Tenterden Schools Trust

ONLINE SAFETY POLICY

Policy is GDPR compliant

Date to Trust Board 1st April 2019 Version 2

TENTERDEN SCHOOLS TRUST

ONLINE SAFETY POLICY

This policy will be reviewed annually.

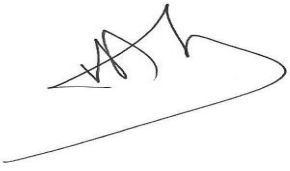
DATE OF POLICY: April 2019

DATE OF REVIEW: April 2020

Members of staff responsible for Policy:

- Chief Executive Officer
- Head of Administration
- Designated Safeguarding Lead

Signed  Chief Executive Officer

Signed  Chair of Directors

Creating an Online Safety Ethos 4
Aims and policy scope 4
Writing and reviewing the online safety policy 5
Key Responsibilities of the Community 6
Key responsibilities of the school management team are: 6
Key responsibilities of the Designated Safeguarding/Online Safety Lead are:**Error! Bookmark not defined.**
Key responsibilities of staff are: 7
Additional responsibilities for staff managing the technical environment are: 8
Key responsibilities of students are: 9
Key responsibilities of parents and carers are: 9
Online Communication and Safer Use of Technology 10
Managing the school website 10
Publishing images and videos online 11
Managing email 11
Official videoconferencing and webcam use 11
Appropriate and safe classroom use of the internet and associated devices 13
Management of school learning platforms/portals/gateways 14
Social Media Policy 14
General social media use 14
Official use of social media 15
Staff Official use of social media 17
Staff personal use of social media 18
Student use of social media 19
Use of Personal Devices and Mobile Phones 20
Rationale regarding personal devices and mobile phones 20
Expectations for safe use of personal devices and mobile phones 21
Students use of personal devices and mobile phones 21
Staff use of personal devices and mobile phones 22

Visitors use of personal devices and mobile phones 23

Policy Decisions 23

Recognising online risks 23

Internet use throughout the wider school community 24

Authorising internet access 24

Engagement Approaches 25

Engagement and education of students 25

Engagement and education of students who are considered to be vulnerable 25

Engagement and education of staff 25

Engagement and education of parents and carers 26

Managing Information Systems 27

Managing personal data online 27

Security and Management of Information Systems 27

Filtering Decisions 28

Management of applications (apps) used to record student progress 28

Responding to Online Incidents and Concerns 29

Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting") 30

Responding to concerns regarding Online Child Sexual Abuse 32

Responding to concerns regarding Indecent Images of Children (IIOC) 33

Responding to concerns regarding radicalisation or extremism online 35

Responding to concerns regarding cyberbullying 35

1. Creating an Online Safety Ethos

1.1. Aims and policy scope

1.1.1. The Tenterden Schools Trust (TST) believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile devices, or games consoles.

1.1.2. The TST identifies that the internet and information communication technologies are an important part of everyday life so students must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

1.1.3. The TST has a duty to provide the school communities with quality Internet access to raise education standards, promote student achievement, support professional work of staff and enhance the schools management functions. The TST also identifies that with this there is a clear duty to ensure that students are protected from potential harm online.

1.1.4. The purpose of this online-Safety Policy is to:

1.1.4.1. Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that the TST is a safe and secure environment.

1.1.4.2. Safeguard and protect all members of the TST's communities online.

1.1.4.3. Raise awareness with all members of the TST's communities regarding the potential risks as well as benefits of technology.

1.1.4.4. To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.

1.1.4.5. Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

1.1.5. This policy applies to all staff including the Directors, LGB's, teachers, associate 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) as well as students and parents/carers.

1.1.6. This policy applies to all access to the internet and use of information communication devices including personal devices or where students, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile device including Chromebooks, iPads and mobile phones.

1.1.7. This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding and Child Protection, Anti-bullying, Behaviour, Data Security, Image use, ICT Acceptable Use, Data Protection, Freedom of Information, Confidentiality and relevant curriculum policies including Computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships education.

1.2. Writing and reviewing the online safety policy

1.2.1. The TST's Online Safety policy has been written by the school, involving staff, students and parents/carers and building on the KCC online safety policy template with specialist advice and input as required.

