POLICY FOR	Online Safety
PERSON RESPONSIBLE	The Head teacher
DATE REVISED	JANUARY 2017
DATE NEXT REVIEW	JANUARY 2018

Our online safety policy

This policy and the procedures that underpin it, apply to all staff, including senior managers and the board of trustees, the Board of Governors, paid staff, volunteers, agency staff, students, visitors, external contractors and anyone working on behalf of the Holmesdale school.
This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones. This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation procedures and relevant curriculum policies.

The purpose of the policy is to:

- safeguard and protect all members of THS community online;
- identify the key principles expected of all members of THS with regards to the safe and responsible use technology to ensure that a safe and secure environment is established in school;
- raise awareness with all members of THS community regarding the potential risks as well as benefits of technology;
- make explicit that all members of THS community understand their essential role and responsibilities in ensuring safety and wellbeing of others, both on and offline;
- make clear to members of the community how to access and seek support and guidance;
- 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;
- identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

We recognise that:

- The school has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- The use of information technology is an essential part of all our lives; our students must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

- Online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- There is a clear duty to ensure that all children and staff are protected from potential harm online.
- All children, regardless of age, disability, gender, racial heritage, religious belief, sexual orientation or identity, have the right to equal protection from all types of harm or abuse; working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

Responsibilities:

Head Teacher:

is responsible for:

- promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school communities;
- ensuring that online safety is viewed by members of THS community as a safeguarding issue and proactively developing a robust online safety culture;
- supporting the Designated Safeguarding Lead (DSL) and the named online safety officer to have sufficient time and resources to fulfil their online safety role and responsibilities;
- ensuring there are appropriate and up-to-date policies and procedures regarding online safety;
- ensuring that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material;
- working with and supporting technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored;
- making certain 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;
- ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours;
- verifying that external agencies and support are liaised with as appropriate;
- ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- overseeing that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices;

- ensuring a member of the Governing Body (or committee, board member as appropriate) is identified with a lead responsibility for supporting online safety, auditing and evaluating current online safety practice to identify strengths and areas for improvement.

Online Safety Lead

The online lead have responsibility for coordinating the whole school/setting online safety approaches, supporting and raising awareness with the wider community, promoting a safe and responsible online safety culture and acting as the lead for dealing with online

These responsibilities include:

- acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate;
- keeping up-to-date with current research, legislation and trends regarding online safety;
- coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day;
- ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches;
- work with the lead for data protection and data security to ensure that practice is in line with current legislation;
- maintaining a record of online safety concerns/incidents and actions taken as part of school's safeguarding recording structures and mechanisms;
- monitor the online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need to report to the Leadership team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures;
- liaising with the local authority and other local and national bodies, as appropriate;
- review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input;
- ensuring that online safety is integrated with other appropriate school policies and procedures;
- initiating an online safety team/group with input from all stakeholder group;
- meet regularly with the governor/board/committee member with a lead responsibility for online safety.

Staff

The key responsibilities for all staff are:

- contributing to the development of online safety policy and procedures;
- reading the school Acceptable Use Policies (AUPs) and adhering to them;
- taking responsibility for the security of school/setting systems and data;
- having an awareness of a range of different online safety issues and how they may relate to the children in their care;
- modelling good practice when using new and emerging technologies;

- embedding online safety education in curriculum delivery wherever possible;
- identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures;
- knowing when and how to escalate online safety issues, internally and externally;
- being able to signpost to appropriate support available for online safety issues, internally and externally;
- maintaining a professional level of conduct in their personal use of technology, both on and off site & adhering to the school code of conduct as regards appropriate use of social networks etc;
- demonstrating an emphasis on positive learning opportunities;
- taking personal responsibility for professional development in this area.

Additional responsibilities for staff managing the technical Environment

Including the above, the additional responsibilities of the ICT team are:

- providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised;
- taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team;
- ensuring that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices;
- ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL;
- ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL;
- reporting any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised;
- developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure;
- reporting any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues;
- providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures;
- ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack;
- ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices;
- ensuring that appropriately strong passwords are applied and enforced for all but the youngest users.

Students

The key responsibilities of children and young people are:

- contributing to the development of online safety policies;
- reading the school/setting Acceptable Use Policies (AUPs) and adhering to them;
- respecting the feelings and rights of others both on and offline.
- seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues;
- taking responsibility for keeping themselves and others safe online;
- taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies;
- assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

Parents/ Carers

The key responsibilities of parents/carers are:

- reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate;
- discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home;
- role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online;
- seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns;
- contributing to the development of the school/setting online safety policies.
- using school systems, such as learning platforms, and other network resources, safely and appropriately;
- taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Managing the school website

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE). The contact details on the website will be the school/setting address, email and telephone number. Staff or pupils' personal information will not be published.

- The Head Teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- Pupils' work will be published with their permission or that of their parents/carers.

- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

Publishing images and videos online

THS will ensure that all images and videos shared online are used in accordance with the school image use policy.

The school/setting will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct.
In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

Managing email

- Pupils may only use school provided email accounts for educational purposes.
- The use of personal email addresses by staff for any official school/setting business is not permitted.
- 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 (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to email systems will always take place in accordance to data protection legislation and in line with the school's code of conduct.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

Appropriate and safe classroom use of the internet and any associated devices

Internet use is a key feature of educational access and all children will receive appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
The school's internet access will be designed to enhance and extend education. The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

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

- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.

