Online Safety Policy

Tees Valley Education Trust

Version:	1.0
Ratified by:	Trust Board
Name of originator/author:	S Mayle
Circulated to:	All staff
Date issued:	September 2025
Review date:	Annual
Target audience:	ALL TRUST EMPLOYEES

TABLE OF CONTENTS

1 STATEMENT OF INTENT 3
2 DEFINITIONS 3
3 KEY ROLES AND RESPONSIBILITIES 3
4 TRAINING AND PROFESSIONAL DEVELOPMENT 4
5 SOCIAL MEDIA USE 4
5.1 Trust/Curriculum 4
5.2 Staff 4
5.3 Pupils and Parents/Carers 5
5.4 Blocked Content 6
6 CYBER BULLYING 6
7 IT SAFETY AND DATA PROTECTION 7
8 GAMING 7
9 PREVENT 8

1 STATEMENT OF INTENT

Tees Valley Education understands that social media, digital technology and online learning is a growing part of life outside our academies. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet in our academies, and to educate our pupils about how to protect themselves online within the wider community.

As a Trust we are committed to:

- encouraging the responsible use of digital technology and online platforms in support of the academy's mission, values and objectives
- using appropriate social media to promote the work of Tees Valley Education and its academies
- protecting our pupils from the dangers of a range of online platforms
- preventing and avoiding damage to the reputation of each academy and the Trust through irresponsible use of social media
- protecting our staff from cyber bullying and potentially career damaging behaviour
- increasing and updating all stake holders' e-safety knowledge on a regular basis
- Providing advice and guidance for remaining safe online whereby online safety refers to any device with the capacity to connect to the internet
- Promoting the PREVENT Duty.

2 DEFINITIONS

Online safety refers to any device with the capacity to connect to the internet and share data and includes but is not limited to internet-connected toys, tablets, smart TVs and watches, phones, laptops and computers.

Tees Valley Education defines "social media" as any online platform that offers real-time interaction between the user and other individuals or groups including but not limited to:

Blogs.

Online discussion forums, such as netmums.com.

Collaborative spaces, such as Facebook, Instagram and Online Gaming.

Media sharing services, such as Class Dojo and YouTube.

'Micro-blogging' applications, such as Twitter.

The Trust defines "cyber bullying" as any use of social media or communication technology to bully an individual or group.

3 KEY ROLES AND RESPONSIBILITIES

The Trust Board delegates the responsibility for the implementation of the Online Safety Policy and procedures to Head Teachers of its academies.

The Trust Board has responsibility for ensuring that the Online Safety Policy, as written, does not discriminate on any grounds, including but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.

Individual Academies and Trust staff have responsibility for correctly handling complaints regarding this policy as outlined in the Trust Complaints Policy.

All staff members within each academy are responsible for ensuring the day-to-day implementation and management of the Online Safety Policy and procedures.

All staff in each academy, including teachers, support staff and volunteers, are responsible for following the Online Safety Policy, as well as ensuring all pupils do so. They are responsible for ensuring the policy is implemented fairly and consistently in the classroom and wider academy community.

Whilst academy staff will support where possible, parents and carers are expected to take responsibility for the online habits of their child/children at home.

Parents and carers are expected to promote safe online behaviour.

4 TRAINING AND PROFESSIONAL DEVELOPMENT

Tees Valley Education recognises that early intervention can protect pupils who may be at risk of cyber bullying or negative online behaviour. As such, all stake holders will receive appropriate online safety training, as organised and facilitated by each individual academy.

Teachers and support staff will receive training on the Online Safety Policy as part of the annual safeguarding training plan, or their academy induction as appropriate.

As well as Online Safety training within safeguarding, Trust staff will also receive appropriate social media training with regard to the academies approaches to promoting the academy and wider Trust.

5 SOCIAL MEDIA USE

5.1 Trust/Curriculum

Trust / Academy social media passwords are kept by delegated Senior Leaders within the establishment. These key staff are responsible for ensuring they are kept secure.

