Thomas's

ONLINE SAFETY POLICY

This policy will be reviewed annually or in response to changes in legislation		
Created	January 2020	Vice Principal
Last Review	August 2023	Designated Safeguarding Leads, Online Safety Officer, Director of IT, Head of Compliance
Approved	September 2023	Education Board

This Policy applies to all year groups at Thomas's Schools, including the EYFS.

Thomas's London Day Schools operates as a united group of schools with a similar ethos and values and as such is referred to as a singular body.

This Policy should be read in conjunction with Thomas's Safeguarding and Child Protection Policy, Anti-bullying Policy, Behaviour Policy, Communication Policy, ICT Acceptable Use Policies and Agreements.

1. *INTRODUCTION*

As active participants in a digital world our broad curriculum and our pupils' personal goals require regular use of a variety of IT systems and communication tools. While developments in technology may bring staff and pupils into contact with a wide variety of influences, some of which may be unsuitable, our schools provide a progressive and appropriate education programme for staff, pupils and parents.

This Online Safety Policy relates to all members of the Thomas's community who have access to, and are users of IT systems and resources both in and out of school and applies to all electronic devices and services provided, whether accessed within school or an external location.

2. *AIMS*

The aims of this policy are to ensure that:

- staff and pupils have the knowledge, skills and confidence to become safe and responsible users of the Internet and other communications technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff and pupils are protected from potential risk in their use of ICT in their everyday work;
- pupils, staff and parents are aware of the School's expectations and respect the privacy of all members of the school community.

The main areas of risk for our school community can be summarised as follows:

	Commercial	Aggressive	Sexual	Values
Content Child as recipient	Advertising Spam Copyright Sponsorship Hacking	Violent content Hateful Content	Pornographic content Unwelcome sexual comments	Bias Racist and extremist content Misleading info/advice Body Image and self-esteem Distressing or offensive content
Contact Child as participant	Tracking Harvesting data Sharing personal information	Being bullied, harassed or stalked	Meeting strangers Sexualised bullying (including sexting) Grooming Online Child Sexual Exploitation	Self-harm and suicide Unwelcome persuasions Grooming for extremism
Conduct Child as actor	Illegal downloading Hacking Gambling Privacy Copyright	Bullying, harassing or stalking others	Creating and uploading inappropriate or illegal content (including "sexting") Unhealthy/inappropriate sexual relationships Child on child sexualised or harmful behaviour	Providing misleading information and advice Encouraging others to take risks online Sharing extremist views Problematic Internet Use or "Addiction" Plagiarism

3. ROLES AND RESPONSIBILITIES

3.1 All Users

All users are responsible for using the school IT and communication systems in accordance with the relevant Safeguarding and Child Protection, Behaviour and ICT Acceptable Use Policies. All staff and pupils will sign an ICT Acceptable Use Agreement and be trained in online safety.

All users are expected to model safe, responsible and professional behaviours in their own use of technology. Responsibilities include:

- to supervise (we recommend the use of Apple Classroom to monitor the use of iPads being used) and guide pupils carefully when engaged in learning activities involving online technology, and use common-sense strategies in learning resource areas where older pupils have more flexible access.
- to report any misuse to the Online Safety Officer/Safeguarding Team in line with the reporting procedures outlined in the Safeguarding policy. See Appendix 1 for specific sanctions related to technology use.
- to take professional, reasonable precautions when working with pupils, previewing websites and resources before use; and using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

3.2 Safeguarding Team

The Designated Safeguarding Lead (DSL) for each school takes lead responsibility for online safety including regularly reviewing the effectiveness of school filtering and monitoring systems.

They are supported by the Online Safety Officer who will ensure that all staff receive suitable training and development to carry out their responsibilities in a safe and supportive environment. A record is kept and reviewed regularly by the Safeguarding team. As part of their induction, new staff are provided with information and guidance regarding the online safety policy.

