The Rosewood School: Online Safety Policy

Date written: **September 2021**

Date agreed and ratified by management committee: **October 2021**

Date of next review: **October 2022**

Contents

---

1. Aims

Our school aims to:

-
-
-
-
-

- This policy applies to staff including the governing body, teachers, support staff, external contractors, visitors, volunteers (and other individuals who work for or provide services on behalf of TRS, as well as pupils and parents/carers.
- This policy applies to all access to the Internet and use of information communication devices including personal devices or where pupils, staff or other individuals have been provided with TRS issued devices for use off-site, such as a work/school laptop or mobile phone.

This policy must be read in conjunction with other relevant TRS policies including (but not limited to) Safeguarding, Anti-bullying, Behaviour, screening, searching and relevant curriculum policies including computing, RSE & HE and non statutory advice - UKCIS_sharing_nudes_and_semi_nudes_advice_for_education_setting,

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2020 (KCSIE 2020), , 'Working Together to Safeguard Children' 2018 and the Kent Safeguarding Children Board procedures.

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

TRS is currently operating in response to coronavirus (Covid-19); our safeguarding principles in accordance with KCSIE 2020 and related guidance, however, remain the same. Where children are asked to learn online at home in response to a full or partial closure, will follow expectations as set out within the Child Protection Policy and in line with DfE Guidance, 'Safeguarding and remote education during coronavirus (COVID-19)' 2020.This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Management Committee

The management committee has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The management committee will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The management committee who oversees online safety is Paul Bargery

All management committee members:

-
-
-
-
-
-
-
-

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's DSL and deputy DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

- To act as a named point of contact on all online safety issues and liaise with other members of staff and agencies as appropriate.

- To keep up-to-date with current research, legislation and trends.
- To coordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- To ensure that online safety is promoted to parents/carers and the wider community through a variety of channels and approaches.
- To work with TRS lead for data protection and data security to ensure that practice is in line with legislation.
- To access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep pupils safe online.
- To ensure that online safety incidents and subsequent actions are recorded as part of TRS safeguarding recording structures and mechanisms. Records will be held in CPOMs and the behaviour MIS, in addition the Business/Finance manager will hold logs (appendix 4)
- To monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- To liaise with the local authority and other local and national bodies as appropriate.
- To report online safety concerns, as appropriate, to the SLT and management committee.
- To work with the leadership team to review and update online safety policies on a regular basis (at least annually).
- To ensure that online safety is integrated with other appropriate TRS policies and procedures.

To meet regularly with the management committee member with a lead responsibility for online safety.This list is not intended to be exhaustive.

3.4 The ICT Manager

The ICT Manager is responsible for:

-
-
- Conducting a weekly check for web filter issues, websites accessed and vulnerabilities, and a monthly security firewall check for issues regarding data breaches / data access (undertaken by DMS offsite).
-
-
-
-
-
- Ensuring that appropriate access and technical support is given to the DSL and safeguarding team to our filtering and monitoring systems, to enable him/her to take appropriate safeguarding action if/when required.
-

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

-
-
-
-

This list is not intended to be exhaustive.

3.6 Pupils

Key responsibilities of pupils are:

1. To respect the feelings and rights of others both on and offline.
2. To seek help from a trusted adult if things go wrong, and support others that may be experiencing online safety issues.
3. To take responsibility for keeping themselves and others safe online.
4. To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
5. To assess the personal risks of using any particular technology and behave safely and responsibly to limit those risks.

3.7 Parents

Parents are expected to:

1. To support TRS's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
2. To role model safe and appropriate uses of new and emerging technology.
3. To identify changes in behaviour that could indicate that their child is at risk of harm online.
4. To seek help and support from TRS or other appropriate agencies, if they or their child encounters online problems or concerns.
5. To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
6. To report any known issues as soon as possible.

4. Online Communication and Safer Use of Technology

4.1 Managing the TRS website

4.2 Publishing images and videos online

- In line with TRS's GDPR policy, written permission from parents/carers will always be obtained before images/videos of pupils are electronically published.

4.3 Managing email

- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and/or encrypted methods.

4.4 Appropriate and safe classroom use of the Internet and associated devices

4.5 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms outlined in the school's AUP policy

5. Social Media Policy

5.1 General social media use

1. Expectations regarding safe and responsible use of social media will apply to all members of the TRS community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
2. All members of the TRS community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.

3. Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the TRS community.
4. All members of the TRS 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.
5. Any concerns regarding the online conduct of any member of the TRS community on social media sites should be reported to the SLT and will be managed in accordance with existing TRS policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
6. Any breaches of TRS policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant TRS policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

5.2 Official use of social media

1. Official use of social media sites by TRS will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
2. Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
3. Official TRS social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
4. Staff will use TRS provided email addresses to register for and manage official TRS approved social media channels.
5. Staff running official TRS social media channels will ensure that they are aware of the required behaviours and expectations of use. They will ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
6. All communication on official TRS social media platforms will be clear, transparent and open to scrutiny.
7. Any online publication on official TRS social media sites will comply with legal requirements will not breach any common law duty of confidentiality, copyright etc.
8. Official social media use by TRS will be in line with existing policies, including: anti-bullying and child protection.
9. Images or videos of pupils will only be shared on official TRS social media sites/channels in accordance with TRS's GDPR policy.
10. Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the TRS website and take place with written approval from SLT.
11. SLT staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
12. Parents/carers and pupils will be informed of any official TRS social media use, along with expectations for safe use and TRS action taken to safeguard the community.
13. The TRS official social media channels will be:
    - https://twitter.com/therosewoodsch
    - https://www.linkedin.com/company/the-rosewood-school/
    - https://www.facebook.com/therosewoodschool/
14. Public communications on behalf of TRS will, where possible, be read and agreed by at least one other colleague.
15. An account will link back to TRS's website and/or AUP to demonstrate that the account is official.

TRS will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

5.3 Staff official use of social media

1. If staff are participating in online activity as part of their capacity as an employee of TRS, then they are requested to be professional at all times and that they are an ambassador for TRS.
2. Staff using social media officially will disclose their official role/position, but always make it clear that they do not necessarily speak on behalf of TRS.
3. Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
4. Staff using social media officially will always act within the legal frameworks they would adhere to within TRS, including: libel; defamation; confidentiality; copyright; data protection as well as equalities laws.
5. Staff must ensure that any image posted on TRS's social media channels have appropriate written parental consent.

6. Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of TRS unless they are authorised to do so.
7. Staff using social media officially will inform their line manager, TRS's online safety lead and/or the headteacher of any concerns such as criticism, or inappropriate content posted online.
8. Staff will not engage with any direct or private messaging with pupils or parents/carers through social media and should communicate via TRS communication channels.
9. Staff using social media officially will sign TRS's AUP before official social media use will take place.

5.4 Pupils use of social media

1. Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
2. Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, TRS attended, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.
3. Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
4. Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
5. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
6. Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
7. Any official social media activity involving pupils will be moderated by TRS where possible.
8. TRS is aware that many popular social media sites state that they are not for children under the age of 13, and therefore this information will be communicated to parents/pupils.
9. Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at TRS, will be dealt with in accordance with existing TRS policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

6. Use of Personal Devices and Mobile Phones

6.1 Rationale regarding personal devices and mobile phones

1. The widespread ownership of mobile phones and a range of other personal devices, including wearable technologies, among children, young people and adults will require all members of the TRS community to take steps to ensure that mobile phones and personal devices are used responsibly.
2. The use of mobile phones and other personal devices by young people and adults will be decided by TRS and covered in appropriate policies including TRS's AUP.

TRS recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but requires that such technologies need to be used safely and appropriately within TRS.

6.2 Expectations for safe use of personal devices and mobile phones

1. Electronic devices of all kinds that are brought in to TRS are the responsibility of the user at all times. TRS accepts no responsibility for the loss, theft or damage of such items. Nor will TRS accept responsibility for any adverse health effects caused by any such devices either potential or actual.
2. Mobile phones and personal devices are not permitted to be used during the school day within the TRS site.
3. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the TRS community and any breaches will be dealt with as part of the TRS behaviour policy.
4. Members of staff will be issued with a TRS/work phone number where contact with pupils or parents/carers is required.
5. All members of the TRS community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
6. All members of the TRS community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

7. All members of the TRS community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene TRS's policies.
8. TRS mobile phones and devices must always be used in accordance with the AUP
9. TRS mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