Whilst these may be delegated roles within each academy, the Head Teacher is ultimately responsible for the academy's social media accounts.

Social media should only be used during lesson time if part of a planned curriculum activity. Any use of personal social media is strictly prohibited.

If inappropriate content is accessed online, an inappropriate website content report form should be completed and passed on to the designated senior leader in each academy (see appendix 2)

The use of mobile phone technology is strictly prohibited as part of curriculum teaching. Further details of use of phones is outlined in our Mobile Phone Policy and individual academy handbooks.

5.2 Staff

Whilst it is not encouraged during the working day, Teachers may use social media on their personal technology devices during their break times. These devices may only be used in designated areas as agreed in each academy.

Members of staff should not use personal social media in front of pupils. Also see mobile phone policy.

Members of staff **must not** "friend" or otherwise contact pupils or parents/carers through social media.

If pupils or parents/carers attempt to "friend" or otherwise contact members of staff through social media, they should be reported to the Head Teacher.

Members of staff should avoid identifying themselves as an employee of Tees Valley Education on social media.

Members of staff **must not** post content on personal social media with regard to the Trust, their academy or any of its staff or pupils.

Where teachers or members of staff use social media in a personal capacity, any views posted should be personal.

Staff members **must** report to their Head Teacher any content they view on social media which brings negative representation to the Trust or Individual Academy.

Teachers or members of staff **must not** post any information which could identify a pupil, class or the academy.

Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.

Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.

Members of staff should be aware that if their out-of-work activity brings Tees Valley Education into disrepute, disciplinary action will be taken.

Members of staff should regularly check their online presence for negative content via search engines.

Attempts to bully, coerce or manipulate members of the academy community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.

Members of staff should not leave a computer or other device logged on when away from their desk, or save passwords (refer to Trusts Password Security Policy).

Staff members should use their academy email address for academy business and personal email address for their private correspondence; the two should not be mixed.

5.3 Pupils and Parents/Carers

Pupils may not access social media during lesson time, unless it is part of a curriculum activity overseen by a member of staff.

Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.

Pupils and parents/carers **must not** attempt to "friend" or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they should be reported to the Head Teacher.

If members of staff attempt to "friend" or otherwise contact pupils or parents/carers through social media, they should be reported to the Head Teacher.

Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.

Pupils and parents/carers **must not** post content online which is damaging to the academy or any of its staff or pupils.

Pupils within Tees Valley Education are reminded that they **must not** sign up to social media sites that have an age restriction above the pupil's age.

If inappropriate content is accessed online on academy premises, it **must** be reported to a teacher.

5.4 Blocked Content

The following websites are identified as blocked by the network's firewalls:

- Facebook
- Instagram
- Twitter
- Any games that involve a chat function

Many other sites are blocked in order to ensure the safety of all stakeholders. This is managed and regularly updated by One IT (Trusts IT provider).

Attempts to circumvent the network's firewalls will result in a ban from using academy computing equipment, other than with close supervision.

Inappropriate content which is accessed on the academy computers should be reported to the Head Teacher so that the site can be blocked.

Requests may be made to access erroneously blocked content by submitting a "blocked content access" form (appendix 1) to the Head Teacher who will make the final decision on whether access to the site may be granted.

KCSIE (Keeping Children Safe in Education) requires schools to implement appropriate online filtering and monitoring systems to protect pupils from harmful content and to ensure a safe online learning environment as well as avoiding disinformation, misinformation and conspiracy theories. These systems are not 100% effective but aim to block inappropriate websites and content while allowing for some user autonomy. The Designated Safeguarding Lead (DSL) is now responsible for ensuring these systems are in place, reviewed annually, and that staff are aware of their importance and limitations. These filtering and monitoring arrangements apply to the use of generative AI where applicable in the classroom. Filtering and monitoring is supported by our IT Provider (ONEIT).