3.3 Online Safety Officer (role held by Digital Lead)

The Online Safety Officer is regularly updated on current online safety issues and legislation, and is aware of the potential for serious child protection concerns. They take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents.

An awareness and commitment to online safety is promoted across the school community by facilitating training and advice for all staff while ensuring online safety education is embedded within the curriculum. The Online Safety Officer monitors the impact of online safety training and assesses future training needs.

The Online Safety Officer communicates regularly with the DSL, School leaderships and IT support to discuss current issues, review incident logs, adjust filtering and amend operational procedures. They ensure that online safety incidents are logged as a safeguarding incident and that all staff are aware of the procedures that must be followed in the event of an incident as outlined in our Safeguarding and Child Protection policy.

3.4 Director of IT

The Director of IT is responsible for ensuring that the school's technical infrastructure is as secure as possible; that only registered users may access the school's networks and devices; that appropriate filtering is applied and updated on a regular basis and that use of the school's ICT facilities is regularly monitored to ensure compliance with ICT Acceptable Use Policy and Staff Code of Conduct.

The Director of IT attends the cross-school Safeguarding Committee at least annually to update and review the monitoring and filtering provision with all DSLs.

3.4 Parents, carers and extended family

To support families in helping their children use technology safely our schools will seek to provide information and awareness to parents and carers through;

- Reference to relevant resources and websites on Thomas's Online Platforms.
- Recommended guidance on technology use in letters and school news
- Parents evenings
- External speakers
- High profile national events e.g. Safer Internet Day

4. PROCEDURES

As a response to changing attitudes to technology in the classroom, all teachers share collective responsibility for promoting and enhancing digital literacy. All teachers use cloud based software to communicate and set digital tasks for pupils. They use Apple technology in the classroom to further embed digital literacy into the wider curriculum, reaching beyond the Computing classroom.

Our schools:

- have a clear, progressive online safety education programme as part of the Computing curriculum and PSHE curriculum. This aims to build resilience, critical thinking skills and behaviours appropriate to their age and experience;

- plan online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will regularly remind pupils about their responsibilities through the Pupil Acceptable Use Policy and reinforce messages as part of pastoral activities such as creating digital manifestos
- ensure staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology both in and out of school, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensure that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Pupils in Year 3 and above are provided with iPads on a 1:1 basis to support their learning and in some year groups the pupils are allowed to take the iPads home with them. The content on these iPads is strictly controlled by the school as is the time that pupils are able to use them, with access being switched off in the evening at different times depending on the age of the pupil. The pupils (and their parents) are also required to sign an online agreement with regards to their use of the 1:1 iPads both at school and at home.

Thomas's London Day Schools are committed to providing staff with regular training and development opportunities. Regular CPD content is provided that reflects current educational research and advances in technology. Staff have regular opportunities to discuss and reflect on current issues as part of structured safeguarding provision.

Requests for information or help with equipment and software should always be directed to IT Support via the helpdesk. Requests for teaching support and guidance with online safety issues should be directed to the Online Safety Officer.

4.1 Passwords

All staff are told to keep their passwords and pin numbers private. All pupils are told to keep passwords and pin numbers private, with the exception of their guardians and teachers. If a password is compromised the school should be notified immediately.

4.2 Digital Images

Expectations with regards to the use of personal devices to take any form of digital images (still or moving) by any pupil or adult can be found in the ICT Acceptable Use policies.

If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given. This includes uploading digital images to a website or using mobile devices to photograph or film any pupil, parent or member of staff without their consent.

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include staff, parents or younger children as part of their Computing and PSHE schemes of work. They are advised to be very careful about placing any personal photos on any online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information

When using social media, for the privacy and protection of all pupils and adults it is vital to be vigilant and follow the agreed procedures outlined in the ICT Acceptable Use Policy.