6.3 Pupils use of personal devices and mobile phones

1. Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
2. All use of mobile phones and personal devices by pupils will take place in accordance with the AUP.
3. Mobile phones and personal devices will be switched off and kept out of sight during classroom lessons, breaks and lunch-times and while moving between lessons.
4. Mobile phones or personal devices will not be used by pupils during lessons or formal TRS time unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
5. If members of staff have an educational reason to allow pupils to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by SLT. If a pupil needs to contact his/her parents/carers he/she will be allowed to use a TRS phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the TRS office. Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
6. Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
7. If a pupil breaches the policy, the phone or device will be confiscated and will be held in a secure place.
    - Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery
    - Searches of mobile phone or personal devices will only be carried out in accordance with the DfE's policy. www.gov.uk/government/publications/searching-screening-and-confiscation ○ Pupils' mobile phones or devices may be searched by a member of the SLT, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. Any content relating to nudes or semi-nudes cannot be viewed by a member of staff. The DSL/Safeguarding team must be alerted if this situation occurs and they must follow the UKCIS guidance on UKCIS_sharing_nudes_and_semi_nudes_advice_for_education_settings_V2. See appendix 3 for further monitoring guidance
    - Mobile phones and devices that have been confiscated will be released to parents or carers.
    - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.
8. Where pupils' mobile phones or personal devices are used when learning at home, such as in response to local or full lockdowns, this will be in accordance with our AUP.

6.4 Staff use of personal devices and mobile phones

1. Members of staff are not permitted to use their own personal phones or devices for contacting pupils, young people and their families within or outside of TRS in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with a senior leader.
2. Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
3. Staff will not use any personal devices directly with pupils and will only use work-provided equipment during lessons/educational activities.
4. Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
5. Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
6. Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of SLT in emergency circumstances.
7. Staff will ensure that any content brought on site via mobile phones and personal devices are compatible with their professional role and expectations.

8. If a member of staff breaches TRS policy then disciplinary action will be taken.
9. 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 then the police will be contacted and allegations will be responding to following the allegations management policy.
10. Where remote learning activities because of Covid-19, staff will use TRS provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the AUP.

6.5 Visitors use of personal devices and mobile phones

1. Parents/carers and visitors must use mobile phones and personal devices in accordance with TRS's policy.
2. Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with TRS's GDPR policy.
3. Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

7. Policy Decisions

7.1 Reducing online risks

TRS is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
Emerging technologies will be examined for educational benefit and TRS's SLT will ensure that appropriate risk assessments are carried out before use in school is allowed.

TRS will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.

Our 'Impero' monitoring system and 'lightspeed' filtering system will:

1. Inspect everything that is typed or done;
2. Take screen shots and will report any suspicious use detected;
3. Detect when proxy bypass sites have been used;
4. Help stop downloads of obscene or offensive content;
5. Potentially get an early warning of predator grooming;
6. Can help warn when pupils are planning to meet people they do not know; 7. Help pick up 'cries for help' helping to:
    - Reduce fears over suicide, self-harm and abuse; •
    - Take appropriate action quickly; o
    - Strengthen our pastoral care.
8. TRS will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a TRS computer or device.
9. TRS will audit technology use to establish if the online safety policy is adequate and that the implementation of the policy is appropriate.
10. Methods to identify, assess and minimise online risks will be reviewed regularly by the SLT.
11. Filtering decisions, Internet access and device use by pupils and staff will be reviewed regularly by the SLT.

7.2 Internet use throughout the wider TRS community

1. TRS will liaise with local organisations to establish a common approach to online safety.
2. TRS will provide an AUP for any guest/visitor who needs to access the TRS computer system or Internet on site.

7.3 Authorising Internet access

TRS will maintain a current record of all staff and pupils who are granted access to TRS's electronic communications.

1. All staff, pupils and visitors will read and sign TRS's AUP before using any TRS ICT resources.
2. Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
3. When considering access for vulnerable members of the TRS community (such as with pupils with special education needs) TRS will make decisions based on the specific needs and understanding of the pupil(s).

