# ONLINE SAFETY POLICY

## INTRODUCTION

While new technologies are enhancing communication and creativity some are also challenging the definitions and boundaries of the school environment. As active participants in a digital world our broad curriculum and our pupils' personal goals requires 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. Our aim is to provide pupils and staff with the knowledge, skills and confidence to become safe and responsible users of technology.

## SCOPE

This Online Safety Policy relates to all members of the school 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.

## AIMS

The aims of this policy are to ensure that:

- staff and pupils are responsible users and stay safe while using 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 | Bullying, harassing or stalking others | Creating and uploading inappropriate or illegal content (including "sexting") | Providing misleading information and advice Encouraging |

| | | | | |
|---|---|---|---|---|
| | Privacy<br>Copyright | | Unhealthy/inappropriate sexual relationships<br>Child on child sexualised or harmful behaviour | others to take risks online<br>Sharing extremist views Problematic Internet Use or "Addiction"<br>Plagiarism |

**ROLES AND RESPONSIBILITIES**

**All Users**
All users are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Policy. All staff and pupils will sign an 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.

**Safeguarding Team**
The Safeguarding team responsibilities are outlined in the Safeguarding and Child Protection policy. They will ensure that all staff receive suitable training and development to carry out their responsibilities in a safe and supportive environment. An online safety log will be kept and reviewed regularly by the Safeguarding team. As part of their induction, new staff will be provided with information and guidance regarding the online safety policy.

**Digital Lead**
The Digital Lead 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 Digital Lead monitors the impact of online safety training and assesses future training needs.

The Digital Lead communicates regularly with the Executive and Associate Heads, SLT, DSLs and IT support to discuss current issues. They ensure that online safety incidents are logged as a safeguarding incident and that all staff are aware of the procedures that need to be followed in the event of an incident as outlined in our Safeguarding and Child Protection policy.

**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 the school website
- Recommended guidance on technology use in letters and bulletins
- Parents evenings
- High profile national events e.g. Safer Internet Day

**EXPECTATIONS**

All users are responsible for using the school IT and communication systems in accordance with the relevant Safeguarding, Behaviour and Acceptable Use Policies.

All staff will supervise 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. Any misuse will be reported to the Digital Lead/Safeguarding Team in line with the reporting procedures outlined in the Safeguarding policy.

All staff are encouraged to take professional, reasonable precautions when working with pupils, previewing websites and resources before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

**School 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 keep a list of all members of staff who have use of a work device and will share this with the Designated Safeguarding Lead.

School devices will only be used by pupils during lessons and with permission from the teacher. Mobile devices are not permitted to be used in certain areas within the school site, e.g. toilets. All users are required to log off or lock the computer/device when they have finished working or are leaving the computer/device unattended.

The school maintains equipment to ensure Health and Safety is followed. 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.

**Personal Mobile Devices**
All users must follow the expectations outlined in our Acceptable Use Policy and Parental Guidance. Whether in school or at an off-site event, mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

**EDUCATIONAL STRATEGIES**
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 iPads in the classroom to further embed digital literacy into the wider curriculum, reaching beyond the Computing classroom.

Our school:
- Embeds online safety education throughout both Computing and Character Curriculum lessons. 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.

Thomas's Academy is committed to providing our staff with regular training and development opportunities. We provide regular CPD content that reflects current educational research and advances in technology. We ensure that staff have regular opportunities to discuss and reflect on current issues as part of structured safeguarding provision.

**SECURITY**

**Passwords**
We ensure that all staff and pupils always keep their passwords and pin numbers private. If a password is compromised the school should be notified immediately.

**Digital Images**
Parents are required to sign an online consent form giving permission for pupils' digital images to be used in a range of formats. Until they have done this it must be assumed that no permission has been given.

The school office keeps a list of the pupils for whom photograph permission is not given and this is shared with any school photographers.

Members of staff can also opt out of having their image on Social Media and should inform the SLT in writing.

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

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 Personal Devices and Photography Policy.

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 school leaders, parents or younger children as part of their Computing and PSHCE 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

**School Website**
The Executive Head 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.

**Internet access, virus protection and filtering**
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 TLDS Director of IT keeps a log of all changes to filtering systems. Any amendments are made in consultation with the Digital Lead.

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.

**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 TLDS Support team:

- use individual, audited log-ins for all users
- use guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- use 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 data protection directive 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 the Academy work in partnership with the IT Support team 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 backup of data.

Staff requests for information or help should always be directed to IT support via the helpdesk. Staff requests for the provision of new software or hardware should be made to your Digital lead.

**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. Also included is the use of SMS and instant messaging clients, such as, WhatsApp, iMessage and Snapchat. Internet/email use is monitored.