4.3 School Website

The Marketing team, supported by the Education and Operations Boards, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The school website complies with statutory DfE requirements. Where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

4.4 Cloud Based Software

Thomas's London Day Schools provides staff and pupils from Year 3 upwards with cloud based software for their professional and educational use both in school and at home. Pupils and staff are expected to follow the signed ICT (Acceptable Use) Policy both on and offsite.

Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community. On school devices, pupils are only allowed to upload and publish within school approved 'Cloud' systems.

4.5 Internet access, virus protection, filtering and monitoring

The School ensures compliance with the DfE's Filtering and monitoring standards for schools by:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring
- Reviewing the filtering and monitoring provision at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet our safeguarding needs.

The school network has educational filtered secure broadband connectivity and ensures network health through use of anti-malware software. A progressive filtering system blocks sites that fall into sensitive categories (e.g. adult content, race hate, gambling) and ensures age appropriate access to resources based on educational needs. The Director of IT keeps a log of all changes to filtering systems. Any amendments are made in consultation with the Online Safety Officer and Designated Safeguarding Leads.

Internet Usage Restrictions are listed in Appendix 2 of this Policy. Alerts are set up to flag any suspicious language used or inappropriate searches, on the internet as well as for Google documents and email. These alerts are received by Director of IT, school Online Safety Officer and school Designated Safeguarding Lead. The DSL and Online Safety Officer will work together to investigate any concerns.

The Thomas's network has been secured to appropriate standards suitable for educational use. The network has a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.

Record keeping - a record of all online safety incidents that have been investigated is maintained by the Online Safety Officer in conjunction with the DSL.

4.6 Network management (user access, backup)

All IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards. The IT team:

- uses individual, audited log-ins for all users;
- uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- is required to be up-to-date with services and policies;
- has daily back-up of school data (admin and curriculum);
- ensures storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU GDPR where storage is hosted within the EU;
- does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems.

Senior Leaders at each school work in partnership with the IT team and the Head to ensure any concerns about the system are communicated so that systems remain robust and protect pupils. There is a clear disaster recovery system in place that includes a secure, remote, off site back up of data.

4.7 Thomas's London Day Schools Equipment

Staff are responsible for ensuring that any equipment loaned to them by the school, is used primarily to support their professional responsibilities. The IT team maintain an asset register to equipment assigned to staff..

Pupils will only use devices with permission from the teacher. Personal mobile devices are only permitted in line with the school Behaviour Policy and are not permitted to be used in certain areas within the school site, e.g. changing rooms and loos.

All users are required to log off or lock the computer/device when they have finished working or are leaving the computer unattended.

All device use is open to monitoring scrutiny and the Head/ SLT are able to withdraw or restrict authorisation for use at any time, if it is deemed necessary. The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

5. ONLINE COMMUNICATION

References to online communications and social media include software, applications (including those running on mobile devices), email and websites, which enable users to interact, create and exchange information online. Examples include, but are not limited to, sites such as Facebook, Twitter, LinkedIn, YouTube, Wikipedia and Instagram, TikTok, momo and Sarahah. Also included is the use of SMS and instant messaging clients, such as, WhatsApp, Kik, iMessage and Snapchat. Internet/email use is monitored. Details of the types of communication technologies that are acceptable by different users in school are listed in Appendix 3.

A teacher should never share information with pupils or parents outside of school communication platforms.

Extreme care should be taken when transferring sensitive personal information online, in particular regarding SEND or safeguarding issues. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption. The IT Department will provide support where required.

5.1 Staff Communication

- Staff should refer and adhere to the Staff ICT Acceptable Use Policy.
- Staff are instructed to always keep professional and private communication separate.
- Use of any school approved social networking will adhere to the ICT Acceptable Use Policy.
- Staff are expected to regularly review their privacy settings on personal social media accounts to ensure that profiles and photographs are not viewable to the general public. The Online Safety Officer or any members of the IT Support team will help staff to check that their privacy settings are robust.