1.2.2. The policy has been approved and agreed by the Leadership/Management Team and Directors.

1.2.3. The TST has appointed a member of the LGB to take lead responsibility for online safety (e-Safety).

1.2.4. The TST has appointed a member of the leadership team as the Online Safety lead.

1.2.5.

1.2.6. The TST's Online Safety Policy and its implementation will be reviewed at least annually or sooner if required.

The TST Online Safety Coordinator is: Miss V English

The TST Designated Safeguarding Lead (DSL) is: Miss V English
Each school within the Trust have their own individual DSLs

The TST Online Safety lead for the Directors is: Gillian Guthrie

Policy approved by Chief Executive Officer: ……

Policy approved by Directors: …...……Chair of Directors

Date: ……

The date for the next policy review is: April 2020

2. Key Responsibilities of the Community

2.1. Key responsibilities of the school management team are:

2.1.1. Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.

2.1.2. Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

2.1.3. Supporting the e-Safety lead in the development of an online safety culture within the school.

2.1.4. Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.

2.1.5. To ensure that suitable, age-appropriate and relevant filtering is in place to protect students from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.

2.1.6. Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

2.1.7. Ensuring that online safety is embedded within a progressive whole school curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

2.1.8. Making appropriate resources available to support the development of an online safety culture.

2.1.9. Taking responsibility for online safety incidents and liaising with external agencies as appropriate.

2.1.10. Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.

2.1.11. Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.

2.1.12. Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

2.1.13. To work with and support technical staff in monitoring the safety and security of schools systems and networks.

2.1.14. To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

2.1.15. Key responsibilities of the Designated Safeguarding/Online Safety Lead are:

2.1.16. Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.

2.1.17. Keeping up-to-date with current research, legislation and trends.

2.1.18. Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

2.1.19. Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.

2.1.20. Work with the lead for data protection and data security to ensure that practice is in line with GDPR legislation.

2.1.21. Maintaining an Online Safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.

2.1.22. Monitor the schools Online Safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Directors and other agencies as appropriate.

2.1.23. Liaising with the local authority and other local and national bodies as appropriate.

2.1.24. Reviewing and updating the Online Safety policy, ICT Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.

2.1.25. Ensuring that online safety is integrated with other appropriate school policies and procedures including GDPR legislation.

2.2. Key responsibilities of staff are:

2.2.1. Contributing to the development of the Online Safety policy.

2.2.2. Reading the school ICT Acceptable Use Policies (AUPs) and adhering to them.

2.2.3. Taking responsibility for the security of school systems and data.

2.2.4. Having an awareness of online safety issues, and how they relate to the students in their care.

2.2.5. Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.

2.2.6. Embedding Online Safety education in curriculum delivery wherever possible.

2.2.7. Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.

2.2.8. Knowing when and how to escalate online safety issues, internally and externally.

2.2.9. Being able to signpost to appropriate support available for online safety issues, internally and externally.

2.2.10. Maintaining a professional level of conduct in their personal use of technology, both on and off site.

2.2.11. Taking personal responsibility for professional development in this area.

2.3. Additional responsibilities for staff managing the technical environment are:

2.3.1. Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.

2.3.2. Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.

2.3.3. To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.

2.3.4. Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the Online Safety lead and DSL.

2.3.5. Ensuring that the use of the schools network is regularly monitored in order that any deliberate or accidental misuse can be reported to the Online Safety lead and DSL.

2.3.6. Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the Online Safety Incident Log, and appropriate action is taken as advised.

2.3.7. Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.

2.3.8. Report any breaches to the DPO in line with the Data Protection Policy and GDPR legislation and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.

2.3.9. Providing technical support and perspective to the Online Safety lead and leadership team, especially in the development and implementation of appropriate online or Online Safety policies and procedures.

2.3.10. Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack in line with GDPR legislation.

2.3.11. Ensuring that appropriate anti-virus software and system updates are installed and maintained on all machines and portable devices.

2.3.12. Ensure that appropriately strong passwords are applied and enforced for all in line with GDPR legislation.

2.4. Key responsibilities of students are:

2.4.1. Contributing to the development of the Online policy.

2.4.2. Reading the school ICT Acceptable Use Policies (AUPs), Data Protection Policy and the Online Safety Rules and adhering to them.

