, staff and pupils in the following ways: via the school website, and on request a copy may be obtained from the School Reception.

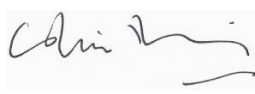
Monitoring and Review:

- This policy will be subject to continuous monitoring, refinement and audit by the Head.
- The Board of Directors undertake a formal annual review of this policy.

Signed:



Fraser Halliwell
Head



Dr Colin Diggory
Chairman of the Board of Directors

August 2023

1. Introduction

- 1.1 It is essential that children are safeguarded from potentially harmful and inappropriate online material. Radnor House Sevenoaks' whole school approach to online safety empowers the school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.
- 1.2 It is recognised by the school that the use of technology presents particular challenges and risks to children and adults both inside and outside of school, including when they are remote learning online at home. Where children are being asked to learn online at home the DFE has provided advice to support schools to do so safely.
- 1.3 All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. 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, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.
- 1.4 Members of staff with appropriate skills, interest and expertise regarding online safety are encouraged to help support the DSL, and any deputy DSLs as appropriate, for example when developing curriculum approaches or making technical decisions. However, the DSL is acknowledged as having overall responsibility for online safeguarding within the school.
- 1.5 Radnor House Sevenoaks identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
 - Content: being exposed to illegal, inappropriate or harmful material, 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 with the intention of grooming or exploiting them.
 - Conduct: personal online behaviour that increases the likelihood of, or causes, harm, for example: making, sending and receiving explicit images, and online bullying.
 - Commerce: being exposed to risks such as online gambling, inappropriate advertising, phishing and or financial scams. If pupils or staff are at risk, the school will report it to <https://apwg.org/>
- 1.6 This policy complements the statement of Acceptable Use of IT for all staff, visitors and pupils and is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.
- 1.7 Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.
- 1.8 At this school 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.
- 1.9 We also encourage anyone, including a pupil who believes our systems are being misused in any way, to speak out and alert us to such possible misuse.
- 1.10 There are codes of conduct for authorised and responsible use of our system for both staff and pupils. Please refer to the Acceptable Use (IT) Policy – Pupils, and the Acceptable Use (IT) Policy – Staff and Directors for further information.

2. Roles and responsibilities

- 2.1 The Board of Directors of the school hold online safety as a central theme in their whole setting approach to safeguarding. The Board is responsible for the approval of this policy and for reviewing its effectiveness. The Board will review this policy at least annually.
- 2.2 Under KCSIE, the Board of Directors must ensure that appropriate online filters and appropriate monitoring systems are in place, so that pupils are safeguarded from potentially harmful and inappropriate online material. However, they must be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding. See Appendix 2 of this policy for further information.
- 2.3 The Directors must also ensure that safeguarding training for staff, including online safety and filtering and monitoring training, is integrated, and considered as part of the whole school safeguarding approach. They will also ensure that the children are taught about safeguarding, including online safety
- 2.3 The Head is responsible for the safety of the members of the school community and this includes responsibility for online safety. This responsibility for online safety has been delegated to the Designated Safeguarding Lead (DSL) who has been appointed as Online Safety Co-ordinator.
- 2.4 The Designated Safeguarding Lead takes lead responsibility for safeguarding and child protection, including online safety and filtering and monitoring. This includes at a strategic level, and regarding the day to day issues relating to online safety, including liaising with the Network Manager, regarding the ongoing monitoring and filtering of the internet in school.
- 2.5 The Designated Safeguarding Lead is expected to:
- liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs or the named person with oversight for SEN in a college) on matters of safety and safeguarding (including online and digital safety);
 - be able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college; and
 - be able to recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online;
 - keep up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International, NSPCC and the Local Authority Safeguarding Children Board.
- 2.6 The Senior Leadership Team is to ensure that:
- staff, in particular the DSL who is the Online Safety Lead, are adequately trained about online safety; and
 - 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.
 - ensure there are appropriate and up-to-date policies regarding Online Safety, including a Staff Code of Conduct and an Acceptable Use of IT Policy/Agreement, which covers acceptable use of technology by staff and pupils.
- 2.7 The school’s technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school’s hardware system, its data and for training the school’s teaching and administrative staff in the use of ICT and our internet filtering system. They routinely use software to monitor the use of the internet for pupils and staff, that produces filtering reports and instant notifications regarding inappropriate usage, which go to the DSL. Emails are not routinely monitored unless a cause for concern has been raised.
- 2.8 All teaching staff receive regular information and training on online safety issues in the form of targeted training and internal briefings, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. This includes updated information regarding online filtering and monitoring responsibilities and procedures in the school.