5.2 Pupil Communication

Pupils are taught about social networking, email, acceptable behaviour and protocols, and how to report misuse, intimidation or abuse through our online safety curriculum. All pupils have their own unique username and password which gives them access to the Internet and other services and are frequently reminded not to divulge these to anyone. Pupils are required to sign and follow the Pupil Acceptable Use Policies both in school and at home.

5.3 Parent Communication

The School will endeavour to assist parents with their awareness of developing technologies and give advice on how to support children towards safe, responsible and appropriate use of the internet and social media. This may be covered through school news, talks or a range of other activities.

It is recommended parents and children develop their own Online agreement to use at home that is respected and followed by all members of the family.

5.4 Remote Learning

On occasions, when groups or whole schools have worked from school, there is a requirement for pupils to access their learning remotely. Guidance is in place to enable pupils to access their online learning safely and protocols and expectations for staff, pupils and parents are set out in Appendix 5 of this Policy.

6. INCIDENT MANAGEMENT AND REPORTING

All members of the Thomas's community are encouraged to be vigilant and report issues, in the confidence that they will be dealt with quickly and sensitively, following guidance in the Behaviour and Safeguarding and Child Protection policies.

If any concerning content or images are found on an electronic device the device should be locked and the DSL contacted immediately. Members of staff should not view images, look for further images, copy or print any images or forward images by email or any other electronic means. **Appendix 4** sets out the Thomas's Online Safety Incident Flowchart.

The DSL should refer to the DfE and UK Council for Internet Safety guidance 'Sharing nudes and semi-nudes: Advice for education settings: Responding to incidents and safeguarding children and young people'.

Support may be sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues. The Police will be contacted if a member of staff or pupils receives online communication that is considered particularly disturbing or breaks the law.

7. REVIEW AND MONITORING

An annual audit of online behaviour and risks provides a record for monitoring and measuring the impact of our online safety education. This enables us to actively use pupil, staff and parent voice to inform school development and review the impact of online safety and prevent training.

8. LEGISLATION AND GUIDANCE

This Policy bears due regard to the following statutory guidance and other advice.

- HM Gov Data Protection Act (2018) and UK GDPR
- DfE statutory guidance 'Keeping Children Safe in Education (September 2023)
- Meeting Digital and technology standards in schools and colleges (March 2022)
- Filtering and Monitoring standards for schools and colleges (March 2023)
- HM Gov Investigatory Powers Act (2016
- DfE statutory guidance 'Revised Prevent duty guidance: for England and Wales' (updated April 2021)
- DfE guidance 'Teaching online safety in school' (June 2019)
- UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' (December 2020)
- UKCIS 'Safeguarding children and protecting professionals in early year settings: online safety considerations' (February 2019)
- UKCIS 'Education for a Connected World framework (June 2020)
- NSPCC: 'Younger children and social networking sites: a blind spot' (2013)
- HM Gov The School Information (England) (Amendment) Regulations (2012)
- HM Gov The Education and Inspections Act (2006 and 2011)
- UK Council for Child Internet Safety (UKCCIS)
  HM Gov Racial and Religious Hatred Act (2006)
- HM Gov Communications Act (2003)
- HM Gov Sexual Offences Act (2003)
- HM Gov The Education Act (2002, Sections 157 and 175)
- HM Gov Criminal Justice & Public Order Act (1994)
- HM Gov Malicious Communications Act (1988)
- HM Gov Public Order Act (1986)
- HM Gov Telecommunications Act (1984)
- HM Gov Computer Misuse Act (1990)
- HM Gov Obscene Publications Act (1959 and 1964)

9. APPENDICES

Appendix 1: Sanctions for misuse of ICT equipment and technology

Appendix 2: Guidance on internet restrictions

Appendix 3: Guidance on usage of communication devices

Appendix 4: Online Safety Incident Flowchart

Appendix 5: Expectations and Protocols for Remote Learning and Online meetings and teaching

APPENDIX 1: SANCTIONS FOR THE MISUSE OF ICT DEVICES AND TECHNOLOGY

Please note: All incidents must be recorded on the ICT incident log.