8. Engagement Approaches

8.1 Education and engagement with learning

1. We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible Internet use amongst pupils by:
    - Ensuring education regarding safe and responsible use precedes Internet access; o Including online safety in RSE & HE and computing programmes of study; o Reinforcing online safety messages whenever technology or the Internet is in use; o Educating pupils in the effective use of the Internet to research; including the skills of knowledge location, retrieval and evaluation;
    - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2. We will support pupils to read and understand the acceptable use policies in a way which suits their age and ability by:
    - Seeking pupil voice when writing and developing online safety policies and practices, including curriculum development and implementation;
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

8.2 Engagement and education of children and young people who are considered to be vulnerable

1. TRS recognises that some pupils are more vulnerable online owing 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.
2. We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
3. When implementing an appropriate online safety policy and curriculum TRS will seek input from specialist staff as appropriate, including the SENCO and Pupil Services staff.

8.3 Engagement and education of staff

The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of TRS safeguarding practice.

1. To protect staff and pupils, TRS will implement an AUP which highlights appropriate online conduct and communication.
2. Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
3. Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis from an external provider.
4. Staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the SLT and will have clear procedures for reporting issues or concerns.
5. TRS will highlight useful online tools which staff should use with pupils in the classroom. These tools will vary according to the age and ability of the pupils.
6. Staff will be made aware that their online conduct out of TRS could have an impact on their role and reputation within TRS. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

8.4 Engagement and education of parents and carers

1. TRS recognises that parents/carers have an essential role to play in enabling pupils to become safe and responsible users of the Internet and digital technology.
2. Parents' attention will be drawn to TRS's online safety policy and expectations in communications, such as letters and the TRS website.
3. We will build a partnership approach to online safety with parents/carers by:
    - Providing information and guidance on online safety in a variety of formats;
    - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events and sports days;
    - Requesting that they read online safety information as part of joining our community, for example, within our home-school agreement;

- Requiring them to read our acceptable use policies and discuss the implications with their children.

9. Managing Information Systems

9.1 Managing personal data online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in TRS's data protection policy.

9.2 Security and Management of Information Systems

1. The security of TRS Information Systems and users will be reviewed regularly.
2. Virus protection will be updated regularly.
3. Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
4. Portable media may not be used without specific permission followed by an anti-virus /malware scan.
5. Unapproved software will not be allowed in work areas or attached to email.
6. Files held on the TRS's network will be regularly checked.
7. The network manager will review system capacity regularly.
8. The appropriate use of user logins and passwords to access the TRS network will be enforced for all but the youngest users.
9. All users will be expected to log off devices if systems are unattended.
10. TRS will log and record Internet use on all TRS owned devices.

9.3 Password policy

1. All users will be informed not to share passwords or information with others and not to login as another user at any time.
2. Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
3. All members of staff will have their own unique username and private passwords to access TRS systems. Staff are responsible for keeping their password private.
4. From Year 7, all pupils are provided with their own unique username and private passwords to access TRS systems. Pupils are responsible for keeping their password private.
5. We require staff and pupils to use strong passwords for access into our system.

9.4 Filtering Decisions

1. TRS Governing Body and SLT have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit pupils' exposure to online risks.
2. The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
3. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
4. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the SLT; all changes to the filtering policy are logged and recorded.
5. The SLT will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
6. 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.

9.5 Management of applications (apps) used to record pupil progress

1. The Headteacher is ultimately responsible for the security of any data or images held of pupils.
2. Apps/systems which store personal data will be risk assessed prior to use.
3. Personal staff mobile phones or devices will not be used for any apps which record and store pupil's personal details, attainment or photographs.
4. Only TRS issued devices will be used for apps that record and store children's personal details, attainment or photographs.
5. Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
6. Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

10. Responding to Online Incidents and Concerns

1. All members of the TRS community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
2. A DSL will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
3. A DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
4. Complaints about Internet misuse will be dealt with under TRS's complaints procedure.
5. Complaints about online bullying will be dealt with under TRS's antibullying policy and procedure
6. Any complaint about staff misuse will be referred to the headteacher
7. Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
8. Pupils, parents and staff will be informed of TRS's complaints procedure.
9. Staff will be informed of the complaints and whistleblowing procedure.
10. All members of the TRS community will need to be aware of the importance of confidentiality and the need to follow the official TRS procedures for reporting concerns.
11. All members of the TRS community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the TRS community.
12. TRS will manage online safety incidents in accordance with the TRS behaviour policy where appropriate.
13. TRS will inform parents/carers of any incidents of concerns as and when required.
14. After any investigations are completed, TRS will debrief, identify lessons learnt and implement any changes as required.
15. Where there is cause for concern or fear that illegal activity has taken place or is taking place then TRS will contact the Education Safeguarding Team or Kent Police via 999, if there is immediate danger or risk of harm.
16. The use of computer systems without permission, or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
17. If TRS is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
18. If an incident of concern needs to be passed beyond TRS then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.
19. Parents and pupils will need to work in partnership with TRS to resolve issues.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and the deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Links with other policies