- 2.9 Teaching and support staff: all staff are required to sign a statement of acceptable use before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.
- 2.10 All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's acceptable use guidelines.
- 2.11 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.
- 2.12 Pupils are responsible for using the school ICT systems in accordance with their signed statements of acceptable use. They have a responsibility to speak out when they believe that the school's systems are being abused in any way.
- 2.13 The school believes that it is essential for parents, guardians and carers to be fully involved with promoting online safety both in and outside of school. We regularly consult and discuss online safety with parents, guardians and carers to reinforce the importance of children being safe online, and seek to promote a wide understanding of the benefits and risks related to internet usage. It is important for parents and carers to be aware of what their children are being asked to do online, including the sites the school will ask them to access and who they will be asked to interact with online. The school will always 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. Parents, guardians and carers are responsible for endorsing their child's confirmation of adherences to the school's acceptable use.
- 2.14 Home Learning - where pupils are being asked to learn online at home the DfE has provided advice to support schools to ensure this is done so safely: [safeguarding-and-remote-education](#). For specific details regarding how the school has organised their home learning programme, technology and online security, please contact the school's Director of Digital Learning or the Designated Safeguarding Lead, who is also the Online Safety Coordinator.

3 Education and training

- 3.1 Staff: awareness and training
- New teaching staff receive information on online safety and acceptable use as part of their induction.
 - All teaching staff receive regular information and training on online safety issues in the form of targeted training and internal briefings, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.
 - All incidents relating to online safety should be reported to the DSL via MyConcern .
- 3.2 Pupils: Online safety in the curriculum
- IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our 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 will also be carried out via PSHEE and assemblies, as well as informally when opportunities arise.
 - Younger pupils are introduced to the concept of online safety through story books and via channels that allow them to be made aware of dangers in a way that is age-appropriate.
 - At age-appropriate levels, and usually via PSHEE, pupils are taught to look after their own online safety. Again at age-appropriate points, pupils are taught 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. Pupils can report concerns to the DSL (who is the Online Safety Lead) and indeed any member of staff at the school.

- Pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images.
- Pupils should be 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 Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL, the Online Safety Lead or other member of staff as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

3.3 Pupils: Vulnerable Pupils

- The school is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- The school will seek input from specialist staff as appropriate, including the SENCO and Head of Student Support.

3.4 Parents: Awareness and Engagement with Parents

- Radnor House Sevenoaks recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
 - Providing information, guidance and training on online safety in a variety of formats.
 - Drawing attention to the Online Safety policy and other online matters via newsletters, letters and website.
 - Requiring they read online safety information when a pupil joins the school e.g. within the home school agreement.
 - Requiring them to read the school AUP and discuss its implications with their children.

4. Reducing Online Risks

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

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

4.2 **Filtering and monitoring** –Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material, but without unreasonably impacting teaching and learning, in line with the DfE [filtering and monitoring standards](#) which were updated in March 2023.

4.3 The school will ensure that appropriate filtering and monitoring systems are in place when pupils and staff access school systems and internet provision, so that exposure to any risks can be reasonably limited. The UK Safer Internet Centre has published guidance as to what “appropriate” filtering and monitoring might be: [Appropriate Filtering and Monitoring | Safer Internet Centre](#). We review our approach to this regularly and assess the effectiveness of the current provision, any gaps, and the specific needs of pupils (their age ranges, those who are at greater risk of harm for example those with SEND, or those with English as an additional language) and our staff : this happens annually, or more often if circumstances dictate such as when:

- a safeguarding risk is identified
- there is a change in working practice (like remote access or BYOD)
- a new technology is introduced

Please see Appendix 1 for further details.