These sanctions apply to the misuse of both school equipment and all types of personal devices brought into school (mobile telephones/tablets/interactive or cellular watches etc)

A ● Unauthorised access to a website ● Unauthorised use of devices ● Disrespect of school and/or others’ ICT resources ● Unauthorised use of email ● Unauthorised use of social networking sites/instant messaging ● Bringing in of any personal electronic device to a classroom without a teacher’s permission
Sanction: Referred to Form tutor for school specific school sanctions.
B ● Continued use of devices during lessons after being warned. ● Continued use of non-educational sites during lessons after being warned ● Unauthorised use of staff logins ● Careless use of school and/or others’ ICT resources ● Unauthorised use of any personal electronic device to photograph, film or send messages ● Continued unauthorised use of email after being warned ● Continued unauthorised use of social networking sites/instant messaging after being warned ● Continued unauthorised use of any technology to photograph, film or send messages after being warned ● Unauthorised use of file sharing software or downloading files from the Internet ● Sending of any message that is not polite or sensible ● Accidentally corrupting or destroying others’ files without notifying a member of staff of it ● Accidentally accessing offensive material and not notifying a member of staff of it ● Editing or deleting computers Internet history files
Sanctions: Referred to Form Tutor and Online Safety Officer. Removal of Internet access rights and/or device for fixed period.
C ● Deliberate damage to school and/or others’ ICT resources ● Deliberately corrupting or destroying someone else’s files ● Using any ICT device, either in or out of school, to deliberately hurt, upset, bully or harass anyone in the school community ● Deliberately trying to access offensive material ● Deliberately attempting to bypass the school’s network security systems ● Using any device to purchase or order items over the Internet
Sanctions: Referred to Online Safety Officer and Head. Parents contacted. Probable removal of ICT access and or personal device for fixed period.
D ● Continued use of any ICT equipment or devices, either in or out of school, to deliberately hurt, upset, bully or harass anyone in the school community ● Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic terrorist related or violent ● Using ICT resources to bring the school into disrepute
Sanctions: Referred to Online Safety Officer and Head. Parents contacted. Probable exclusion for a fixed period.