2.4.3. Respecting the feelings and rights of others both on and offline.

2.4.4. Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

2.4.5. Taking responsibility for keeping themselves and others safe online.

2.4.6. Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2.4.7. Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

2.5. Key responsibilities of parents and carers are:

2.5.1. Reading the school ICT Acceptable Use Policies, Data Protection Policy and Online Safety Policy, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

2.5.2. Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.

2.5.3. Role modelling safe and appropriate uses of new and emerging technology.

2.5.4. Identifying changes in behaviour that could indicate that their child is at risk of harm online.

2.5.5. Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

2.5.6. Contributing to the development of the school Online Safety policy.

2.5.7. Using school systems, such as learning platforms, and other network resources, safely and appropriately.

2.5.8. Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

3. Online Communication and Safer Use of Technology

3.1. Managing the school website

3.1.1. The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.

3.1.2. The contact details on the website will be the school address, email and telephone number. Staff or students' personal information will not be published without consent in line with GDPR guidelines.

3.1.3. The Chief Executive Officer will take overall editorial responsibility for online content published by the TST and will ensure that content published is accurate and appropriate. The TST website will comply with the TST's guidelines for publications including respect for intellectual property rights, privacy policies, GDPR legislation and copyright.

3.1.4. Students work will only be published with their permission or that of their parents/carers.

3.1.5. The administrator account for the school website will be safeguarded with an appropriately strong password in line with GDPR legislation.

3.1.6. The school will post information about safeguarding, including online safety on the school website.

3.2. Publishing images and videos online

3.2.1. The school will ensure that all images are used in accordance with the school image use policy.

3.2.2. In line with the schools image policy, written permission from parents or carers will always be obtained before images/videos of students are electronically published, in line with GDPR legislation.

3.3. Managing email

3.3.1. Students may only use school provided email accounts for educational purposes.

3.3.2. All members of staff are provided with a specific school email address to use for any official communication.

3.3.3. The use of personal email addresses by staff for any official school business is not permitted.

3.3.4. The forwarding of any inappropriate chain messages/emails etc. is not permitted.

3.3.5. Any electronic communication which contains any content which could be subject to GDPR legislation must only be sent using secure and password protected methods.

3.3.6. Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school e-Safety incident log.

3.3.7. Sensitive or personal information will only be shared via email in accordance with GDPR legislation.

3.3.8. Access in school to external personal email accounts may be blocked.

3.3.9. Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper would be.

3.3.10. School email addresses and other official contact details will not be used for setting up personal social media accounts.

3.4. Official videoconferencing and webcam use

3.4.1. All video conferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.

3.4.2. The equipment will be kept securely and if necessary locked away when not in use.

3.4.3. School videoconferencing equipment will not be taken off school premises without permission.

3.4.4. Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

3.4.5. Staff will ensure that external videoconferences are suitably risk assessed and that accounts and systems used to access events are appropriately safe and secure.

3.4.6. Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

3.4.7. Students will ask permission from a teacher before making or answering a videoconference call or message.

3.4.8. Videoconferencing will be supervised appropriately for the students' age and ability.

3.4.9. Parents and carers consent will be obtained prior to children taking part in videoconferences.

3.4.10. Video conferencing will take place via official and approved communication channels following a robust risk assessment.

3.4.11. Only key administrators will be given access to videoconferencing administration areas or remote control pages.

3.4.12. Unique login and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

3.4.13. When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely and in accordance with the Data Retention Policy.

3.4.14. If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.

3.4.15. The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

3.5. Appropriate and safe classroom use of the internet and associated devices

3.5.1. The school's internet access will be designed to enhance and extend education.

3.5.2. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.

3.5.3. Students will use age and ability appropriate tools to search the Internet for content. Homewood School uses Lightspeed Systems Web Filtering managed by Kent County Council.

3.5.4. Internet use is a key feature of educational access and all students will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.

3.5.5. The school will ensure that the use of Internet-derived materials by staff and students complies with copyright law and is GDPR compliant and acknowledge the source of information.

3.5.6. All members of staff are aware that they cannot rely on filtering alone to safeguard students and supervision, classroom management and education about safe and responsible use is essential.