- 4.4 The school uses a wide range of technology in the classroom. All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- 4.5 All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.
- 4.6 Supervision of pupils will be appropriate to their age and ability, as follows:
- Teachers actively talk about online dangers with pupils before activities are carried out online, and pupils are reminded to act appropriately and follow the guidance contained in their Acceptable Use of IT Agreement.
 - Early Years Foundation Stage and Key Stage 1 – pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for pupils' age and ability.
 - Key Stage 2 - pupils will use age-appropriate search engines and online tools.
 - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.
 - Key Stage 3, 4, 5 - pupils will be appropriately supervised when using technology, according to their ability and understanding.

5. Social Media

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

- 5.1 Expectations
- The expectations' regarding positive, safe and responsible use of social media applies to all members of Radnor House Sevenoaks community. The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
- 5.2 All members of Radnor House Sevenoaks community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Concerns regarding the online conduct of any member of Radnor House Sevenoaks community on social media, should be reported to the school and will be managed in accordance with our Anti-Bullying, Behaviour, and Safeguarding Policies, and Staff Code of Conduct.
- 5.3 Staff Personal Use of Social Media
- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
 - Staff use of social media forms part of the school Staff Code of Conduct
 - For their own protection, staff who make use of social media sites are asked to ensure that their privacy settings are set to the maximum level, so that only 'friends' can access their pictures and information.
- 5.4 Pupils' Personal Use of Social Media
- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.

- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

5.4 Official School Use of Social Media

- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
- Official social media use will be conducted in line with existing policies, including: Anti-Bullying, Data Protection, and Safeguarding and the Staff Code of Conduct.
- Any official social media activity involving pupils will be moderated by the school where possible.
- The school will ensure that any official social media use does not exclude members of the community who are unable use social media channels.

5.5 Staff Guidelines

- Members of staff who follow and/or like the school social media channels are advised to use dedicated (i.e. not personal) accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
 - Be professional, responsible, credible and fair at all times and aware that they are an ambassador for the school.
 - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
 - Ensure that they have appropriate written consent before posting images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
 - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
 - Immediately inform their line manager, the Designated Safeguarding Lead and/or the Head of any concerns, such as criticism, inappropriate content or contact from pupils.

6 Use of school and personal devices

6.1 Staff

- 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. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents, guardians and carers and under no circumstances may staff contact a pupil or parent, guardian or carer using a personal telephone number, email address, social media or messaging system.
- Personal cameras belonging to staff and volunteers are not to be used on the school premises or school grounds at any time. Cameras on staff owned mobile phones should not be used on school premises or school grounds at any time. No images may be taken of the school or any pupils using mobile phones or personal cameras.
- Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

- Personal mobile phones may be used in dedicated staff areas or in class and teaching rooms only if the children are not present, or in the event of needing to use the authenticator application.
- Staff should not accept mobile phone calls during a lesson or when they are with children. The only exception to this is if the Head calls a staff member (usually only on Sports Days or on school trips, or if the School Office calls in similar circumstances). These calls will only be made in unusual or emergency situations.
- Phones brought to school should be left in an individual's own bag and should be turned off or on silent.
- Staff are advised to ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- The school cameras may be used for official photographs under the direction of the Head. These photographs must only be downloaded using the school's computers and not onto a personal, private computer. Please refer to the Staff Code of Conduct for further details.
- If a member of staff breaches the school Online Safety Policy, action will be taken in line with the Staff Code of Conduct.
- 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, the police will be contacted.

6.2 Pupils

- Radnor House Sevenoaks recognises the importance of mobile phones as means of communication and safety when travelling to and from school, where pupils have smart phones, parents are responsible for ensuring that they have age appropriate content filtering configured in the phone settings.
- As soon as pupils arrive at school their mobile phones must be switched off; for senior pupils, mobiles must be placed in their lockers, for Prep pupils phones must be handed into the Prep School Office. Phones found outside lockers during the hours of 8.20-16.00 will be confiscated and given to Head of School, this will also result in a Friday detention. Pupils will be able to collect their phones at the end of the school day. After school activities are deemed to be within the school day.
- These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.
- 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 should arrange a meeting with the SENDCo to agree how the school can appropriately support such use. The SENDCo Lead will then inform the pupil's teachers, the DSL, the IT Services Manager and other relevant members of staff about how the pupil will use the device at school. (see also school's BYOD (Bring Your Own Device) policy)
- If a pupil needs to contact their parents or carers whilst on site, they will be allowed to use a school phone – following permission from a teacher.
- Parents are advised to contact their child via the school office.
- Where pupils' mobile phones or personal devices are used when learning at home, this will be in accordance with the school Acceptable Use Policy and Remote Learning policy.
- Mobile phones and personal devices must not be taken into examinations. Pupils 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 learners use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.

- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
- Searches of mobile phone or personal devices will be carried out in accordance with the DfE 'Searching, Screening and Confiscation' guidance: [Searching, screening and confiscation at school - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/searching-screening-and-confiscation-at-school)
- Pupils mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil 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 parents/carers.
- Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
- Concerns regarding policy breaches by learners 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 learner'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.

7 Use of internet and email

7.1 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 whilst in staff-only areas of school.
- When accessed from personal 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.
- The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.
- Staff must immediately report to the DSL/the Online Safety Lead 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.
- Any online communications must not either knowingly or recklessly:
 - harm or place a child or young person at risk of harm;
 - bring Radnor House Sevenoaks 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;
 - liking and/or disliking and/or retweeting (or the equivalent) any post or other element of social media; and

- posting links or material which is discriminatory or offensive.
- Under no circumstances should school pupils or parents be added as social network 'friends'.
- Any digital communication between staff and pupils or parents, guardians and carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

7.2 Pupils

- All pupils from year 1 upwards are assigned a school login (email address) for use on our network and to facilitate cloud resources. Access is via a login, which is password protected. This official email service may be regarded as safe and secure, and must only be used for school work: assignments, research and projects. Pupils should be aware that all digital communication is monitored.
- Enterprise anti-virus and firewall protection is used within the school domain. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work such as assignments, research and projects pupils should contact the IT support team.
- Pupils should immediately report, to the DSL/the Online Safety Lead or another member of staff, 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.
- The school expects pupils to think carefully before they post any information online including liking and/or disliking and/or retweeting (or the equivalent) any post or other element of social media. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.
- Pupils must report any accidental access to materials of a violent or sexual nature directly to the DSL/Online Safety Lead or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems is monitored.
- Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work, pupils should contact the IT team.

8. Managing Personal Data Online

The school takes its compliance with the Data Protection Act 2018 seriously. Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation. Full information can be found in the school's Data Protection Policy (available on the school website).

9 Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems. This is reviewed annually, or more regularly if circumstances dictate. For further details, please see Appx 3.

9.1 Data storage and processing -

- 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 or personal cloud storage, but instead stored on an encrypted USB memory stick or school provided cloud storage.
- Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT team.

9.2 Password security -

- All Pupils from year 1 upwards and staff have individual school network logins [email addresses] and storage folders on the server (for purposes of remote login access). 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 three months by all staff and twelve months by students;
 - not write passwords down; and
 - not share passwords with other pupils or staff.

10 Safe use of digital and video images

- 10.1 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, guardians or 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.
- 10.2 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 images on the internet (e.g. on social networking sites).
- 10.3 For parents, guardians and carers of older children: they are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them or (if minors) without the permission of their parents, guardians and carers, nor should parents, guardians and carers comment on any activities involving other children or pupils in the digital or video images.
- 10.4 Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.
- 10.5 Care should be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- 10.6 Pupils must not take, use, share, publish or distribute images of others without their permission.
- 10.7 Written permission from parents, guardians or carers will be obtained before photographs of pupils are published on the school website.
- 10.8 Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- 10.9 Radnor House 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 (or deputy).
- 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.

11 Management of Applications which Record Children's Progress (Data and Images)

- 11.1 The school uses SIMS and Tapestry (EYFS) to track pupils progress and share appropriate information with parents and carers. The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed prior to use, and that they are used in accordance with GDPR and data protection legislation

To safeguard data:

- only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- personal staff mobile phones or devices will not be used to access or upload content.
- school devices will be appropriately encrypted if taken off site to reduce the risk of a data security breach in the event of loss or theft.
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

12 Radicalisation and the Use of Social Media

- 12.1 The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems.