APPENDIX 2: INTERNET USAGE RESTRICTIONS

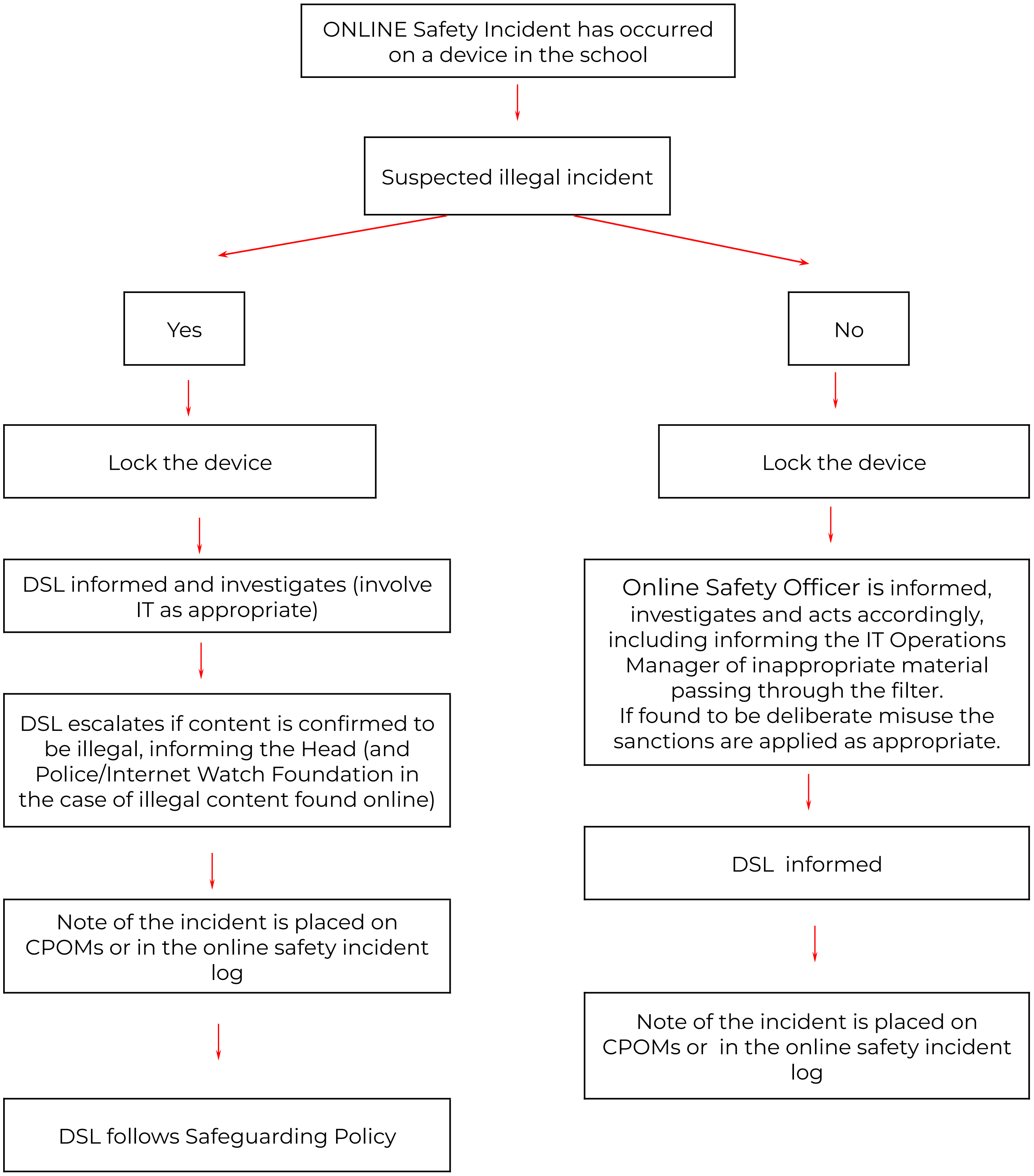
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain Internet usage as follows:

Actions of any person using TLDS network		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images				✔
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				✔
	adult material that potentially breaches the Obscene Publications Act in the UK				✔
	criminally racist material in UK				✔
	pornography			✔	
	promotion of any kind of discrimination			✔	
	promotion of racial or religious hatred			✔	
	threatening behaviour, including promotion of physical violence or mental harm			✔	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			✔	
Using school systems to run a private business				✔	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				✔	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✔	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✔	
Creating or propagating computer viruses or other harmful files				✔	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the Internet				✔	
Online gaming (educational)			✔		
Online gaming (non-educational)				✔	
Online gambling				✔	
Online shopping / commerce			✔		
File sharing			✔		
Use of social networking sites (Staff)			✔		
Use of social networking sites (Pupils)				✔	
Use of video broadcasting eg Youtube (Staff)			✔		
Use of video broadcasting eg Youtube (Pupils)				✔	

APPENDIX 3: COMMUNICATIONS

Communication Technologies that are accepted in school	**Staff and other adults**			**Pupils**		
	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✔				✔	
Use of personal mobile phones in lessons			✔			✔
Use of personal mobile phones in non-teaching time but never when a child is present		✔				✔
Taking photos on personal mobile phones		✔				✔
Taking photos on school devices	✔				✔	
Use of school mobile devices		✔			✔	
Use of personal email addresses in school, or on school network		✔				✔
Use of school email for personal emails			✔			✔
Use of personal chat rooms / facilities / instant messaging		✔				✔
Use of school chat rooms / facilities, instant messaging	✔					✔
Use of social networking sites for personal use		✔				✔
Use of blogs		✔			✔	
Use of forums	✔			✔		

