Thomas Telford School

E-Safety Policy

Prepared by Phil Nicholls

September 2020

Review date: September 2021

Reviewed and updated September in line with 'Keeping Children Safe in Education' statutory guidance – annex C: Online safety

Introduction

Thomas Telford School recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning.

However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the School while supporting staff and learners to identify and manage risks independently and with confidence.

We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners and the Every Child Matters agenda, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This E-Safety policy should be read alongside other relevant School policies/guidance:

- Safeguarding/Child Protection Policy (Updated Sept 2020)
- IT Acceptable Use Policy (Updated July 2020)
- Anti-Bullying Policy (Updated July 2020)
- Grievance Policy (Updated July 2020)
- Complaints Procedure (Updated July 2020)
- Mobile Telephone Policy (students) (Updated July 2020)
- Staff Use of Communications Systems (Updated July 2020)
- Parents' Guide to the Internet (Updated July 2020)
- Behaviour Policy (Updated July 2020)
- Equal Opportunities (Updated July 2020)

Monitoring and Review

The impact of the policy will be monitored regularly with a full review being carried out yearly or earlier, dependent on particular national issues or internal issues that may be raised which impact on our use of e safety.

This E-Safety policy was approved by the Governors and Parents Advisory Council:	September 2020 (TBA)
The implementation of this E-Safety policy will be monitored by:	David Smith – IT Director Phil Nicholls – Safeguarding Officer Bethan Cash- Deputy safeguarding officer Ian Rawlings – E-Safety Officer (CEOP Trained Staff) Sir Kevin Satchwell - Headmaster
The Governing Body will receive updates of the implementation of E-Safety at regular intervals:	Annually
The E-Safety policy will be reviewed annually, or more frequently in the light of any significant developments in the use of technologies, new threats to E-Safety or incidents that have taken place.	September 2021
Should serious E-Safety incidents take place, the following persons should be informed:	David Smith – IT Director **Ian Rawlings – E-Safety Officer (staff)** (CEOP Trained)

	Phil Nicholls- E-Safety Officer (students) Sir Kevin Satchwell - Headmaster
Should serious E-Safety incidents take place, the following external persona/agencies should be informed.	LA safeguarding Officer, Police.

The School will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring of network activity
- Surveys/questionnaires

Scope of the Policy

The policy applies to all users/all students and staff/all members of the School community who have access to the School IT systems, both on the premises and remotely.

Any user of School IT systems must adhere to the **E-Safety Rules and the Acceptable Use Agreement**.

The E-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones and social media sites.

The Education and Inspectors Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the School site, and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying or other E-Safety incidents covered by this policy, which may take place outside Thomas Telford School, but is linked to membership of Thomas Telford School.

The 2011 Education Act increased these powers with regard to the searching of electronic devices and the deletion of data.

In the case of both acts, action can only be taken over issues in line with the Behaviour Policy.

Thomas Telford School will deal with such incidents within this policy, associated behaviour and anti-bullying policies. We will, where known, inform parents/carers of the incidents of inappropriate E-Safety behaviour which takes place at Thomas Telford School.

Roles and Responsibility

Concern:	**Report to:**
Safeguarding	Phil Nicholls Bethan Cash Sir Kevin Satchwell
IT or equipment	David Smith
E-Safety	Ian Rawlings Phil Nicholls

There are clear lines of responsibility for E-Safety within the School. The first points of contact for Staff should be David Smith (DS) Director of IT, Ian Rawlings and Phil Nicholls.

All staff are responsible for ensuring the safety of students and should report any concerns immediately to the Senior Member of staff shown above.

All learners must know what to do if they have E-Safety concerns and who to talk to. In most cases, this will be Head of Key Stage or Personal Tutor. Heads of Key Stage will liaise with David Smith or as appropriate. All incidents will be recorded in a log and reported accordingly to the Headmaster.

E-Safety Officers:

The E- Safety Officers are responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will be expected to complete, review and update the E-Safety Policy and deliver staff development and training.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• **Content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• **Contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Students

Learners are responsible for using the School IT systems and mobile devices in accordance with the School's Acceptable Use Policy, Mobile Phone Policy, Student Charter and E-Safety Rules.

Students must act safely and responsibly at all times when using the internet and/or mobile technologies. If a student is worried or concerned, or where they believe an E-Safety incident has taken place involving them or another member of the School community, this must be reported to the Head of Key Stage, Personal Tutor or any suitable member of staff.

Staff

All staff are responsible for using the School's IT systems and mobile devices in accordance with the Staff Use of Communications Systems.

Staff are responsible for attending staff training on E-Safety and displaying a model example to learners at all times through embedded good practice.