Electronic messages are not anonymous and can be tracked and live forever on the Internet. Social Media sites archive content posted, even when deleted from online profiles. Once information is placed online, the author relinquishes control of it. A teacher should never share information with pupils or parents in ANY environment that they would not willingly or appropriately share in a school or school-related setting or in the community.

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. Staff use encrypted devices or secure remote access where staff need to access sensitive data off-site.

**All Staff**
Staff are instructed to always keep professional and private communication separate. Use of email and internet for personal purposes is permitted but any such use must be limited and must not disrupt staff duties.

Staff members who wish to communicate with pupils online may do so only with the approval of the school, using official Thomas's Academy sites and accounts created specifically for this purpose. These sites are managed and controlled by TLDS administrators. There should be no connection made between any personal accounts and school accounts used for educational purposes. Use of any school approved social networking will adhere to the Acceptable Use Policy.

Teachers are advised that they should use a separate email address just for social networking so that any other contact details are not given away. They should also be aware that they can be vulnerable to unintended misuses for electronic communication. Email, texting and social media

encourage casual dialogue and often innocent actions can easily be misconstrued or manipulated. Social networking sites blur the line between work and personal lives and discretion should be used at all times with both parents and colleagues.

Staff are expected to regularly review their privacy settings to ensure that profiles and photographs are not viewable to the general public. The Digital Leads or any members or the IT Support team will help staff to check that their privacy settings are robust.

**Pupils**
Pupils are taught about social networking, email, acceptable behaviour and protocols, and how to report misuse, intimidation or abuse through our online safety curriculum. Pupils from Year 3 to Year 6 all have their own unique username and password which gives them access to the desktop PCs, the internet and other services and are frequently reminded not to divulge these to anyone. Pupils are required to sign and follow our age appropriate Pupil Acceptable Use Policies both in school and at home.

**Parents**
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 bulletin articles, 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.

## INCIDENT MANAGEMENT AND REPORTING

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

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

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 Digital Lead.

## 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.

**Thomas's Academy reserves the right to monitor staff communications in order to:**
- establish the existence of facts;
- ascertain compliance with regulatory or self-regulatory procedures;
- monitor standards, which are achieved by persons using the system in the course of their duties and for staff training purposes;
- prevent or detect crime;
- investigate or detect unauthorised use of the school's telecommunications systems;
- ensure the effective operation of the system such as protection against malware, backing up and making routine interceptions, such as forwarding emails to correct destinations;
- gain access to routine business communications, for instance checking voicemail and email when staff are on holiday or sick leave.

## REFERENCES

This policy has been informed by:
HM Gov Data Protection Act (1998 and 2018)
DfE statutory guidance 'Keeping Children Safe in Education (September 2019)
HM Gov Investigatory Powers Act (2016
DfE advice 'The Prevent Duty' (June 2015) from The Counter-Terrorism and Security Act (2015)
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) ( est 2010)
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)

**See also:** Anti-bullying Policy, Behaviour Policy, ICT Acceptable Use Policy and Agreements, Personal Devices and Photography Policy, Safeguarding and Child Protection Policy

| **This policy will be reviewed annually** | | | |
|---|---|---|---|
| Latest TLDS Review: January 2020 | By: | Joanna Copland, Vice Principal, Michael Swart, Director of IT Operations, Digital Leads | Changes made |
| Latest Academy Version: March 2021 | By: | Miles Chester, Executive Head, Suzanne Kelly, Associate Head and Stephanie Chambers, Digital Lead | |
| Edited | By: | Stephanie Chambers, Digital Lead and Suzanne Kelly Associate Head Teacher | |

Appendix 1: Guidance on internet restrictions
Appendix 2: Guidance on usage of communication devices
Appendix 3: Online Safety Incident Flowchart

## ONLINE SAFETY POLICY APPENDIX 1

### 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:

| User Actions | | 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 | | | ✔ | | |
| Use of video broadcasting eg Youtube | | | ✔ | | |

## ONLINE SAFETY POLICY APPENDIX 2

### 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 mobile phones in lessons | | | ✔ | | | | ✔ |
| Use of mobile phones in social time | | ✔ | | | | | ✔ |
| Taking photos on mobile phones | | ✔ | | | | | ✔ |
| Taking photos on camera devices | ✔ | | | | | ✔ | |
| Use of hand held devices eg PDAs, PSPs | | ✔ | | | | ✔ | |
| Use of personal email addresses in school, or on school network | | ✔ | | | | ✔ | |
| Use of school email for personal emails | | | ✔ | | | ✔ | |
| Use of chat rooms / facilities | | ✔ | | | | | ✔ |
| Use of instant messaging | | ✔ | | | | | ✔ |
| Use of social networking sites | | ✔ | | | | ✔ | |
| Use of blogs | | ✔ | | | | ✔ | |
| Use of forums | ✔ | | | | ✔ | | |

## ONLINE SAFETY POLICY APPENDIX 3

### ONLINE SAFETY INCIDENT FLOWCHART