APPENDIX 4: ONLINE SAFETY INCIDENT FLOWCHART



ONLINE Safety Incident has occurred on a device in the school

Suspected illegal incident

Yes

Lock the device

DSL informed and investigates (involve IT as appropriate)

DSL escalates if content is confirmed to be illegal, informing the Head (and Police/Internet Watch Foundation in the case of illegal content found online)

Note of the incident is placed on CPOMs or in the online safety incident log

DSL follows Safeguarding Policy

No

Lock the device

Online Safety Officer is informed, investigates and acts accordingly, including informing the IT Operations Manager of inappropriate material passing through the filter.
If found to be deliberate misuse the sanctions are applied as appropriate.

DSL informed

Note of the incident is placed on CPOMs or in the online safety incident log

The DSL should refer to the DfE and UK Council for Internet Safety guidance ‘Sharing nudes and semi-nudes: Advice for education settings: Responding to incidents and safeguarding children and young people’.

APPENDIX 5: EXPECTATIONS AND PROTOCOLS FOR ONLINE MEETINGS AND TEACHING

In the event of online learning, pupils will be taught via Google meet or Zoom with work available on Seesaw / Showbie / Google classroom.

If parents do not consent to their child accessing Face to Face learning sessions, they should inform their child's form teacher and the Online Safety Officer of their school in writing.

By agreeing to the online learning sessions, it is understood that the following protocols will be adopted.

Protocols for pupils (with parental support if necessary)

- It is very important that your workspace is in a neutral space. You must not be in a bedroom and the area should be quiet and without distractions.
- If you have headphones with a microphone these could be helpful
- Ensure you are dressed appropriately for the session.
- Your teacher will send you a link to an online session through your Seesaw, Showbie or Google Classroom platform.
- This link must be kept private and not shared. Do not put any meeting links on social media or outside the invited group
- Make sure you are ready for the session and click on the link at the appropriate time (with help if needed)
- Wait in the "waiting room" until your teacher invites you to join the session
- You must not record or photograph any aspect of the session
- All your interactions between your teachers and peers must respect the School's Code of Conduct