Social Media
Expectations regarding safe and responsible use of social media will apply to all members of THS and exist in order to safeguard both the school and the wider community, on and offline.

- All members THS 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.

THS will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.

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

Any concerns regarding the online conduct of any member of THS on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour, child protection.
Any breaches of school policy may result in criminal, disciplinary or civil action being taken.

Official use of social media

- Official use of social media sites will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by senior leaders.
- Members of staff running official social media channels will ensure they are 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.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred

by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected and take place with written approval from THS 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.

Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school/setting Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' 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 Designated Safeguarding Lead and/or the Head Teacher.
- If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use official school provided communication tools.
- All communication between staff and members of THS community on school business will take place via official approved communication channels.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head Teacher.
- Any communication from pupils/parents received on personal social media accounts will be reported to the school's designated safeguarding lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- 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.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their

social media use is compatible with their professional role and is in accordance with school's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online.
- Members of staff will notify the Leadership 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 schools.
- Members of staff are encouraged not to identify themselves as employees of 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 community.
- Members of staff will ensure that they do not represent their personal views as that of THS on social media.
- THS email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like THS social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

Staff official use of social media

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

- 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 school.
- 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.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of THS unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the Head Teacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.

Pupils' use of social media
Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
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.
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, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

- 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.
- 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.
- 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.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.

THS is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts within school specifically for children under this age.
Any concerns regarding pupils' 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.
Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

Use of Personal Devices and Mobile Phones
The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of THS community to take steps to ensure that mobile phones and personal devices are used responsibly.
THS recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

Expectations for safe use of personal devices and mobile phones
All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. THS 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.

- Mobile phones and personal devices are not permitted to be used in certain areas within the school's site such as changing rooms and toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the behaviour policy.
- All members of THS community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of THS 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.
- All members of THS 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 THS policies.
- Mobile phones and devices must always be used in accordance with the Acceptable Use Policy.
- School 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.

Pupils' use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.
- Pupils' personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during lessons and while moving between lessons. Mobile phones or personal devices will not be used by pupils 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.
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Leadership Team.
- If a pupil needs to contact his/her parents/carers they will be allowed 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 office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Head Teacher.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Mobile phones and personal 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.

- If a pupil breaches THS policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- 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 then the device will be handed over to the police for further investigation.

Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data Acceptable Use
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- 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.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school's allegations management policy.

Visitors' use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with THS image use policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- 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.

Reducing online risks
THS 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 the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

THS will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.
THS 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 always possible to guarantee that access to unsuitable material will never occur via a school computer or device.

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

Internet use throughout the wider school community
The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
THS will provide an Acceptable Use Policy for any guest/visitor who needs to access the school's' computer system or internet on site

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly. 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.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the school's expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.
- The network manager will review system capacity regularly.

- The appropriate use of user logins and passwords to access the school network will be enforced for all.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices.
- 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 pupils 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.
- Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- All monitoring of school owned/provided systems will take place to safeguard members of the community. All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- THS filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The 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.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the Head Teacher.

- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of THS complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members THS community will need to be aware of the importance of confidentiality and the need to follow the official THS procedures for reporting concerns.
- 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 THS community.
- THS will manage online safety (e-Safety) incidents in accordance with the school's behaviour policy.
- The school will inform parents/carers of any incidents of concerns as and when required.
- 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 101 or 999 if there is immediate danger or risk of harm.
- 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.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond THS community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Kent. Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

THS will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
The school will implement preventative approaches via a range of appropriate educational approaches for pupils, staff and parents/carers.
THS views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB "Responding to youth produced sexual imagery" guidance

If the school is made aware of incident involving creating youth produced sexual imagery the school will:

- Act in accordance with the school child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the designated safeguarding lead who will then:
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Refer to the school's behaviour leads who will then implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.
- 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.
- Inform parents/carers about the incident and how it is being managed.
- The school will not view an 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 (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- 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.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.

- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

THS 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.

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

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

If the school 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.

If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSET team by the DSL.

If the school are made aware of incident involving online child sexual abuse of a child then the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform Kent police via 101 (using 999 if a child is at immediate risk)
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safetycentre/
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- 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.
- 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.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils 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.

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

Responding to concerns regarding Indecent Images of Children (IIOC)

THS 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.
The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
The school will take action to prevent access accidental access to of 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.
If the school 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.
If the school is made aware of Indecent Images of Children (IIOC) then the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the school Designated Safeguard Lead.
- Store any devices involved securely.
- 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).

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

- Ensure that the Designated Safeguard Lead 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.

If the school is made aware that indecent images of children have been found on the school's electronic devices then the school will:

- Ensure that the Designated Safeguard Lead 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 services (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.

If the school 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:

- Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
- Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school's managing allegations policy.
- Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation and extremism online

THS will take all reasonable precautions to ensure that children 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.

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 safeguarding policy.

Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.

Responding to concerns regarding cyberbullying

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

All incidents of online bullying reported will be recorded.

If the school 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.

Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.

The school 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.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in online or cyberbullying may include:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- 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 school's anti-bullying, behaviour policy or Acceptable Use Policy.
- 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

Online hate in THS will not be tolerated. Further details are set out in the policies regarding anti-bullying and behaviour.

All incidents of online hate reported to the school will be recorded.

All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.

The Police will be contacted if a criminal offence is suspected. If the school 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.