3.5.7. Supervision of students will be appropriate to their age, ability and understanding when using technology.

3.5.8. All TST school owned devices will be used in accordance with the school ICT Acceptable Use Policy and with appropriate safety and security measures in place. We use Lightspeed Mobile Device Management or Google Device Management to profile all of our mobile devices in the Trust.

3.5.9. Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3.5.10. The school will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.

3.5.11. Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3.5.12. The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

3.5.13. Members of staff will always evaluate websites, tools and apps fully, including performing a Data Protection Impact Assessment if necessary before use in the classroom or recommending for use at home.

3.6. Management of school learning platforms/portals/gateways

3.6.1. SLT and staff will regularly monitor the usage of the LP by students and staff in all areas, in particular message and communication tools and publishing facilities.

3.6.2. Students/staff will be advised about acceptable conduct and use when using the LP.

3.6.3. Only members of the current student, parent/carers and staff community will have access to the LP.

3.6.4. All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

3.6.5. When staff, students etc. leave the school their account or rights to specific school areas will be disabled.

3.6.6. Any concerns about content on the LP may be recorded and dealt with in the following ways:

3.6.6.1. The user will be asked to remove any material deemed to be inappropriate or offensive.

3.6.6.2. The material will be removed by the site administrator if the user does not comply.

3.6.6.3. Access to the LP for the user may be suspended.

3.6.6.4. The user will need to discuss the issues with a member of leadership before reinstatement.

3.6.6.5. A student's parent/carer may be informed.

3.6.7. Students may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

4. Social Media Policy

4.1. General social media use

4.1.1. Expectations regarding safe and responsible use of social media will apply to all members of the TST communities 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.

4.1.2. All members of the TST communities will be encouraged to engage in social media in a positive, safe and responsible manner at all times.

4.1.3. Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the TST communities.

4.1.4. All members of the TST communities 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.

4.1.5. The TST will control student and staff access to social media and social networking sites whilst on site and using school provided devices and systems.

4.1.6. The use of social networking applications during school hours for personal use is not permitted.

4.1.7. Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

4.1.8. Any concerns regarding the online conduct of any member of the TST on social media sites should be reported to the Trust leadership team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

4.1.9. Any breaches of school 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 school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

4.2. Official use of social media

4.2.1. Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.

4.2.2. Official use of social media sites as communication tools will be risk assessed and formally approved by the Chief Executive Officer.

4.2.3. Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.

4.2.4. Staff will use school provided email addresses to register for and manage official school approved social media channels.

4.2.5. Members of staff running official school social media channels will be aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.

4.2.6. All communication on official school social media platforms will be clear, transparent and open to scrutiny.

4.2.7. Any online publication on official school social media sites will comply with legal requirements including the Data Protection Act 2018, right to privacy conferred by the Human Rights Act 1998, GDPR legislation or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.

4.2.8. Official social media use by the school will be in line with existing policies including anti-bullying and child protection.

4.2.9. Images or videos of students will only be shared on official school social media sites/channels in accordance with the school image use policy under GDPR legislation.

4.2.10. Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.

4.2.11. 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 TST website and take place with written approval from the Leadership Teams.

4.2.12. Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.

4.2.13. Parents/Carers and students will be informed of any official school social media use, along with expectations for safe use and school action taken to safeguard the community.

4.2.14. TST official social media channels are managed by senior staff within the individual schools and Nursery.

4.2.15. Public communications on behalf of the school will, where possible, be read and agreed by at least one other colleague.

4.2.16. The school's social media accounts will link back to the school's website and/or ICT Acceptable Use Policy to demonstrate that the accounts are official.

4.2.17. The TST 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.

4.3. Staff Official use of social media

4.3.1. If members of staff are participating in online activity as part of their capacity as an employee of the Trust, then they are requested to be professional at all times and that they are an ambassador for the Tenterden Schools Trust.

4.3.2. 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 the Trust.

4.3.3. 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.

4.3.4. Staff using social media officially will always act within the legal frameworks they would adhere to within the Trust, including libel, defamation, confidentiality, copyright, data protection, GDPR as well as equalities laws.

4.3.5. Staff must ensure that any image posted on the Trusts social media channels have appropriate written parental consent.

4.3.6. Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the Trust unless they are authorised to do so.

4.3.7. Staff using social media officially will inform their line manager, the Trust's online Safety lead and/or the Chief Executive Officer of any concerns such as criticism or inappropriate content posted online.