Any incident that is reported to or discovered by a staff member must be reported to the E-Safety Officer and/or line manager without delay. (See table on previous page).

Security

Thomas Telford School Governing Body will do all that they reasonably can to protect students exposure while using appropriate filters to enable a programme which will not lead to unreasonable restrictions.

This will be monitored through the filters and monitoring system in place.

Thomas Telford School will do all that it can to make sure the network is safe and secure. Every effort is made to keep security software up to date. Appropriate security measures include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc.

Computer services monitor all internet activity by staff and students.

Multiple levels of safeguarding and E-Safety.

'Sophos Management Appliance' which keeps lists of sites and categories of sites which are not to be permitted and blocks staff/students from accessing these sites. We are able to add / remove sites to these lists if new threats emerge. The appliance also logs attempts to access suspect sites which we can use to generate reports.

The School also uses a product called Impero which allows staff to actively monitor students' use of the PCs. It also keeps a log of everything the student does on any PC. In addition, Impero flags suspicious/worrying activity. The system also automatically takes a screenshot of the activity. Staff use Impero around the School to monitor their areas. This tool allows them greater control over PC use and highlights areas of concern/misuse very early.

Email is also monitored by our email appliance. As well as junk filtering the appliance monitors student email and automatically flags concerning phrases/words to Computer Services.

Risk Assessment

Risk assessment procedures are in place whenever new technologies are being considered by the IT team. All software is installed through Computer Services. This includes the use of DVDs.

Behaviour

Thomas Telford School will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy and related policies.

Thomas Telford will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes.

Where conduct is found to be unacceptable, the School will deal with the matter internally. Where conduct is considered illegal, the School will report the matter to the Police.

Communications

Thomas Telford requires all users of IT to adhere to the strict rule which states clearly all student mobile phones must be switched off during the school day.

Use of image and video

No image/photographs of students or student based activities should be copied, downloaded, shared or distributed online. Photographs of activities on the School premises should be considered carefully and have the consent of Dave Smith prior to any usage. Approved photographs should not include names of individuals without consent.

Sexting

If a child is under the age of 18, it is illegal for them to make, possess or distribute any inappropriate explicit imagery of someone under the age of 18 which is 'indecent'.

Young people who share sexual imagery of themselves, or peers are breaking the law. Incidents involving a child producing a sexual imagery will be treated as a safeguarding issue.

Even though the age of sexual consent is 16, the Protection of Children Act 1999, amended Sexual Offences Act 2003 (England and Wales) means it is against the law for a child to share a sexual image, even if it is with someone who is also under the age of 18.

For the most purposes, if imagery contains a naked young person, topless photos of girls, any sex acts or display of genitals it will be considered indecent. Indecent images may also include overtly sexualised imagery of young people in underwear.

Where the Police are notified of a child under the age of 18 who is in possession of an indecent image or has been sending or taking these type of photos, they are obliged, under the Home Office Counting Rules and National Crime Recording Standards, to record the incident on their crimes system.

If it is disclosed that a Thomas Telford student has received an inappropriate sexually explicit image or video, sent an image or video or shared an image or video the school will take this matter very seriously and appropriate action will be taken, in line with the school procedures, which could result in expulsion from the School.

Upskirting

Thomas Telford School understands that 'upskirting' typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm. We accept that this is now a criminal offence (Voyeurism offences Act- April 2019) and any such incidents will be dealt with accordingly.

Personal Information

Any processing of personal information needs to be in compliance with the GDPR legislation and Data Protection Act 1998. Any device on which images are stored must be immediately given to Computer Services for approval and storage. Images must not be shared by staff or students.

Thomas Telford School collects and stores the personal information of students and staff. The School will keep that information safe and secure and will not pass it on to anyone else without the express permission of the learner/parent/ carer.

Only names and work email addresses of (senior) staff will appear on the School website. No staff/students' personal information will be available on the website.

Staff must keep students' personal information safe and secure at all times. When using an online platform, all personal information is password protected. No personal information of individuals is permitted offsite. Every user of IT facilities is required to log off on completion of any activity, or when they are physically absent from a device for any period this continues at regular intervals throughout the student's lifetime at the School.

All School mobile devices such as a laptop, USB (containing personal data) require to be encrypted, password protected and signed out by a member of the IT staff before leaving the premises. Smart watches are not allowed in school.

Education and Training

With the current unlimited nature of internet access, it is impossible for Thomas Telford School to eliminate all risks for staff and learners. It is our view, therefore, that the School should support staff and learners to stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

Resources to support students and staff (KCSIE 2020) include:

• **Be Internet Legends** developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils

• **Disrespectnobody** is Home Office advice and includes resources on healthy relationships, including sexting and pornography

• **Education for a connected world framework** from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety

• PSHE association provides guidance to schools on developing their PSHE curriculum

• Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements

• **Thinkuknow** is the National Crime Agency/CEOPs education programme with age specific resources

• UK Safer Internet Centre developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum

For Students and Parents/Carers

Year 7 Students and parents/carers attend an induction E-Safety session which takes place at the beginning of a new School year/during the induction period.