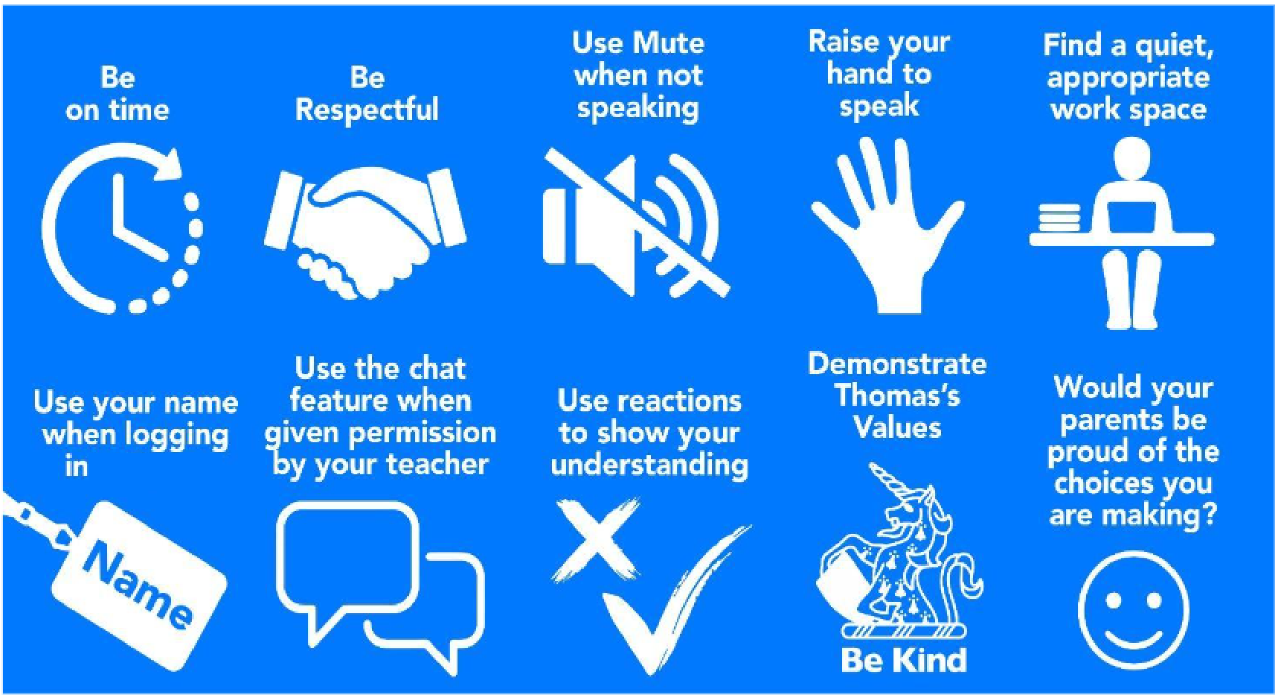
Protocols for parents

- Parents should be nearby and able to support their child as needed during the online learning session
- Parents should refrain from including themselves in the online learning session and must not share or comment on public forums about the sessions, teachers or departments.
- Devices should be linked to a WiFi network to avoid incurring unexpected mobile data costs
- If your child is unwell and unable to access the online learning sessions, please inform the school office as normal, to enable us to keep a record of attendance.

Protocols for teachers

- Online meetings should only be held during the school day
- Only use the school device that you have been given. Personal devices should not be used
- Set up your working environment that is neutral, quiet, safe and free from distractions
- Ensure you have a consistent and appropriate background. It should be one of the following:
    - the standardised background sent to all staff
    - a background that is relevant to your lesson

    - a background that is neutral and non-specific (if your computer doesn't support uploading the standardised image)
- Post the meeting link securely in Seesaw, Showbie or Google Classrooms. Do not display it publicly or send by email.
- Be mindful of pupils' access to devices when scheduling meetings
- Ensure you are always in professional dress or kit that is appropriate to the task (eg PE kit for games session)
- Use a new meeting room/link each time
- Do not add parents or pupils to your contacts list
- Ensure you are on time for the meeting to let pupils in from of the "waiting room"
- Ensure that there is always more than just one pupil in any online learning session (except for Individual Music lessons, Learning Specialist lessons and the occasional drop in sessions or when letting the first pupil in from the waiting room).
- Ensure that the attendees are set to "mute" on joining the session
- Consider the age of the pupils, both in terms of age requirements of the service you are using together with their ability to participate
- Be aware that larger groups may be more challenging during an interactive session so more passive or broadcast approaches may be more suitable
- Establish ground rules in the first session that focus on the protocols and parameters of online learning, using the guidance poster below, and after that, start every session with a brief reminder of the expectations, rules and regulations that keep pupils and teachers safe online and show courtesy to others, eg
    - Put your hand up if you wish to ask a question, just as in class
    - Do not record any part of the lesson
    - How to ask permission to leave a session if needed
- Tell pupils what Plan B is (ie if you do have to abort the meeting, where will the meeting move to and how can pupils rejoin)
- Turn screen sharing off
- Do not share a screen shot of everyone,
- Do not record any lessons
- Turn off your microphone unless it is needed
- Remember that the Thomas's ICT (Acceptable Use) Policy continues to apply
- Ensure you are the last person to leave the meeting or end the meeting so that pupils cannot continue unsupervised.
- Follow up any non-attendance in sessions promptly
- Report any safeguarding concerns to your DSL immediately



Be on time

Be Respectful

Use Mute when not speaking

Raise your hand to speak

Find a quiet, appropriate work space

Use your name when logging in

Use the chat feature when given permission by your teacher

Use reactions to show your understanding

Demonstrate Thomas's Values

Would your parents be proud of the choices you are making?