4.3.8. Staff will not engage with any direct or private messaging with students or parents/carers through social media and should communicate via their schools.

4.4. Staff personal use of social media

4.4.1. Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

4.4.2. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the Trusts ICT Acceptable Use Policy.

4.4.3. All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with line manager/ member of Leadership Team/Chief Executive Officer.

4.4.4. If ongoing contact with students is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools in line with GDPR legislation.

4.4.5. All communication between staff and members of the school community on school business will take place via official approved communication channels (email and school phone system.) Staff must not use personal accounts or information to make contact with students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher/Line Manager.

4.4.6. Any communication from students/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.

4.4.7. Information staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

4.4.8. All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential. It is recommend that first and middle names are used rather than surname. Staff should not state that they work in the TST.

4.4.9. All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with schools policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

4.4.10. Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

4.4.11. Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.

4.4.12. Members of staff must not identify themselves as employees of the TST on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider school community.

4.4.13. Members of staff will ensure that they do not represent their personal views as that of the school on social media.

4.4.14. School email addresses will not be used for setting up personal social media accounts.

4.4.15. Members of staff who follow/like the schools social media channels will be advised to use dedicated professionals accounts where possible to avoid blurring professional boundaries.

4.5. Student use of social media

4.5.1. Safe and responsible use of social media sites will be outlined for students and their parents as part of the TST ICT Acceptable Use Policy.

4.5.2. Personal publishing on social media sites will be taught to students 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.

4.5.3. Students 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, school attended. Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

4.5.4. Students 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.

4.5.5. Students will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

4.5.6. Students 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.

4.5.7. Students will be informed of any official social media use with students and written parental consent will be obtained, as required.

4.5.8. Any official social media activity involving students will be moderated by the TST where possible.

4.5.9. The TST is aware that many popular social media sites state that they are not for children under the age of 13, therefore the TST will not create accounts within school specifically for children under this age.

4.5.10. Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

5. Use of Personal Devices and Mobile Phones

5.1. Rationale regarding personal devices and mobile phones

5.1.1. The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the TST to take steps to ensure that mobile phones and personal devices are used responsibly.

5.1.2. The use of mobile phones and other personal devices by young people and adults will be decided by the school and covered in appropriate policies including the TST's ICT Acceptable Use Policy.

5.1.3. The TST recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers but requires that such technologies need to be used safely and appropriately within the Trusts communities.

5.2. Expectations for safe use of personal devices and mobile phones

5.2.1. Electronic devices of all kinds that are brought in to school are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

5.2.2. Mobile phones and personal devices are not permitted to be used in certain areas within the schools such as changing rooms and toilets.

5.2.3. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Trust community and any breaches will be dealt with as part of the TST's discipline/behaviour policy.

5.2.4. Members of staff will have access to a school/work phone number and email address where contact with students or parents/carers is required.

5.2.5. All members of the TST will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

5.2.6. All members of the TST 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.

5.2.7. All members of the TST 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 the TST's policies.

5.2.8. TST's mobile phones and devices must always be used in accordance with the ICT Acceptable Use Policy.

5.2.9. School mobile phones and devices used for communication with parents and students must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

5.3. Students use of personal devices and mobile phones

5.3.1. Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.

5.3.2. All use of mobile phones and personal devices by children will take place in accordance with the ICT Acceptable Use Policy.

5.3.3. Mobile phones and personal devices will be switched off and kept out of sight during classroom lessons and while moving between lessons.

5.3.4. Mobile phones or personal devices will not be used by students during lessons or formal school 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.

5.3.5. If a student needs to contact his/her parents/carers they will be encouraged to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school offices. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Chief Executive Officer.

5.3.6. Phones and devices must not be taken into examinations. Students 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 student's withdrawal from either that examination or all examinations.

5.3.7. If a student breaches the TST's policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released to parents/carers in accordance with the TST's policy.

5.3.8. School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device may be searched by a member of the Leadership team or the online Safety Officer with the consent of the student or parent/carer.

5.3.9. If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

5.4. Staff use of personal devices and mobile phones

5.4.1. Members of staff are not permitted to use their own personal phones or devices for contacting students and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with leaders/managers.

