Name of Policy	Online Safety
Document owner	Miss Hayley Bennett (Head of School Curriculum)
Designated Safeguarding Lead	Mrs Tina Hamer (Executive Headteacher)
Named Management committee member with lead responsibility	
Document issued/last reviewed	November 2024
Date for review	November 2025

Contents

It is essential that children are safeguarded from potentially harmful and inappropriate online material, behaviour and interactions. An effective approach to online safety empowers settings to protect and educate learners and staff in their use of technology and establishes clear mechanisms to identify, intervene in, and escalate any concerns where appropriate.

1. Policy Aims and Scope

- This policy has been written by The Rosewood School, involving staff, pupils/students and parents/carers, building on the Kent County Council LADO and Education Safeguarding Advisory Service policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage (if applicable to the school) 'Working Together to Safeguard Children' and our local Safeguarding Children Multi-agency Partnership procedures.
- We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all pupils/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 our pupils/students and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.
- The Rosewood School understands that 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, for example, 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.

- The Rosewood 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 other children online.
- This policy applies to pupils/students, parents/carers and all staff, including the management committee, 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).
- The Rosewood School identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, is an important part of everyday life, and presents 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.

- Staff at The Rosewood School recognise that children may not feel ready or know how to tell someone that they are being abused, exploited, or neglected online, and/or they may not recognise their experiences as being abusive or harmful. This should not prevent staff from having professional curiosity and speaking to a member of the inclusion team or senior leadership/ DSLs if they have any online safety concerns about a child.

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

- Anti-bullying policy

- Acceptable Use Policies (AUP)
- Code of conduct/staff behaviour policy
- Behaviour policy
- Child protection policy
- Confidentiality policy
- Curriculum policies, such as: Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data protection
- Data/information security
- Cameras and image use policy
- Mobile and smart technology
- Social media
- Searching, screening and confiscation policy.

2. Responding to Emerging Risks

- The Rosewood 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 which will be supported by an annual risk assessment which considers and reflects the specific risks our pupils/students face.
- 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.

3. Policy monitoring and review

Technology evolves and changes rapidly. The Rosewood School will review this policy at least annually. The policy will 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. Any issues identified will be incorporated into our action planning.
- To ensure they have oversight of online safety, the head teacher will be informed of online safety concerns, as appropriate. Amend as appropriate.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body. Amend as appropriate.
- All members of the community will be made aware of how our school will monitor policy compliance: for example, AUPs, staff training, classroom management.

4. Roles and Responsibilities

The management committee have a strategic leadership responsibility for our school's online safeguarding arrangements; they will ensure that they comply with their duties under legislation and will ensure the policies, procedures and training in our school is effective and comply with the law at all times. The Executive head teacher and the Head of School for curriculum will ensure that the online safety policies and procedures, adopted by our management committee and proprietors, are understood, and followed by all staff.

• The Executive headteacher who is our Designated Safeguarding Lead (DSL) has overall responsibility for the day-to-day oversight of safeguarding and child protection systems, including online safety and understanding the filtering and monitoring systems and processes in place. Whilst the activities of the DSL may be delegated to the deputies, the ultimate lead responsibility for online safety remains with the DSL and this responsibility will not be delegated. Whilst activities of the DSL may be delegated to an appropriately trained deputy, the lead responsibility for safeguarding and child protection, including online safety remains with them.

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

4.1 Leadership and management

The leadership and management 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 the DSL, Medway Grid for Learning (MGfL)/TRS Network to ensure that suitable and appropriate filtering and monitoring systems are in place but hold overall responsibility for procuring our filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of our provision and overseeing any reports.
- Support the DSL and any deputies 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, pupils/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 pupils/students to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL):

The leadership and management team 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 (If appropriate) to ensure online safety is recognised as part of our safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Taking lead responsibility for overseeing and acting on any concerns identified by our filtering and monitoring systems.