- 12.2 In line with Prevent guidance, protecting children from the risk of radicalisation, Radnor House Sevenoaks has a number of measures in place to ensure that children are safe from terrorist and extremist material when accessing the internet in school, and to help prevent the use of social media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by pupils
- Pupils, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

- 12.3 Further details on how social media is used to promote extremism and radicalisation can be found on the Educate Against Hate site, which is designed to equip schools and college leaders, teachers and parents with the information, tools and resources they need to recognise and address extremism and radicalisation in young people, including in online issues. [Educate Against Hate - Prevent Radicalisation & Extremism](#)

13 Responding to Online Safety Incidents and Concerns

- 13.1 All members of the school community will be made aware of the reporting procedure for online safety and safeguarding concerns regarding pupil welfare, including: breaches of filtering, youth produced sexual imagery (sexting), upskirting, cyberbullying, sexual harassment and illegal content. The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- 13.2 All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns. For further detailed information, the school Safeguarding Policy, Complaints Policy and Procedures, and Whistleblowing Policy can be found on the school website.
- 13.3 After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- 13.4 If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Kent Education Safeguarding Team. Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.

- 13.5 Any allegations regarding a member of staff's online conduct will be referred to the Head, and discussed with the DSL/Online Safety Lead and the LADO (Local Authority Designated Officer) if necessary. Appropriate action will be taken in accordance with the Staff Code of Conduct.
- 13.6 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.

The DSL will respond to the concerns as set out in the non-statutory UKCIS (UK Council for Child Internet Safety) guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

The DSL will also refer to online guidance from KSCMP:

'Safer Professional Practice with Technology: Frequently Asked Questions' and

'Responding to Nude and Semi-Nude Image Sharing: Guidance for Professionals'.

[Online safety - Kent Safeguarding Children Multi-Agency Partnership \(kscmp.org.uk\)](http://kscmp.org.uk)

Kent and Medway Safeguarding Partnerships have collaboratively developed these documents to provide a clear procedure for anyone working with children and young people. The 'Safer Professional Practice with Technology' document will assist professionals to work safely and responsibly online, and to monitor their own standards and practice. It will also support managers and leaders in establishing a culture which safeguards staff and children/adults online.

The 'Responding to 'Nude and Semi-Nude Image Sharing: Guidance for Professionals' is based on the national 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance from UKCIS, and is a multiagency document for professionals working with children and young people in Kent.

- 13.7 For further details regarding the procedures for responding to specific online incidents or concerns, please contact the school Online Safety Lead, and see Appendix 3.
- 13.8 For a list of Useful Links for Educational Settings, see Appendix 4.

14 Reporting

- 14.1 The school will not tolerate illegal activities or activities that are inappropriate in a school context. The school will always report illegal material and illegal activity to the police and/or the Local Children Safeguarding Partnership. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the local children's services and/or police.
- 14.2 Incidents of misuse or suspected misuse must be investigated by staff and where appropriate this will be in accordance with the school's Safeguarding Policy and procedures and/or Anti-bullying Policy.
- 14.3 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 Anti-Bullying Policy, BYOD (Bring Your Own Device) Policy, and Acceptable User agreement noting that instances of bullying may be a pupil safeguarding concern.

15 Visitors' Use of Mobile and Smart Technology

- 15.1 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 acceptable use of technology policy and other associated policies, including child protection.
- 15.2 Visitors wifi codes are available from Reception.
- 15.3 If visitors require access to mobile and smart technology, for example when working with pupils as part of multi-agency activity, this will be discussed with the IT Services Manager prior to use being permitted and will be noted on the visitor risk assessment form held by HR.
- 15.4 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 IT Services Manager of any breaches of our policy.

16 Complaints

- 16.1 As with all issues of safety at the school, if a member of staff, a pupil or a parent, guardian or 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 undertake an immediate investigation and liaise with the Senior Leadership Team and any members of staff or pupils involved. Please see the Complaints Procedures for further information.
- 16.2 Incidents of or concerns around online safety will be recorded and reported to the school's Designated Safeguarding Lead.