This online safety policy is linked to our:

-
-
-
-
-
-

Appendix 1: KS2 to KS5 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile 'phone or other personal electronic device into school:** • I will switch my 'phone off once I am in school. • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding the sharing of youth produced 'nudes' and 'seminudes'

1. TRS recognises youth produced sexual imagery is a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy). We will follow the advice as set out in the non-statutory UKCCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people:
2. TRS will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing or producing sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.
3. We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
4. We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
5. We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so;
    - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented;
    - Send, delete, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will: o Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures;

- Ensure the DSL (or deputy) responds in line with the Sharing nudes and semi-nudes: advice for education settings working with children and young people Responding to incidents and safeguarding young people' guidance; o Store the device securely;
- If an 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.
- Carry out a risk assessment which considers any vulnerability of pupils involved; including carrying out relevant checks with other agencies;
- Inform parents/carers, if appropriate, about the incident and how it is being managed;
- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sharing nudes and semi-nudes: advice for education settings working with children and young people
- Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support;
- Implement appropriate sanctions 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 UKCCIS: Sharing nudes and seminudes: advice for education settings working with children and young people
- 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 SLT will also review and update any management procedures, where necessary.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

1. TRS will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
2. TRS recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
3. We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.
4. We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to pupils and other members of our community on the TRS website.

5. If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
   - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures;
     1. If appropriate, store any devices involved securely;
     2. Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk;
     3. Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies);
     4. Inform parents/carers about the incident and how it is being managed;
     5. Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support;
     6. Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
6. We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
   1. Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
7. If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or Kent Police.
8. If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy).
9. If pupils at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

Responding to concerns regarding Indecent Images of Children (IIOC)

1. TRS will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
2. We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
3. We will seek to prevent accidental access to IIOC by using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
4. If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Service.
5. If made aware of IIOC, we will: o Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures; o Store any devices involved securely;
   - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police.

6. If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:
   - Ensure that the DSL (or deputy) is informed;
   - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk ;
   - Ensure that any copies that exist of the image, for example in emails, are deleted; ○ Report concerns, as appropriate to parents/carers.

7. If made aware that indecent images of children have been found on the setting provided devices, we will:
   - Ensure that the DSL (or deputy) is informed;
   - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk ;

- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate);
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only; o Report concerns, as appropriate to parents/carers.

8. If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

o Ensure that the Headteacher is informed in line with our managing allegations against staff policy;
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy; o Quarantine any devices until police advice has been sought.

Responding to concerns regarding radicalisation or extremism online

1. TRS will take all reasonable precautions to ensure that pupils are safe from terrorist and extremist material when accessing the Internet in school and that suitable filtering is in place which takes into account the needs of pupils.
2. When concerns are noted by staff that a pupil may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with TRS's Safeguarding policy.
3. If we are concerned that staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Responding to concerns regarding cyberbullying

1. Cyberbullying, along with all other forms of bullying, of any member of the TRS's community will not be tolerated. Full details are set out in TRS policies regarding anti-bullying and behaviour.
2. All incidents of online bullying reported will be recorded.
3. There are clear procedures in place to investigate incidents or allegations and support anyone in the TRS community affected by online bullying.
4. If TRS is unclear if a criminal offence has been committed, then the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
5. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
6. TRS will take steps to identify the bully where possible and appropriate. This may include examining TRS system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
7. Pupils, staff and parents/carers will be required to work with TRS to support the approach to cyberbullying and TRS's e-safety ethos.
8. Sanctions for those involved in online or cyberbullying may include the following. o Those involved being asked to remove any material deemed to be inappropriate or offensive.
    - A service provider being contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at TRS for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to TRS's anti-bullying, behaviour policy or AUP.
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Responding to concerns regarding Online Hate

1. 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 anti-bullying and behaviour.
2. All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
3. The Police will be contacted if a criminal offence is suspected.
4. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or Kent Police.

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of IT team recording the incident**