- 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 pupils/students safe online, including the additional risks that pupils/students with Special Educational Needs 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 through a variety of channels and approaches.
- Maintain records of online safety concerns as well as actions taken, as part of the schools 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. Amend as appropriate
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (include frequency) with the governor with a lead responsibility for safeguarding.

4.3 Members of staff

It is the responsibility of all members of staff to:

- Contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- 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 pupils/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 pupils/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 pupils/students and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 IT Staff/IT Service Providers

It is the responsibility of IT staff/IT Service providers who are managing our technical environment to:

- Provide technical support and perspective to the DSL and leadership team in the development and implementation of our online safety policies and procedures, including appropriate filtering and monitoring systems.
- Support the leadership team and DSL to procure systems, identify risk, carry out reviews and carry out checks to our filtering and monitoring systems.

- Whilst responsibility for the procurement and implementation of appropriate filtering and monitoring is held by the leadership team and responsibility for acting on safeguarding concerns is led by the DSL; technical staff will 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.
- Implement appropriate security measures including (add any specific examples or signpost to other policies) as directed by the leadership team to ensure that the schools IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

4.5 Pupils/students

It is the responsibility of pupils/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 acceptable use of technology and behaviour policies.
- 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 Parents/carers

It is the responsibility of parents and carers to:

- Read our Acceptable Use of technology policies and encourage their child(ren) to adhere to them.
- Support our online safety approaches by discussing online safety issues with their child(ren) and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement and/or acceptable use of technology policies.
- Seek help and support from the school or other appropriate agencies if they or their child(ren) 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. Amend as appropriate.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their child(ren) access and use at home.

5.1 Education and engagement with pupils/students

The Rosewood 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 pupils/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 Relationships Education, Relationships and Sex Education, Health Education and Citizenship.
- Ensuring that online safety is embedded into breakfast club so students become aware of local, national and international issues
- Reinforcing online safety principles in other curriculum subjects and whenever technology or the internet is used on site.
- Creating a safe environment in which all students feel comfortable to say what they feel, without fear of getting into trouble and/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 educational resources used are appropriate for our pupils/students.
- Using external visitors, where appropriate, to complement and support our internal online safety education approaches.

The Rosewood School will support students to understand and follow our Acceptable Use policies in a way which suits their age and ability by:

- Sharing our acceptable use policies with them in accessible and appropriate ways.
- Displaying acceptable use posters in all rooms with internet access.
- Informing students that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
- Seeking student's voice when writing and developing online safety policies and practices, including curriculum development and implementation.

The Rosewood 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 and/or ability 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 pupils/students and those who are potentially at greater risk of harm

The Rosewood School recognises that any students 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, child who are care leavers, children who are adopted, children who are, or who are perceived to be, lesbian, gay, bisexual, trans (LGBT) or gender questioning, and those with special educational needs or disabilities (SEND), who may be more susceptible or may have less support in staying safe online.

- The Rosewood School will ensure that differentiated and appropriate online safety education, access and support is provided to all pupils/students who require additional or targeted education and/or support. Initially this will be through breakfast club and PSHE unless targeted intervention is required.

- Staff at The Rosewood School will seek input from specialist staff as appropriate, including the DSL, SENCO, PSHE specialist 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 acceptable use policy, with all members of staff, including management committee members as part of induction.
- Provide up-to-date and appropriate training for all staff, including management committee members, which is integrated, aligned and considered as part of our overarching safeguarding approach. This will be achieved as part of our existing annual safeguarding and child protection training/updates or within separate or specific online safety sessions.
- Ensure our training for management committee members equips them with the knowledge to provide strategic challenge to test and assure themselves that our online safety policies and procedures in place in are effective and support the delivery of a robust whole school approach.
- Ensure that online safety training provided to all staff is regularly updated.
- Ensure our training covers the potential risks posed to pupils/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

The Rosewood 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 ensure parents and carers understand and are aware of:

- The systems used at school to filter and monitor their child's online use
- What their children are being asked to do online
- We will build a partnership approach and reinforce the important of online safety through regular contact and communication with parents and carers by:
- Providing information and guidance on online safety through emails on uploaded to the school's social media
- 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.
- Requesting parents and carers read online safety information
- Requiring them to read our acceptable use of technology policies and discuss the implications with their children.