At the Year 7 E-Safety information evening, parents are provided with a range of useful documents and a check-list for:

- E-Safety parents/carers guide to internet – Link to Child net/Cyber bullying

Check list for parents:

- What are the risks
- Data Removal
- Internet Safety
- Information on bullying
- Mobile phone use

Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

A programme of E-Safety assemblies and information sessions are run throughout the year to ensure all students are continual aware of potential threats and how to use the internet safely.

For Staff:

Staff will take part in E-Safety update training during the first term of the school year. This will be delivered by a Safeguarding Lead. Further resources of useful guidance and information will be issued to all staff following the session. Each member of staff must record the date of the training attended on their CPD calendar.

Incidents and Response

Where an E-Safety incident is reported to the School, the matter will be dealt with very seriously. The School will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring to students or employers.

If a student wishes to report an incident, they can do so to their Head of Key Stage, Personal Tutor or other appropriate staff member. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible or Dave Smith or Phil Nicholls.

Following any incident, the School will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Feedback and Further Information

Thomas Telford School welcomes all constructive feedback on this and any other School policy. If you would like further information then please contact our E-Safety Officers, Mr Phil Nicholls or Mr Ian Rawlings.

Safeguarding

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation; technology often provides the platform that facilitates harm.

Thomas Telford Schools approach is to protect and educate the whole school community in the use of technology and we will work to identify and intervene where appropriate.

The breadth of issues classified within online safety is considerable:

- **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Our information technology (IT) department monitor software in school, this will be reviewed, updated and checked regularly. On occasions, unacceptable websites might be accessed inadvertently; if this occurs IT services will actively look to close down access immediately. It will be logged and reported to the Headteacher, Designated Safeguarding Lead and to the Director of IT services.

Thomas Telford School will teach children about online safety. We will use the Teaching online safety in school (government publication) guidance to ensure our pupils understand how to stay safe and behave online as part of our curriculum.

Thomas Telford School recognises that many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular. We will manage this by:

- teaching children about online safety
- not allowing children to use personal electronic devices during the school day
- not allowing children to take images of other children or staff
- only allowing children to access their personal electronic devices off the school premises or in the company of a senior member of staff, or post end of school day.

We recognise that all information technology, whether personal or work based, is a whole school issue and all staff have a duty to be vigilant.

Thomas Telford School recognises online safety is a major concern for all professionals'. For information and support staff will refer to the **'information and support' section of Annex C: Online safety KCSIE 2020.**

Thomas Telford School takes seriously its duties to assist parents and help them with online safeguarding resources. As such, we will make them aware of the webpage "Parent Info" which is a comprehensive, free resource for parents is covering a range of safeguarding topics and information about apps and when they are updated etc. The content can be found at http://parentinfo.org/

Thomas Telford School Acceptable Use Policy can be found in the shred area/staff handbook.

Safe use of electronic devices

Thomas Telford School will take all reasonable measures to ensure the safety and welfare of our children in our care. All staff's personal electronic devices are not permitted for use, in the presence of children.

Therefore we will ensure that we take measures including;

1. All personal electronic devices will be kept in a secure place and should not be accessed throughout contact time with the children, unless for an emergency.
2. Photographs or images of any children within our care may only be taken following parental consent and only using a school device and those images should remain within the setting
3. When on outings, electronic devices may only be used to make or receive phone calls relating directly to ensuring the safety and well-being of the children.

Thomas Telford School will follow the good practice guidance from the Information Commissioners Office, on taking photographs in educational institutions. In the interests of safeguarding a common sense approach on a case by case basis will be taken in this area.

This policy should be read in conjunction with Thomas Telford School Child Protection and Safeguarding Policy September 2020, Acceptable Use Policy and Mobile Phone Policy 2020

Information and support

Organisation/Resources	What it provides
thinkuknow	NCA CEOP's advice online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges.
Internet matters	Help for parents on how to keep their children safe online.
parentzone	Help for parents on how to keep their children safe online.
Childnet cyberbullying	Guidance for schools on cyberbullying.
pshe	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images.
educateagainsthate	Practical advice for parents, teachers and Governors on protecting children from extremism and radicalisation.
The use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety • Education for a connecting world framework.
NSPCC	NSPCC advice for schools and colleges.
Net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings and other information about all types of media for children and their parents.
Searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones.