THOMAS ESTLEY COMMUNITY COLLEGE

E Safety Policy

Approved/reviewed by	
Date of next review	March 2025

This plan is reviewed annually to ensure compliance with current regulations.

Version	Reviewed by	Summary of changes	Date
v3	Cathy Cornelius	Updated to include current legislation and good practice	29/03/2022
V4	Cathy Cornelius	Section 3 – Monitoring and Filtering section included to reflect new KCSIE 2023	23/10/23

Thomas Estley Community College

E-safety Policy

This policy should be read alongside Thomas Estley additional policies and procedures on child protection, safeguarding and antibullying.

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices;
- provide staff and volunteers with the overarching principles that guide our approach to online safety;
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

1. Introduction

Thomas Estley Community College (TECC) recognises the Internet and other digital technologies provide a good opportunity for children and young people to learn. These new technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement, we at TECC want to ensure that new technologies are used to:

- Raise standards
- Develop the curriculum and make learning exciting and purposeful
- Enable students to learn in a way that ensures their safety and security
- Enhance and enrich their lives and understanding

We are committed to an equitable learning experience for all students using ICT technology and we recognise that ICT can give disabled students increased access to the curriculum to enhance their learning.

We are committed to ensuring that **all** students will be able to use new technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are informed about the risks that exist so that they can take an active part in safeguarding children.

The nominated senior person for the implementation of the School's e-safety policy is the designated safeguarding lead (Cathy Cornelius –Vice Principal) supported by the Network Manager.

2. Scope of Policy

The Policy applies to:

- all students;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the school's facilities where they are used by voluntary, statutory or community organisations;

TECC will ensure that the following elements are in place as part of its safeguarding responsibilities to students:

- a list of authorised persons (IT Department and DSLs) who have various responsibilities for e-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using new technologies;
- audit and training for all relevant staff;
- close supervision of students when using new technologies;
- education that is aimed at ensuring safe and responsible use of new technologies;
- a monitoring and reporting procedure for abuse and misuse. Infrastructure and Technology

- Partnership working:

    - TECC recognises that as part of its safeguarding responsibilities there is a need to work in partnership. As part of our commitment to partnership working, we fully support and will continue to work with School's Broadband to ensure that student and staff usage of the Internet and digital technologies is safe. Our internet filtering is managed off site through RmSafetyNet and the Network Manager.

3. Monitoring and filtering

All our staff have 'an understanding of the expectations, applicable to their roles and responsibilities in relation to filtering and monitoring' of ICT systems and regular monitoring of school's equipment and networks.

Our school approach to online safety, including appropriate filtering and monitoring on school devices and school networks is reflected in this Child Protection Policy including awareness of the ease of access to mobile phone networks. (See KCSiE 2023 Paragraph 138).

Our Senior DSL and the DSL team has the lead responsibility in this area, which is overseen and regularly reviewed by the 'Governing body, along with considering the number of and age range of their children, those who are potentially at greater risk of harm, and how often they access the IT system along with the proportionality of costs versus safeguarding risks.'

Our Governing body will ensure they maintain oversight of the Online Safety Policy contained within our main child protection policy, and the arrangements put in place to ensure appropriate filtering and monitoring on school devices and school network.

The appropriateness of any filtering and monitoring systems will in part be informed by the risk assessment required by the Prevent Duty as required by KCSiE 2023 paragraph138 to147.

This will include: - identify and assign roles and responsibilities to manage filtering and monitoring systems. - review filtering and monitoring provision at least annually. - block harmful and inappropriate content without unreasonably impacting teaching and learning. - have effective monitoring strategies in place that meet the school's safeguarding need. - review and discuss the standards with the leadership team, IT staff and service providers to ensure the school/college meets the standard published by the Department for Education filtering and monitoring standards.

Our Governing body will ensure a review is maintained to ensure the standards and discuss with IT staff and service providers these standards and whether more needs to be done to support our school in meeting and maintaining this standard and communicating these to staff, our students, parents, carers and visitors to the school who provide teaching to children as part of the learning and educational opportunities we provide.

- An additional layer of filtering is managed on site by the IT Department using Netsupport DNA.

- There are additional esafety and safeguarding programs built into Netsupport DNA such as trigger words. Certain words will trigger an alert to the current safety officer, Mrs. Cathy Cornelius via email and the software will also alert the Network Manager at the same time. Internet browsing is also monitored and NetsupportDNA will also take screen shots of Medium to High Trigger words as well as keep a log of any website visited whilst logged onto our network.

- As part of our wider safeguarding responsibilities, we seek to ensure that voluntary, statutory and community partners also regard the welfare of children as paramount. We therefore expect any organisation using the school's ICT or digital technologies to have appropriate safeguarding policies and procedures.

4. Policies and Procedures:

- Use of new technologies:

  - We seek to ensure that new technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.
  - TECC expects all staff and students to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:[1] These expectations are also applicable to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Users are not allowed to:

- Visit Internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:

    - Indecent images of children
    - Promoting discrimination of any kind
    - Promoting racial or religious hatred
    - Promoting illegal acts
    - Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e. cyber bullying) including abusive text or images; promotion of violence; gambling; criminally racist or religious hatred material

- The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and permission given by Senior Leaders or the Network Manager, so that the action can be justified, if queries are raised later.

- Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

    - Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
    - Adult material that potentially breaches the Obscene Publications Act in the UK
    - Criminally racist or anti-religious material
    - Violence and bomb making
    - Illegal taking or promotion of drugs
    - Software piracy
    - Other criminal activity

In addition, users are not allowed to:

- Use the school's broadband provider's facilities for running a private business;

- Visit sites that might be defamatory or incur liability on the part of the school or adversely impact on the image of the school;

- Reveal or publicise confidential or proprietary information, which includes, but is not limited to financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;

- Use the Internet for soliciting, revealing confidential information or in any other way that could reasonably be considered inappropriate;
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded

within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe;

- Assist with unauthorised access to facilities or services accessible via RM Broadband;
- Undertake activities with any of the following characteristics:
    - wasting staff effort or networked resources, including time on end systems accessible via the network and the effort of staff involved in support of those systems;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    - other misuse of the network, such as introduction of viruses;
    - Use any new technologies in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal

As a school, we will adhere to the guidance in the Computer Misuse Act 1990.

- Cyber Bullying
    - To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
    - Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes RSE education, and other subjects where appropriate.
    - All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
    - In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and safeguarding policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavors to ensure the incident is contained.
    - The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.
- Reporting Abuse
    - There will be occasions when either a student or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the student or adult should report the incident immediately.

- The School also recognises that there will be occasions where students will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances LSCB[2] Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will refer details of an incident to Children's Social Care or the Police.
- The School, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures[3] assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Examining Electronic Devices

- School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for, and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

- When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
  - Cause harm, and/or
  - Disrupt teaching, and/or
  - Break any of the school rules

- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
  - Delete that material, or
  - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
  - Report it to the police
  - Parents/Carers will be informed if a phone has been confiscated unless there is a safeguarding reason to withhold that information.

---

[2]Chapter 9 of the LSCB Procedures

[3]Chapters 5, 9, 12 and 13 of the LSCB Procedures

6. Education and Training

- TECC recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

- As part of achieving this, we aim to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our students to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use new technologies safely.

- To this end we will: -

  - Provide an age-related, comprehensive curriculum for e-safety which enables students to become safe and responsible users of new technologies. This will include teaching students to exercise the skills of critical awareness, digital literacy and good online citizenship, in line with the RSE curriculum.

  - Audit the training needs of all school staff and provide training to improve their

knowledge and expertise in the safe and appropriate use of new technologies.
    - Work closely to educate families on e-safety, to help them ensure that their children use new technologies safely and responsibly both at home and school. We will also provide them with relevant information on our e-safety procedures through our school website.

- Preventing the radicalisation of young people online.

    - Following the passing of the Counter-Terrorism and Security Act 2015, the active prevention and detection of radicalism has become a statutory obligation for education providers. The scope of e-safety and safeguarding has changed, with unprecedented online threats posed to children across the UK. So, it is crucial that children are able to develop vigilance online. Staff need to be given the confidence and awareness to provide a 'Counter narrative' to extremism, as well as being able to identify children who are potentially at risk or showing signs of radicalization.

    - Our staff are given on-going training and information regarding the ever-changing climate of keeping students safe online. One resource we have used is www.elearning.prevent.homeoffice.gov.uk which gives staff a comprehensive insight into extremism and radicalisation, what signs to look for and what to do if they have any concerns. Radicalisation and extremism are included in staff safeguarding training.

7. Standards and Procedures

TECC recognises the need to regularly review policies and procedures in order to ensure that its practices are effective and that the risks to students are minimised.

- Monitoring

    - Monitoring the safe use of new technologies includes both the personal use of the Internet and electronic mail and the monitoring of patterns and trends of use.

    - With regard to monitoring trends, within the school and individual use by school staff and students, TECC will audit the use of the Internet and electronic mail in order to ensure compliance with this document as needed. The monitoring practices of the school are influenced by a range of national guidance documents and will include the monitoring of content and resources.

    - We will also monitor the use of our school laptops, which are accessed by students and staff, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our students, and where necessary, support individual students where they have been deliberately or inadvertently been subject to harm.

- Sanctions

    - We will support students and staff as necessary in the event of a policy breach.

    - Where there is inappropriate or illegal use of new technologies, the following sanctions will be applied:

        - *Child / Young Person*

- The child/young person will be disciplined according to the behaviour policy of the school.
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

- *Adult (Staff and Volunteers)*

  - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy.
  - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for example, illegal Internet use or child protection concerns.
  - If inappropriate material is accessed, users are required to immediately report this to the designated safeguarding lead (Vice Principal) and the Network Manager at TECC so this can be considered for monitoring purposes and appropriate action will then be taken.

8. Working in Partnership with Parents and Carers

- We are committed to working in partnership with parents and carers and understand the key role they play in maintaining the safety of their children, through promoting Internet safety at home and elsewhere.

- We also appreciate that there may be some parents who are concerned about the use of the new technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a strategy that will allow their child to fully access the curriculum, whilst remaining safe.

9. Appendices of the E-safety Policy

- Related aspects of the school's e-safety framework include acceptable use policies for both staff and students; ICT equipment (onsite and offsite) and data security.

- The School ICT AUP policies are electronic and appear when staff/students first log on to the school network and/or if changes are made to the AUP.

- When staff/students accept the Policy this is logged on our Management System (RM). If staff/students decline the policy it will not let them log into our network. If staff/students have any concerns they should speak to the Network Manager.

- We use RmSafetynet for our Internet filtering. All filtering is via a transparent proxy for students and a proxy bypass for staff and can be viewed by the IT Department.

- Our staff/student data is backed up offsite to secure cloud servers via GenzoSolutions. Any staff/student network files that are lost/deleted can be reasonably retrieved and restored but there may be times when said files maybe corrupt before being backed up.