5.4.2. Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.

5.4.3. Staff will not use any personal devices directly with students and will only use work-provided equipment during lessons/educational activities.

5.4.4. Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.

5.4.5. Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.

5.4.6. Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team or in emergency circumstances.

5.4.7. Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.

5.4.8. If a member of staff breaches the TST's policy then disciplinary action will be taken.

5.4.9. 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 responded to following the allegations management policy.

5.5. Visitors use of personal devices and mobile phones

5.5.1. Parents/carers and visitors must use mobile phones and personal devices in accordance with the TST's ICT Acceptable Use policy.

5.5.2. Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

5.5.3. The Trust will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

5.5.4. Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

6. Policy Decisions

6.1. Recognising online risks

6.1.1. The TST is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

6.1.2. Emerging technologies will be examined for educational benefit and the TST leadership team will ensure that appropriate risk assessments are carried out before use in the Trust is allowed.

6.1.3. The schools will ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content.

6.1.4. The school 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 school computer or device.

6.1.5. The TST will audit technology use to establish if the Online Safety Policy is adequate and that the implementation of the policy is appropriate.

6.1.6. Methods to identify, assess and minimise online risks will be reviewed regularly by the TST's leadership team.

6.1.7. Filtering decisions, internet access and device use by students and staff will be reviewed regularly by the Learning Systems Team Leader.

6.2. Internet use throughout the wider school community

6.2.1. The TST will liaise with local organisations to establish a common approach to online e-Safety.

6.2.2. The TST will provide an ICT Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.

6.3. Authorising internet access

6.3.1. The TST will maintain a current record of all staff and students who are granted access to the school's electronic communications.

6.3.2. All staff, students and visitors will read and sign the Trusts ICT Acceptable Use Policy before using any school ICT resources.

6.3.3. Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability.

6.3.4. Parents will be asked to read the TST's ICT Acceptable Use Policy for student access and discuss it with their child, where appropriate.

6.3.5. When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the student(s).

7. Engagement Approaches

7.1. Engagement and education of students

7.1.1. An online Safety curriculum will be established and embedded throughout the whole of the Trust, to raise awareness regarding the importance of safe and responsible internet use amongst students.

7.1.2. Education about safe and responsible use will precede internet access.

7.1.3. Students input will be sought when writing and developing school online safety policies and practices.

7.1.4. Students will be supported in reading and understanding the TST's ICT Acceptable Use Policy in a way which suits their age and ability.

7.1.5. All users will be informed that network and Internet use will be monitored.

7.1.6. Online Safety will be included in the PSHE, Citizenship and Computing programmes of study covering both safe school and home use.

7.1.7. Online Safety education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.

7.1.8. The Online Safety Rules posters will be posted in all rooms with Internet access.

7.1.9. Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

7.1.10. External support will be used to complement and support the schools internal e-Safety education approaches.

7.2. Engagement and education of students who are considered to be vulnerable

7.2.1. The TST is aware that some students may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online Safety education is given, with input from specialist staff as appropriate (e.g. SENCO).

7.3. Engagement and education of staff

7.3.1. 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 school safeguarding practice.

7.3.2. To protect all staff and students, the schools will implement the TST ICT Acceptable Use Policy which highlights appropriate online conduct and communication.

7.3.3. Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

7.3.4. 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.

7.3.5. Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.

7.3.6. All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. 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.

7.4. Engagement and education of parents and carers

7.4.1. The TST recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

7.4.2. Parents/Carers' attention will be drawn to the school Online Safety Policy and expectations in newsletters, letters and on the TST websites.

7.4.3. A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. consultation days, focus days and transition events.

7.4.4. Parents will be requested to read the e-Safety rules and information as part of the Home School Agreement.

7.4.5. Information and guidance for parents on online safety will be made available to parents in a variety of formats, such as the school website and Digital Parenting Magazine.

8. Managing Information Systems

8.1. Managing personal data online

8.1.1. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and GDPR regulations.

8.1.2. Full information regarding the schools approach to data protection and information governance can be found in the TST Data Protection Policy.

