1. Introduction

IT and the internet are a significant part of the curriculum and is a necessary tool for learning.

The safe and appropriate use of technology results from a co-ordinated approach between curriculum leadership, safeguarding leadership, and network management. This policy reflects key responsibilities in ensuring this and should be read in conjunction with other Trust and Academy policies including:

- Information Security Policy
- Acceptable Use Policies
- Surveillance Policy
- Code of Conduct policies
- Child Protection and Safeguarding Policy
- Student code of conduct policy and disciplinary procedures
- Behaviour policies

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for Academies on:

- Teaching online safety in academies
- Preventing and tackling bullying and online bullying: advice for headteachers and academy staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle online bullying by, if necessary,

searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and Responsibilities

Academy Leadership (CEO, Academy Head Teachers, Senior Leadership Team):

- Ensure the safety (including online safety) of all members of the academy community
- Ensure adequate training is provided to staff regarding online safety including at induction
- follow procedures in the event of a serious online safety allegation being made concerning a member of staff or student
- Ensure online safety is considered alongside other safeguarding discussions at staff meetings
- Monitor
- online safety incidents to inform future areas of teaching/learning or training
- Ensure all staff complete Online Safety training.
- Provide academy-wide opportunities to discuss online safety in detail
- Provide information and awareness to parents and staff through a variety of sources including newsletters, parents' forums, and signposting.

IT Manager

- Ensure the academy's infrastructure is secure and not open to misuse/attack
- Stay up to date regarding network security and implement security measures
- Ensure monitoring systems are operational to keep track of internet sites used across the academies and colleges or ensure that third party monitoring and filtering complies with these requirements
- Manage, review and monitor the academy filtering policy with the DoR
- Review breaches with the DoR

Curriculum leadership

- Ensure a planned online safety curriculum is provided, ensuring relevance, breadth, and progression, including sharing relevant resources with teaching teams such as Child Exploitation and Online Prevention (CEOP).
- Ensure appropriate training within the academy community on Online safety
- Ensure staff are aware of procedures in the event of an Online safety incident

Teaching/Support staff

- Have up to date awareness of online safety matters and the Trust's online safety policy (and associated policies) and practices
- Embed online safety issues in the curriculum, as well as pastoral and tutorial activities, to ensure that students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Report any suspected misuse or incident to the trust leadership.
- Guide students to age-appropriate websites, checked as suitable for their use

Designated Safeguarding Leads and Deputy Safeguarding Officers

Safeguarding leadership must ensure they have relevant training in Online 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

- online bullying

These are child protection issues, not technical issues, where technology provides additional means for child protection issues to develop. The Safeguarding leadership must engage with outside agencies as appropriate e.g., where criminal activity may be suspected.

Local Governing Body & Trustees

Monitor the implementation of this policy as part of the overall monitoring arrangements carried out across the various sites within the trust.

4. Incidents of misuse

All members of the trust are expected to be responsible users of digital technologies. However, there may be times when infringements of the policy could take place, through careless, lack of understanding, SEN, irresponsibility or, very rarely, through deliberate misuse.

Incidents of misuse will be investigated. At least one senior member of staff will be involved in this process to protect individuals if accusations are subsequently reported. Investigations will contain access logs of individuals under investigation, which will be saved and shared with investigating bodies. The URL of any site containing the alleged misuse will be recorded and the nature of the content causing concern will be described. It may also be necessary to record and store screenshots of the content to be used in the investigation. These may be printed and attached to any incident investigation report (except in the case of images of child sexual abuse). Any internal response, disciplinary procedures or referral to local authority agencies or the police will depend on the outcome of any investigation.

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

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

It is more likely that the trust will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents of misuse may be dealt with through disciplinary procedures set out in the Staff Disciplinary procedure. All types of misuse cannot be predicted due to the changing nature of IT.

Examples of misuse include:

- Deliberately accessing or trying to access material that could be considered illegal
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person’s account
- Careless use of personal data e.g., holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying data of other users or causing deliberate damage to hardware or software
- Sending an email, or other message regarded as offensive, harassing or of a bullying nature

- Actions which could compromise a staff member's professional standing
- Actions which could bring the trust into disrepute or breach the integrity of the trust's ethos
- Using software or internet sites to subvert the academy's filtering system
- Breaching copyright or licensing regulations

Where the misuse relates to filtering or security breaches, or use of sites which should be filtered, the IT Manager will investigate and report to Academy Leadership and the Executive Team.

5. Educating parents about online safety

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

6. IT Infrastructure, Equipment, Filtering and Monitoring

Academies within the Trust are responsible for ensuring that infrastructure is safe and secure and that procedures within this policy are implemented. The management of technical security is the responsibility of the IT Manager.