6 Safer Use of Technology

6.1 Classroom use

The Rosewood 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, webcams and video cameras.

All school owned devices will be used in accordance with our acceptable use of technology/mobile technology and social media policies and with appropriate safety and security measures in place.

Use of video sharing platforms will be in accordance with our acceptable use of technology policies, following an informed risk assessment and with appropriate safety and security measures in place. This includes:

- We will ensure that the use of internet-derived materials by staff and pupils/students complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to pupils/students age and ability. This includes: Amend as appropriate

Key Stage 3, 4, 5

- Students will use age-appropriate search engines and online tools.
- Students will be appropriately supervised when using technology, according to their ability and understanding.

The Rosewood School recognises that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, it is important to recognise that AI tools can also 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, and additionally its use can pose moral, ethical and legal concerns.

- Staff and students will be made aware of the benefits and risks of using AI tools through PSHE specific lessons and staff training/CPD
- Staff are required to carry out a risk assessment and seek written approval from the senior leadership team prior to any use of AI in school
- TRS will respond to any misuse of AI in line with relevant policies, including but not limited to, anti-bullying, behaviour and child protection.
- Where the School believes that AI tools may have facilitated the creation of child sexual abuse material, including the sharing of nude/semi-nude images by children, the school will respond in line with the UKCIS guidance 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' and the local KSCMP guidance.

6.2 Managing internet access

- All users will read and agree and/or acknowledge our acceptable use policy, appropriate to their age, understanding and role, 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 Managing personal data online

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

6.4 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.
- 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. To support the school in implementing appropriate monitoring and ensuring that a prompt response to any safeguarding concerns is taken, it is recommended that individual logins are in place for all but the youngest or most vulnerable students.

- 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, full details can be found in the TRS cyber security policy

6.4.1 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.

We require all users to

- Use strong passwords for access into our system.
- 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.

6.5 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, and respect for intellectual property rights, privacy policies and copyright.
- Staff or students' personal information will not be published on our website; the contact details on the website will be our 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.

6.6 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones policies.

6.7 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.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- 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 (name and role of designated member of staff, for example, the DSL, network manager).
- 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. Amend as appropriate.
- We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

6.7.1 Staff email

All members of staff have read and agreed with our code of conduct policy and adhere to the following:

- 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.

6.7.2 Pupils/students email

Pupils/students will:

- Use a provided email account for educational purposes.
- Agree an Acceptable Use Policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

6.9 Management of learning platforms

The Rosewood School uses Google classroom as its official learning platform and all access and use takes place in accordance with our acceptable use policies.

- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.

- Only current members of staff, students and parents will have access to the LP. When staff and/or students leave the school, their account will be disabled or transferred to their new establishment.

Any concerns about content on the LP 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 to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
- Student's parents/carers may be informed.
- If the content is illegal, we will respond in line with existing child protection procedures.

6.10 Management of applications (apps) used to record progress

We use SENECA to track student progress and share appropriate information when necessary.

- The headteacher (amend as appropriate) 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 (GDPR) and Data Protection legislation.

To safeguard pupil/student data:

- Only school issued devices will be used for apps that record and store pupils/students' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store pupils/students personal details, attainment or images.
- 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.

6.11 Management of remote learning

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

- The Rosewood 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. Policy and agreements will be shared as per our Remote Learning provision.
- All communication with pupils/students and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and/or agreed systems: Google Classroom, Microsoft 365 or equivalent.
- Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and pupils/students will engage with remote teaching and learning in line with existing behaviour principles as set out in our behaviour policy/code of conduct and Acceptable Use Policies.
- Staff and pupils/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.
- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP)
- 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.