8.2. Security and Management of Information Systems

8.2.1. The security of the school information systems and users will be reviewed regularly.

8.2.2. Virus protection will be updated regularly.

8.2.3. Steps will be taken going forward to ensure that 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.

8.2.4. Unapproved software, websites or services is not allowed.

8.2.5. Files held on the school's network will be regularly checked.

8.2.6. The Network Manager will review system capacity regularly.

8.2.7. The appropriate use of user logins and passwords to access the school network will be enforced for all.

8.2.8. All users will be expected to log off or lock their screens/devices if systems are unattended.

8.2.9. The TST will log and record internet use on all devices using Lightspeed Systems Web Filtering managed by Kent County Council.

8.2.10. All users will be informed not to share passwords or information with others and not to login as another user at any time.
Staff and students must always keep their password private and must not share it with others or leave it where others can find it.
All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
Students are provided with their own unique username and private passwords to access school systems. Students are responsible for keeping their password private.
We require staff and Students to use STRONG passwords for access into our system in line with GDPR legislation.

8.3. Filtering Decisions

8.3.1. The TST's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our students, with advice from technical, educational and safeguarding staff.

8.3.2. The TST uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our students.

8.3.3. The TST uses Lightspeed Systems Web filtering which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.

8.3.4. The TST will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and students from being accidentally or deliberately exposed to unsuitable content.

8.3.5. The school will work with KCC and the Schools Broadband team or broadband/filtering provider to ensure the filtering policy is continually reviewed.

8.3.6. The TST will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all students) will be made aware of.

8.3.7. If staff or students discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and/or the Network Manager and will then be recorded and escalated as appropriate.

8.3.8. Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.

8.3.9. The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.

8.3.10. Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

8.4. Management of applications (apps) used to record student progress

8.4.1. The Chief Executive Officer is ultimately responsible for the security of any data or images held of students.

8.4.2. Apps/systems which store personal data will be risk assessed prior to use.

8.4.3. Personal staff mobile phones or devices will not be used for any apps which record and store student's personal details, attainment or photographs.

8.4.4. Only school issued devices will be used for apps that record and store student's personal details, attainment or photographs.

8.4.5. Steps will be taken going forward to ensure that devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.

8.4.6. 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.

9. Responding to Online Incidents and Concerns

9.1. All members of the TST will be informed about the procedure for reporting online concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

9.2. The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.

9.3. The Designated Safeguarding Lead (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.

9.4. Complaints about Internet misuse will be dealt with under the School's complaints procedure.

9.5. Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure

9.6. Any complaint about staff misuse will be referred to the Chief Executive Officer.

9.7. Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

9.8. Students, parents and staff will be informed of the schools complaints procedure.

9.9. Staff will be informed of the complaints and whistleblowing procedure.

9.10. All members of the Trust's community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns in line with GDPR legislation.

9.11. All members of the school 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 school community.

9.12. The TST will manage online Safety incidents in accordance with the TST discipline/behaviour policy where appropriate.

9.13. The TST will inform parents/carers of any incidents or concerns as and when required.

9.14. After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

9.15. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Kent Police via 999 if there is immediate danger or risk of harm.

9.16. 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.

9.17. If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.

9.18. If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Kent.

9.19. Parents and students will need to work in partnership with the school to resolve issues.

9.20. Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

9.20.1. The TST will ensure that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating incident images of children.

9.20.2. The Trust will implement preventative approaches via a range of age and ability appropriate educational approaches for students, staff and parents/carers.

9.20.3. The TST views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

9.20.4. If the Trust is made aware of incident involving indecent images of a child the school will:

9.20.4.1. Act in accordance with the schools Child Protection and Safeguarding Policy and the relevant Kent Safeguarding Child Boards procedures.

9.20.4.2. Immediately notify the Designated Safeguarding Lead.

9.20.4.3. Store the device securely.

9.20.4.4. Carry out a risk assessment in relation to the student(s) involved.

9.20.4.5. Consider the vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).

9.20.4.6. Make a referral to children's social care and/or the police (as needed/appropriate).

9.20.4.7. Put the necessary safeguards in place for students e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.

9.20.4.8. Inform parents/carers about the incident and how it is being managed.

9.20.4.9. Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.

9.20.4.10. Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.

9.20.5. The school will not view the image unless there is a clear need or reason to do so.

9.20.6. The school will not send, share or save indecent images of children and will not allow or request children to do so.