The IT Manager will ensure that:

- users can only access data to which they have right of access
- no user should be able to access another's files, other than that allowed for monitoring purposes within the academy's policies, unless specifically shared by the owner of these files.
- access to personal data is securely controlled in line with the Trust's Data Protection policy
- logs are maintained of access by users and of their actions while using the system (e.g., via firewall logs, inadvertent or deliberate access of unauthorised systems or data)
- there is effective guidance for users
- there is oversight from senior leaders, and this has impact on policy and practice.
- Appropriate security measures are in place through network software to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the academy systems and data. The academy infrastructure and individual workstations are protected by up to date protection software.
- All users will have clearly defined access rights to academy technical systems**.** Guest temporary access onto the trust's networks will be via dedicated guest user accounts (which have very minimal access). Access to specific academy systems will be by agreement of the academy's leadership. Guest account use must be recorded for possible future auditing.
- A safe and secure username/password system will apply to all trust technical systems, including networks, devices, email.
- Internet access is filtered for all users. Content lists are regularly updated automatically, and Internet use is logged and regularly monitored. Requests for filtering changes must be agreed by relevant staff.

Staff who have responsibility for web sites, or other systems that requires external authentication, must record user account data in a password protected document to support disaster recovery.

7. Online Bullying

Online bullying takes place through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing online bullying

To help prevent online bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The academy will actively discuss online bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss online bullying with their students.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover online bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, trustees and volunteers (where appropriate) receive training on online bullying, its impact and ways to support students, as part of safeguarding training

Academies within the trust send information on online bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of online bullying, the academy will follow the processes set out in the behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The Principal/Headteachers, and any member of staff authorised to do so by these members of staff can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students
- Is identified in the academy rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Principal/headteacher/DSL.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student’s cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm
- Undermine the safe environment of the academy or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to [the staff member in conjunction with the DSL / Principal / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next.

Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

8. Staff remote working

It is understood that on some occasion employees of the Trust will need to work at home or away from the Trust premises. If this is the case then the employees will adhere to the controls listed in the Trust' Information Security Policy.

9. Acceptable use of the internet

Use of the trust's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. Our ICT team monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. Staff must read the Computer Users Code of Conduct and ensure they abide by the requirements of online safety.

Across college campuses students upon enrolment are provided with a copy of the Computer Users' Code of Conduct and must sign a student agreement.

Within the primary academy there is an EYFS-KS1 and KS2 acceptable use agreement in place and across the Behavioural Unit there are also acceptable use agreements in place for students.

Internet is moderated by the IT support team who follow the measures outlined in the Web Filtering and Monitoring IT Systems Policy to ensure acceptable use of the internet.

In the event that there is an unacceptable use of the internet within the trust the measures identified in Section 4 of this policy will be carried out.

Date of Last Approval/Revision	October 2022
Review interval (years)	Three Years
Responsible Officer	IT Manager
Approval/review body (ies)	Extended Executive Team
Date of next review	October 2025
Public File location	TVCT SharePoint

This policy has been subject to an Equality Impact Assessment by:

Author/Reviewer: D.Laybourne/M.Russon

SLT/EET: EET Dec 2022

Governors/Trustees:

Appendix 1. Annual review

Tees Valley Collaborative Trust recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. It is essential however that care is taken with the information that is made public because once a comment or posting is made, it may not be possible to take it back; there will always be a permanent digital record of it. The Trust aims to deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology, including mobile and smart technology. This review has been created to protect all members of the academy community (including staff, students, students, volunteers, parents/carers and visitors) who have access to and are users of academy systems both in and out of the trust.

The trust will complete a risk assessment to review all risks face by our academy community on an annual basis to ensure robust control measures are in place to safeguard stakeholders to the organisations

Risk Assessment to consider and cope with risks faced by the academy community

Service Area Tees Valley Collaborative Trust			**Section**	**Work activity** Online Security risks faced by the TVCT community
Date of assessment October 2022	**Date of previous**	**Review Date** October 2023	**Number of pages** 2	**Persons involved in assessment** Dean Laybourne – Director of Resources Mark Russon – IT Manager

Hazard Identified		**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**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	Child sexual abuse images –The making, production, or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					□
	Grooming, incitement, arrangement, or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					□
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					□
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of					□

contain or relate to:	sexual orientation) - contrary to the Public Order Act 1986					
	Pornography				□	
	Promotion of any kind of discrimination					□
	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 academy or brings the academy into disrepute				□	
Using academy systems to run a private business					□	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the trust					□	
Infringing copyright					□	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						□
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					□	
On-line gaming (educational)		□				
On-line gaming (non educational)			□			
On-line gambling					□	
On-line shopping / commerce				□		
File sharing				□		
Use of social media					□	
Use of messaging apps					□	
Use of video broadcasting e.g. YouTube					□	