6 CYBER BULLYING

Within Tees Valley Education cyber bullying of any stakeholder is taken very seriously.

Incidents of cyber bullying will be dealt with and reported in line with the Anti-Bullying and safeguarding Policy.

Staff members should never respond or retaliate to cyberbullying incidents. Incidents should instead be reported as inappropriate, and support sought from their line manager or senior staff member.

Evidence from the incident should be saved, including screen prints of messages or web pages, and the time and date of the incident.

Where the perpetrator is a current pupil or colleague, most cases can be dealt with through the academy's own disciplinary procedures.

Where the perpetrator is an adult, in nearly all cases, a senior staff member should invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.

If the perpetrator refuses to comply, the incident and content will be reported to the CEO in order to decide upon next points of action. This may include contacting the individuals by formal letter or contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions.

If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the police will be contacted.

As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and PSHE.

Be **SMART** online

All teachers and pupils will embody a **SMART** approach to online behaviour which will be made explained and embedded through definitive and explicit teaching:

Safe – Do not give out personal information, or post photos of yourself to people you talk to online. Follow age restriction rules.

Meeting – Do not meet somebody you have only met online. We encourage parents/carers to speak regularly to their children about who they are talking to online.

Accepting – We advise that pupils only open emails and other forms of communication from people they already know.

Reliable – We teach pupils about the dangers of believing everything they see online.

Tell – We encourage pupils to tell a teacher, parent or carer if they see anything online that makes them feel uncomfortable.

A number of further resources to support staff pupils and parents are available at https://brambles.teesvalleyeducation.co.uk/parents/e-safety/

7 IT SAFETY AND DATA PROTECTION

The Trust advocates the use of ONE IT to support safety infrastructure and Data Protection alongside a rigid GDPR Policy. The academy must ensure:

- Manage data in compliance with the Data Protection Act 2018 (see GDPR Policy)
- uses a firewall and robust antivirus software
- uses a recognised internet service provider

- actively monitors and filters any inappropriate websites or content
- uses an encrypted and password protected WiFi network.

8 GAMING

Online gaming is hugely popular with children and young people and there are many ways for users to connect and play games online.

These include free games found on the internet, games on mobile phones, handheld consoles and other devices, as well as downloadable games and boxed games on PCs and consoles. Internet connectivity in a game adds a new opportunity for gamers as it allows players to find, chat with and play against/with other players from around the world (in a multi-player game).

The guidance for gaming includes all aspects relating to online safety. By using the SMART principles, acceptable use and guidance above children should be able to use these platforms safely. However, there are additional expectations to be considered:

- Parents, pupils and teachers should talk with children about the types of games they are playing. Discuss the levels of appropriateness of game type (role-playing games, sports games, strategy games or first-person shooters)
- Pupils and parents should be aware of the age and content ratings on games. These ratings should be treated the same way that we treat film classifications. The regulatory body **PEGI** rate all games on sale in the UK. Teachers should discuss these ratings with staff through explicit online safety teaching
- Parents and pupils need to be aware that some games may offer children the chance to chat with other players by voice and text. Teachers should ensure children are aware that they need to know who they are playing with and talking to. If chat is available, then the type of language that is used by other players may be an issue for consideration. Explicit teaching by parents and teachers should include identifying what to do if they experience anything they deem as unacceptable.

9 PREVENT

The passing of the Counter-Terrorism and Security Act 2015 means educational establishments now have a statutory duty to prevent students from being drawn into terrorism. With the Internet and social media playing a huge role in the radicalisation of young people, a comprehensive security approach is essential for complying with the government's Prevent duty.

Schools now have a requirement to look much deeper into internet and social media traffic to identify potential children at risk. This includes identifying sites that may appear innocuous but attempt to display harmful content to children and to keep accurate records of exactly who does what, whether the internet requests are allowed or blocked. This helps to identify the signs of radicalisation, whether explicit or significant as part of a pattern of behaviour.