E-Safety Policy

This document has been approved for operation within:	Kathryn Towers
Date effective from	April 2024
Date of next review	July 2025
Review period	1 Year
Status	Statutory
Owner	Tower Learning School Independent School (TLCIS)
Version	1.2

E-Safety Policy

Contents:

Roles and Responsibilities:

Appropriate and Inappropriate Use by Staff, Children or Adults:

Monitoring of the E-Safety Policy will take place at regular intervals.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be July 2025

Scope of the Policy

This policy applies to all members of TLCIS (including staff, pupils, parents/carers and visitors,) who have access to and are users of TLCIS ICT systems.

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

TLCIS will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that takes place within the School.

Roles and Responsibilities

E-Safety Policy

The following section outlines the e-safety roles and responsibilities of individuals within TLCIS

Proprietor:

Proprietor is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Proprietor by receiving regular information about e-safety incidents and monitoring reports.

The role of the Proprietor will include:

• regular meetings with the Senior Staff

• regular monitoring of e-safety incident logs

• regular monitoring of filtering/change control logs

Proprietor and Senior Staff:

• The Proprietor has a duty of care for ensuring the safety (including e-safety) of Tower Learning School, though the day to day responsibility for e-safety will be delegated to the Natalie Partington – Designated Safeguarding Officer

• The Proprietor and (at least) another member of the Senior Staff should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

• The Proprietor / Senior Staff Team are responsible for ensuring that the Designated Safeguarding Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

• The Proprietor / Senior Staff Team will ensure that there is a system in place to allow for monitoring and support of those in the school who carry out the internal e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

• The Senior Staff Team will receive regular monitoring reports from the Designated Safeguarding Officer.

Designated Safeguarding Officer:

• leads on e-safety issues

• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the e-safety policies/documents

• ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

• provides training and advice for staff

• liaises with the Local Authority/relevant body

• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

• meets regularly with Proprietor to discuss current issues, review incident logs and filtering/change control logs

• reports regularly to Senior Staff Team

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

• they have an up to date awareness of e-safety matters and of the current e-safety policy and practices.

• they have read, understood and signed the IT Acceptable Usage Policy.

• they report any suspected misuse or problem to the Proprietor / Safeguarding Officer for investigation/action/sanction.

• all digital communications with pupils/parents/carers should be on a professional level and only carried out using official TLCIS systems, as approved by the Proprietor

• e-safety issues are embedded in all aspects of the curriculum and other activities.

• pupils understand and follow the e-safety and acceptable use agreements.

• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

• in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Officer:

The Designated Safeguarding Officer should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

• sharing of personal data

• access to illegal/inappropriate materials

• inappropriate on-line contact with adults/strangers

• potential or actual incidents of grooming

• cyber-bullying

Pupils:

• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.

• should understand the importance of adopting good e-safety practice when using digital technologies

Parents/Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Parents and carers will be encouraged to support the School in promoting good e-safety practice.

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Pupils should be taught in lessons (where applicable) to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Internet Use Agreements.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings
- The Safeguarding Officer will provide advice/guidance/training to individuals as required.

Technical – infrastructure/equipment, filtering and monitoring:

The School will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- the technical systems will be managed in ways that ensure that meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of the technical systems
- filtering system is managed locally and through a DNS server (Webroot)
- Internet activity is monitored locally by tutors and by a DNS server (Webroot)
- Wifi filtering is managed locally by a DNS server (Webroot)

Users may use the following types of removable media for the purposes detailed:

- CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
- USB Media (memory sticks) – this type of media can be used on devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
- Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the schools' Data Protection Policy.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any lesson in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, chat, etc) must be professional in tone and content.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school / website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity:

TLCIS has a duty of care to provide a safe learning environment for pupils and staff. TLCIS could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school.
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly.

Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the school's systems so that they can obtain age-appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in. All staff should receive a copy of the E-Safety Policy and a copy of the Internet Use Agreement, which they need to sign, return to the school, to keep under file with a signed copy returned to the member of staff.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Proprietor immediately and then the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Children or Young People:

Children and young people are expected to use the internet and other technologies within School, including downloading or printing of any materials. The children and young people must understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at the school, the following consequences should occur:

- Any child found to be misusing the internet may have a phone called made to their appropriate adult / carer or parent.
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.
- A letter / phone call to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person accidentally accesses inappropriate materials the child should report this to a teacher immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Responding to incidents of misuse:

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity the school will report immediately to the police.

Other Incidents

It is hoped that all staff in the school will be responsible users of digital technologies, who understand and follow School policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

• Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

• Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

• It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

• Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

• Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- Internal response or discipline procedures.
- Involvement by Local Authority or national/local organisation (as relevant).
- Police involvement and/or action.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:

- incidents of 'grooming' behaviour.
- the sending of obscene materials to a child.
- adult material which potentially breaches the Obscene Publications Act.
- criminally racist material.
- other criminal conduct, activity or materials.
- isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the Policy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.