- The Rosewood School will continue to be clear who from the school (if anyone) 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. Appropriate Filtering and Monitoring on School Devices and Networks

The appropriateness of filters and monitoring systems are a matter for individual schools; decisions about what is appropriate will be informed by the risk assessment required by the Prevent Duty, and will depend on the IT systems in place as well as the school risk profile, which includes: the age range/ability of children, the number of children, those who are potentially at greater risk of harm and how often they access devices and IT systems. The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like; DSLs and SLT should ensure they are familiar with this guidance and its implications.

To support schools to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems.
- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet their safeguarding needs.

Please refer to the Child Protection Policy in relation to filtering and monitoring

8 Online child-on-child abuse

- The Rosewood School recognises that whilst risks can be posed by unknown individuals or adults online, pupils/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
- 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.

- The Rosewood School adopts a zero-tolerance approach to child-on-child abuse. We believe that abuse is abuse and it will never be tolerated or dismissed as "just banter", "just having a laugh", "part of growing up" or "boys being boys"; this can lead to a culture of unacceptable behaviours and can create an unsafe

environment for children and a culture that normalises abuse, which can prevent children from coming forward to report it.

- TRS believes that all staff have a role to play in challenging inappropriate online behaviours between children. Staff recognise that some online child-on-child abuse issues may be affected by gender, age, ability and culture of those involved.

- TRS recognises that even if there are no reported cases of online child-on-child abuse, such abuse is still likely to be taking place and it may be the case that it is just not being reported. As such, it is important that staff speak to the DSL (or deputy) about any concerns regarding online child-on-child abuse.

- Concerns about child-on-child abuse taking place online offsite will be responded to as part of a partnership approach with pupils/students' and parents/carers; concerns will be recorded and responded to in line with existing appropriate policies, for example anti-bullying, acceptable use, behaviour and child protection policies. Note: section 89(5) of the Education and Inspections Act 2006 gives headteachers a statutory power to discipline pupils for poor behaviour outside of the school premises, for example, when children are not under the lawful control or charge of a member of school staff, to such extent as is reasonable. This legislation is for schools only and is not applicable to independent schools.

- TRS 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, including child protection, anti-bullying and behaviour. Pupils/students who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

8.1 Child on child online sexual violence and sexual harassment

Headteachers and DSLs may find it helpful to access Childnet's online sexual harassment guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

- When responding to concerns relating to online child on child sexual violence or harassment, TRS will follow the guidance outlined in Part Five of KCSIE.
- 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.

TRS 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.

The Rosewood 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 services, and for things to move from platform to platform online.

- TRS 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.
- TRS 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. Identify resources or curriculum policies as appropriate.

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, adult students (if appropriate) and staff and any actions that are required to protect them.

Reports will initially be managed internally by the DSL, 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 pupils/students personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice. This guidance applies to schools only.

Following an immediate risk assessment, the school will:

- Provide the necessary safeguards and support for all pupils/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.
- TRS recognises that 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. <School name> also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

8.2 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. The UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance outlines how schools and colleges should respond to all incidents of consensual and non-consensual image sharing, and should be read and understood by DSLs working will all age groups, not just older pupils/students.

- TRS recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos") is a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

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 under the age of 18.

When made aware of concerns regarding nude and/or semi-nude imagery, TRS 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'

TRS 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. Link to curriculum policies such as RSE and resources as appropriate.

- 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, forward, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already inadvertently viewed imagery, 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 child protection policies 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 pupils/students involved, including the possibility of carrying out relevant checks with other agencies
- A referral will be made 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.
- The child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
- The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.

If DSLs are unsure how to proceed, advice will be sought from the local authority.

- Store any devices securely:
- If content is contained on pupils/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 pupils/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.
- 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. Note, DSLs should follow 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' 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 pupils/students to do so.