Appendix 1 - Filtering and monitoring of the internet by the school

The school will ensure that appropriate filtering and monitoring systems are in place when pupils and staff access school systems and internet provision, so that exposure to any risks can be reasonably limited. The school acknowledges that whilst filtering and monitoring is an important part of the school's online safety responsibilities, it is only one part of our approach to online safety. Pupils and adults may have access to systems external to the school control such as mobile phones and other internet enabled devices and technology and where concerns are identified appropriate action will be taken.

Any checks to the School's filtering provision are completed and recorded as part of the filtering and monitoring review process. The Directors have overall strategic responsibility for meeting this requirement, and they have assigned day to day responsibility for the following to the Finance and Operations Director, the Head and the IT Services Manager:

- procuring filtering and monitoring systems
- reviewing the effectiveness of the Foundation's provision
- overseeing reports

They must also ensure that all staff:

- are appropriately trained for their role
- understand that it is everyone's responsibility to keep the online environment safe, including the effective use of filtering and monitoring
- follow the Staff Code of Conduct, all policies, processes and procedures
- act on reports and concerns, and record them appropriately

The DSL has the lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT Support Department has the technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead. The School therefore reserves the right to regularly monitor and filter an employee's/pupil's use of the internet, social media and e-mail systems when at work or when using Foundation electronic equipment. Such monitoring/filtering includes the right to read e-mails sent or received on electronic equipment provided by the School or view photographic images captured on electronic equipment provided by the School to check that the use by employees is in accordance with this policy.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They must report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

The Board of Directors support the senior leadership team to review the effectiveness of monitoring strategies and reporting process. Any incidents that are picked up, are acted on with urgency and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. Staff know that in the first instance, they report their concerns to the DSL.

If it is discovered that any of the systems are being abused and/or that the terms of this Policy are being infringed, disciplinary action may be taken in accordance with the provisions of the School's disciplinary policies and procedures.

Decision Making

- Radnor House Sevenoaks Board of Directors, Head and SLT have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.

- They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively, and know how to escalate concerns when identified.
- The governors and leaders are aware of the need to prevent “over blocking”, as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

Filtering

- The school uses educational broadband connectivity through London Grid for Learning (LGFL); as part of this service Webscreen 3.0 is used for webfiltering and reporting; e.g. blocking sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- 365/Azure intelligent language filter works across 365 Apps and Email.
Sophos anti-virus is installed on all staff/student devices – this works as a filter and blocker both in and out of school.
- The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The school works with LGFL to ensure that our filtering policy is continually reviewed.
- South West Grid for Learning (swgfl.org.uk) have created a tool to check whether a school’s filtering provider is signed up to the relevant lists to ensure effective blocking (e.g. sexual, terrorist and child abuse content).

Dealing with filtering breaches

- The school has a clear procedure for reporting filtering breaches.
- If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediately to their teacher (pupils are able/encouraged to report concerns directly to the IT department)
- The teacher will report the concern to the and the IT department.
- The IT Services Manager will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

Monitoring

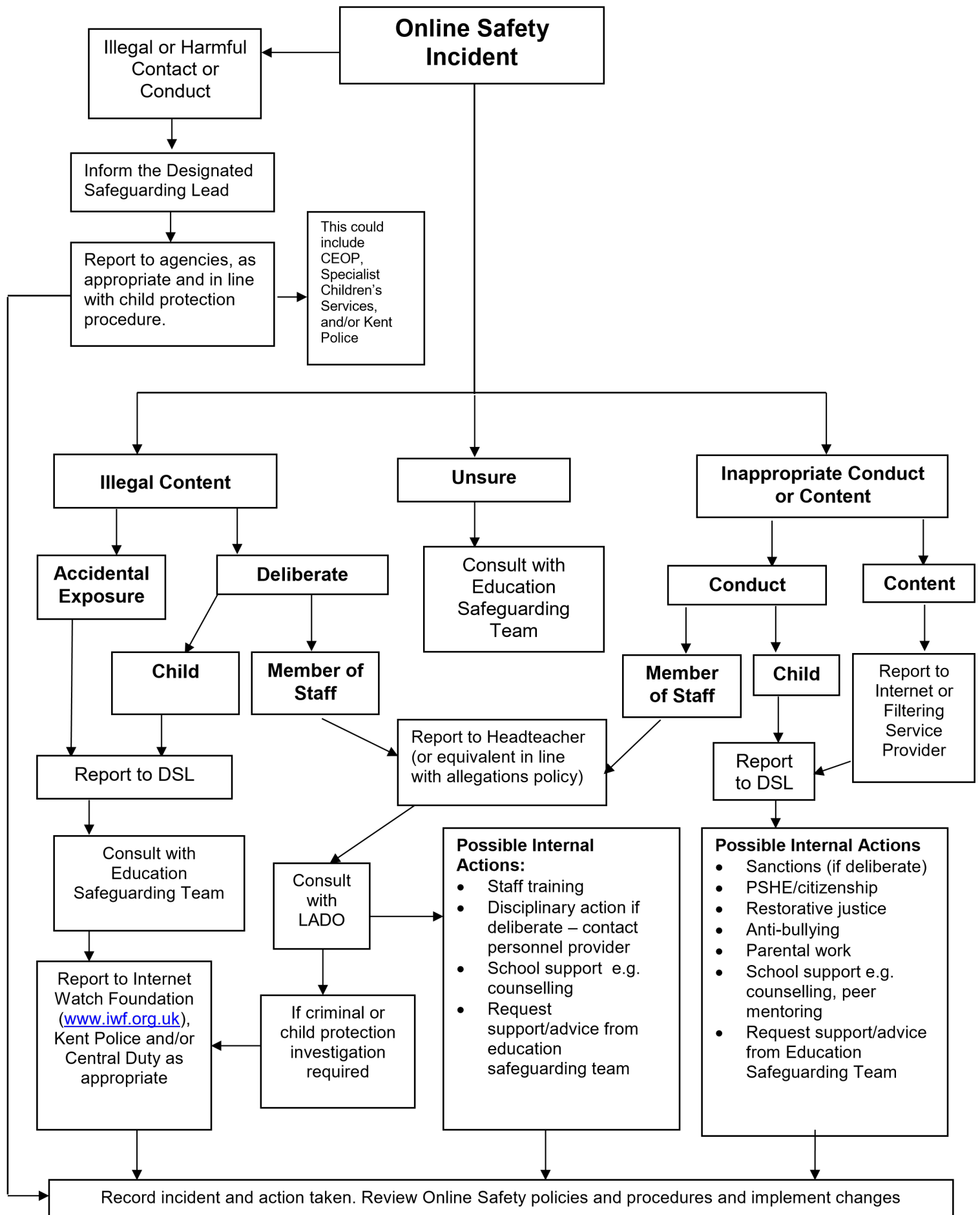
- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
- In the Prep school, pupils are not left alone with electronic devices. From Year 1 to Year 13 all pupils and staff have individual logons, allowing tracking and monitoring of internet use.
- The school has a clear procedure for responding to concerns identified via monitoring approaches: To monitor device and internet use RH7 are using a product called Senso. The DSL receives daily Senso reports as well as having access to the online Senso portal to view alerts. The DSL meets weekly with the IT Services Manager to review any concerns flagged by the reports. Any pupil concerns will be passed through to Heads of Schools to raise with pupils in their section. Behaviour and Sanctions procedures will be followed. Any concerns regarding staff internet searches will be passed by the DSL to the Headteacher.
- At a granular level, within school, Network deep packet analysis is monitored by Logrhythm
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Appendix 2 - Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including (but not limited to):

- 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.
- Regularly checking files held on the school's network,
- The appropriate use of user logins and passwords to access the school network.
- Specific user logins and passwords will be enforced for all but the youngest users.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found at (list the separate technical policies or procedures such as AUPs that contain other information)

Appendix 3: Responding to an Online Safety Concern



Appendix 4 Sources of Information for schools and parents to keep children safe online

(KCSIE 2023, Annex B 'Additional Advice and Support') (The following list is not exhaustive but should provide a useful starting point).