9.20.7. If an indecent image has been taken or shared on the school network or devices then the school will take action to block access to all users and isolate the image.

9.20.8. The school will need to involve or consult the police if images are considered to be illegal.

9.20.9. The school will take action regarding indecent images, regardless of the use of school equipment or personal equipment, both on and off the premises.

9.20.10. The school will follow the guidance (including the decision making flow chart and risk assessment template) as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it".

9.20.11. The school will ensure that all members of the community are aware of sources of support.

9.21. Responding to concerns regarding Online Child Sexual Abuse

9.21.1. The TST will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

9.21.2. The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for students, staff and parents/carers.

9.21.3. The TST views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

9.21.4. If the Trust is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

9.21.5. If the Trust is made aware of an incident involving online child sexual abuse of a child then the school will:

9.21.5.1. Act in accordance with the schools Child Protection and Safeguarding Policy and the relevant Kent Safeguarding Child Boards procedures.

9.21.5.2. Immediately notify the Designated Safeguarding Lead.

9.21.5.3. Store any devices involved securely.

9.21.5.4. Immediately inform Kent police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: https://www.ceop.police.uk/safety-centre/.

9.21.5.5. Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse.

9.21.5.6. Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).

9.21.5.7. Make a referral to children's social care (if needed/appropriate).

9.21.5.8. Put the necessary safeguards in place for student(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.

9.21.5.9. Inform parents/carers about the incident and how it is being managed.

9.21.5.10. Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

9.21.6. The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.

9.21.7. The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.

9.21.8. If students at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

9.21.9. The school will ensure that the Click CEOP report button is visible and available to students and other members of the school community, for example including the CEOP report button on the school website and on the intranet.

9.22. Responding to concerns regarding Indecent Images of Children (IIOC)

9.22.1. The TST will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

9.22.2. The TST will take action regarding Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.

9.22.3. The school will take action to prevent accidental access to Indecent Images of Children (IIOC) for example using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.

9.22.4. If the TST is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

9.22.5. If the TST is made aware of Indecent Images of Children (IIOC) then the TST will:

9.22.5.1. Act in accordance with the individual school's Child Protection and Safeguarding Policies and the relevant Kent Safeguarding Child Boards procedures.

9.22.5.2. Immediately notify the school Designated Safeguard Lead.

9.22.5.3. Store any devices involved securely.

9.22.5.4. Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

9.22.6. If the TST is made aware that a member of staff or a student has been inadvertently exposed to indecent images of children whilst using the internet then the school will:

9.22.6.1. Ensure that the Designated Safeguard Lead is informed.

9.22.6.2. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk and Kent County Council.

9.22.6.3. If at all possible ensure that any copies that exist of the image, for example in emails, are deleted.

9.22.7. If the TST is made aware that indecent images of children have been found on the schools electronic devices then the school will:

9.22.7.1. Ensure that the Designated Safeguard Lead is informed.

9.22.7.2. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.

9.22.7.3. Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).

9.22.7.4. 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.

9.22.8. If the TST is made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:

9.22.8.1. Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.

9.22.8.2. Contact the police regarding the images and quarantine any devices involved until police advice has been sought.

9.22.8.3. Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.

9.22.8.4. Follow the appropriate school policies regarding conduct.

9.23. Responding to concerns regarding radicalisation or extremism online

9.23.1. The TST will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of students.

9.23.2. When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school Safeguarding Policy.

9.24. Responding to concerns regarding cyberbullying

9.24.1. Cyberbullying, along with all other forms of bullying, of any member of the TST Community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

9.24.2. All incidents of online bullying reported will be recorded.

9.24.3. There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

9.24.4. If the TST is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

9.24.5. Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.

9.24.6. The TST will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying

and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

9.24.7. Students, staff and parents/carers will be required to work with the TST to support the approach to cyberbullying and the TST's online Safety ethos.

9.24.8. Sanctions for those involved in online or cyberbullying may include:

9.24.8.1. Those involved will be asked to remove any material deemed to be inappropriate or offensive.

9.24.8.2. A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.

9.24.8.3. Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools Anti-bullying, Behaviour or ICT Acceptable Use Policy.

9.24.8.4. Parent/carers of students involved in online bullying will be informed.

9.24.8.5. The Police will be contacted if a criminal offence is suspected.