8.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at TRS.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

8.4 Online child abuse and exploitation

- TRS 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 child protection policy.
- TRS 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 pupils/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 pupils/students, staff and parents/carers. Identify policies and curriculum approaches as appropriate.
- 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:

- In accordance with our child protection policies and the relevant local safeguarding children partnership procedures.
- Store any devices containing evidence securely:
- If content is contained on pupils/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 Work Service and inform the police via 101, or 999 if a pupil/student is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of pupils/students 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 pupils/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, pupils/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 Local Authority and/or police.
- We will ensure that the NCA-CEOP reporting tools are visible and available to pupils/students and other members of our community. Include where this can be accessed, for example, on the school website, intranet.
- 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 pupils/students at other schools or settings 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.

8.5 Child Sexual Abuse Material (CSAM)

- TRS will ensure that all members of the community are made aware of the possible consequences of accessing Child Sexual Abuse Material (CSAM), also known as Indecent Images of Children (IIOC), as appropriate. Any concerns related to consensual and non-consensual nude or semi-nude images sharing by children, will be responded to in line with section 11.1.2 of this policy.
- We will respond to concerns regarding CSAM on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to CSAM 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 Local Authority.

If made aware of concerns relating to CSAM, we will:

- Act in accordance with our child protection policy and the relevant local safeguarding children partnership procedures.
- Lock/limit access and store any devices involved securely to prevent further viewing or deletion of evidence etc, until advice has been sought.
- If content is contained on pupils/students personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice. This guidance applies to schools only.
- Immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a pupil/student has been exposed to CSAM we will:
- Ensure that the DSL is informed urgently so appropriate safeguarding action/support can be taken/provided in line with our child protection policy.
- Ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk and/or to the police.
- Inform the police as appropriate, for example if images have been deliberately sent to or shared by pupils/students.
- Report concerns as appropriate to parents and carers.
- If made aware that CSAM has been found/viewed on school provided networks/devices, we will:
- Ensure that the DSL is informed urgently so appropriate safeguarding action/support can be taken/provided in line with our child protection policy.
- 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 has viewed or is in possession of CSAM, we will:

- Quarantine any involved school provided devices/network access until police advice has been sought.
- Ensure that the head teacher is informed in line with our behaviour/managing allegations against staff policy
- Inform the LADO and other relevant organisations, such as the police, in accordance with our behaviour/managing allegations against staff policy.

8.6 Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at TRS and will be responded to in line with existing policies, including child protection, anti-bullying 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.

8.7 Online radicalisation and extremism

- As per section 7 of this policy, we will take all reasonable precautions to ensure that pupils/students and staff are safe from terrorist and extremist material when accessing the internet on site. Schools will need to highlight specifically how internet use will be filtering and monitored, either here or within previous sections.

- If we are concerned that a child or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that a member of staff may be at risk of radicalisation online, the head teacher will be informed immediately, and action will be taken in line with our child protection, staff behaviour/code of conduct and/or allegations policies. Amend as appropriate.

8.8 Cybercrime

- TRS 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.
- Where there are concerns about 'cyber-enabled' crime such as fraud, purchasing of illegal drugs online, child sexual abuse and exploitation, or other areas of concern such as online bullying or general online safety, they will be responded to in line with our child protection policy and other appropriate policies.

9 Useful Links

This section can be added to policies if felt to be appropriate; additional links can be found in part two and annex B of KCSIE. Local organisations, resources and contacts should also be included.

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
- South West Grid for Learning (SWGfL): 360 Safe Self-Review tool for schools www.360safe.org.uk
- London Grid for Learning: https://lgfl.net/safeguarding
- 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.ceopeducation.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

- Internet Matters: www.internetmatters.org
- Childnet: www.childnet.com
- NSPCC: www.nspcc.org.uk/onlinesafety
- Parents Protect: www.parentsprotect.co.uk
- NCA-CEOP Child and Parent Resources: www.ceopeducation.co.uk
- Parent Zone: https://parentzone.org.uk
- Get Safe Online: www.getsafeonline.org
- Common Sense Media: www.commonsensemedia.org