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- [Childnet](#) provide guidance for schools on cyberbullying
- [Educateagainshtate](#) provides practical advice and support on protecting children from extremism and radicalisation
- [London Grid for Learning](#) provides advice on all aspects of a school or college's online safety arrangements
- [NSPCC](#) provides advice on all aspects of a school or college's online safety arrangements
- [Safer recruitment consortium](#) "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- [Searching screening and confiscation](#) is departmental advice for schools on searching children and confiscating items such as mobile phones
- [South West Grid for Learning](#) provides advice on all aspects of a school or college's online safety arrangements
- [Use of social media for online radicalisation](#) - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an [Online Safety Audit Tool](#) to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) [Online safety guidance if you own or manage an online platform](#) provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) [A business guide for protecting children on your online platform](#) provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote education, virtual lessons and live streaming

- [Case studies](#) on remote education practice are available for schools to learn from each other
- [Departmental guidance on safeguarding and remote education](#) including planning remote education strategies and teaching remotely
- Guidance Get help with remote education resources and support for teachers and school leaders on educating pupils and students
- [London Grid for Learning](#) guidance, including platform specific advice
- [National cyber security centre](#) guidance on choosing, configuring and deploying video conferencing
- [UK Safer Internet Centre](#) guidance on safe remote learning

Support for children

- [Childline](#) for free and confidential advice
- [UK Safer Internet Centre](#) to report and remove harmful online content
- [CEOP](#) for advice on making a report about online abuse

Parental support

- [Childnet](#) offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- [Commonsensemedia](#) provide independent reviews, age ratings, & other information about all types of media for children and their parents
- [Government advice](#) about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- [Government advice](#) about security and privacy settings, blocking unsuitable content, and parental controls
- How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online
- [Internet Matters](#) provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world [Let's Talk About It](#) provides advice for parents and carers to keep children safe from online radicalisation
 - [London Grid for Learning](#) provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
 - [Stopitnow](#) resource from [The Lucy Faithfull Foundation](#) can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
 - [National Crime Agency/CEOP Thinkuknow](#) provides support for parents and carers to keep their children safe online
 - [Net-aware](#) provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
 - [Parentzone](#) provides help for parents and carers on how to keep their children safe online
 - [Parent info](#) from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
 - Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parent guide on talking to your children about online sexual harassment
 - #Ask the awkward – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships
 - [UK Safer Internet Centre](#) provide tips, advice, guides and other resources to help keep children safe online

Appendix 5 - Useful Links for Educational Settings

Kent Support and Guidance

- Kent County Council Education Safeguarding Team:
 - Rebecca Avery, Education Safeguarding Adviser (Online Protection)
 - Ashley Assiter, E-Safety Development Officer
esafetyofficer@kent.gov.uk Tel: 03000 415797
- Kent Area Safeguarding Advisor (Education Safeguarding Service)
 - North Kent Area Safeguarding Advisor (Education): Anup Kandola
Email: anup.kandola@theeducationpeople.org
 - North Kent Area Safeguarding Assistant: Joanne Barnett
Safeguarding Admin Support: Rachel Unsworth
Email: rachel.unsworth@theeducationpeople.org
Telephone: office hours: 03301 651 240
Mobile: 07971 531800
[Safeguarding Contacts | The Education People](#)
- Guidance for Educational Settings:
 - <https://www.theeducationpeople.org/our-expertise/safeguarding/online-safety/>
 - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
 - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
 - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
 - KSCB: www.kscb.org.uk

Official Guidance

- DfE advice for schools: “teaching online safety in schools” June 2019; which outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements: [Teaching online safety in schools - GOV.UK \(www.gov.uk\)](#)
- UKCIS ‘Education for a Connected World’ Framework, June 2020 : [Education for a Connected World - GOV.UK \(www.gov.uk\)](#)
- DfE advice for schools: “sharing nudes and semi-nudes, advice for education settings working with children and young people”: [Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK \(www.gov.uk\)](#)
- UKCIS guidance: [Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK \(www.gov.uk\)](#)

Kent Police

- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101
- www.kent.police.uk or [Parent resources: At-home learning and activity packs for children | Kent Police](#)

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- <https://www.bbc.com/ownit/take-control/own-it-app>
- CEOP: www.thinkuknow.co.uk; www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Fearless: [Home - Fearless](#)
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety

- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- <https://www.thinkuknow.co.uk/>
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- Young Gamblers Association: <https://www.ygam.org/>

360 Safe Self-Review tool for schools: www.360safe.org.uk