THE CONSORTIUM
ACADEMY TRUST

Shaping Positive Futures

Online Safety Policy (Secondary Schools)

The Consortium Academy Trust (TCAT)
An Exempt Charity Limited by Guarantee
Company Number 07665828

Status:	Live
Policy Owner (position)	Trust DSL
Statutory / Recommended	Statutory
Date Adopted	February 2025
Review Period	12 months
Latest Review Date	10.2.25
Revision	0
Next Review Date	February 2026
Advisory Committee	LGB
Linked Documents and Policies	**Legislation/Statutory guidance.** • Voyeurism (Offences) Act 2019 • The UK General Data Protection Regulation (UK GDPR) • Data Protection Act 2018 • DfE (2024) 'Filtering and monitoring standards for schools and colleges' • DfE (2021) 'Harmful online challenges and online hoaxes' • DfE (2024) 'Keeping children safe in education 2024' • DfE (2023) 'Teaching online safety in school' • DfE (2022) 'Searching, screening and confiscation' • DfE (2023) 'Generative artificial intelligence in education' • Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' • UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition' • National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

	This policy operates in conjunction with the following school policies/documents: • ICT Acceptable Use Policy • Child Protection and Safeguarding Policy • Child-on-child Abuse Policy • Anti-Bullying Policy • Staff Code of Conduct • Behaviour Policy • Disciplinary Policy and Procedure • Data Protection Policy • Device User Agreement • Prevent Policy • Whistleblowing Policy

**NB – This document can only be considered valid when viewed on The Consortium Academy Trust website. If the copy is printed or downloaded and saved elsewhere the Policy date should be cross referenced to ensure the current document is referenced*

CONTENTS

POLICY STATEMENT

1.0 Why the Policy is Needed

2.0 What the Policy is About

3.0 What the Policy will Achieve

PROCEDURE

Table of Contents:

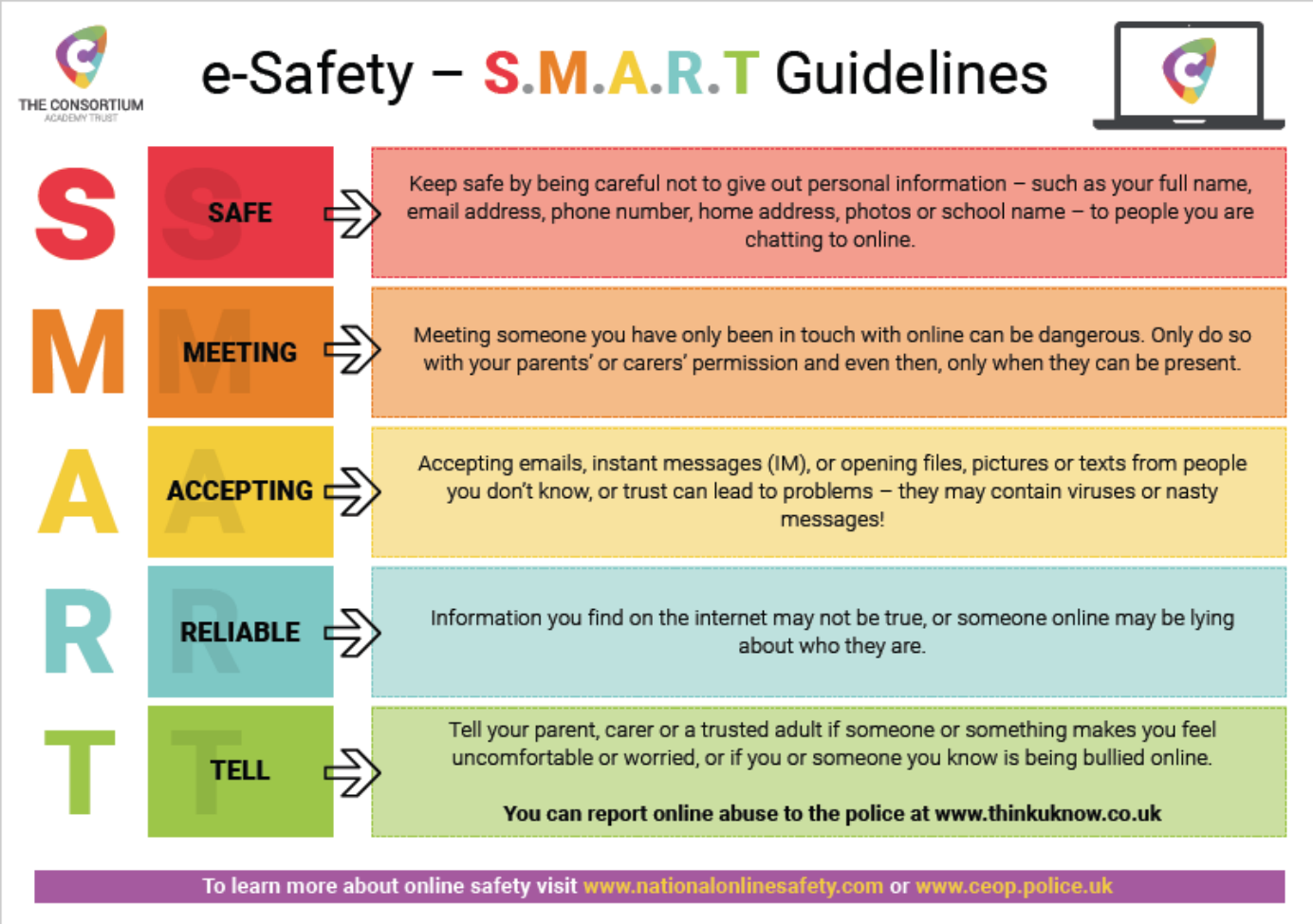
POLICY STATEMENT

1 Why the Policy is needed

At the Consortium Academy Trust we understand that using online services is an important aspect of raising educational standards, promoting learner achievement and enhancing teaching and learning. The use of online services is embedded throughout our schools and therefore we have a number of controls in place to ensure the safety of learners and staff.

This policy is specifically for staff and learners in our secondary schools and sixth form colleges. There is a separate E Safety Policy for primary schools.

The policy should be read with the e safety SMART guidelines:



2 What the policy is about

We have outlined the responsibilities of all online users and made it clear how users should report any concerns when online.

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

Content – Being exposed to illegal, inappropriate or harmful material e.g. pornography, fake news, self – harm and suicide and discriminatory or extremist views

Contact – Being subjected to harmful online interaction with other users e.g. peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit children

Conduct – Personal online behaviour that increases the likelihood of, or causes harm e.g. sending/receiving explicit messages and cyber bullying

Commerce – Risks such as online gambling, inappropriate advertising, phishing and / or financial scams

3 What the policy will achieve

All staff, learners and governors will be aware of their responsibilities towards online safety.

We created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all learners and staff.

PROCEDURE

1. Roles and responsibilities

The Trust Board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring each school DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.

The Headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive annual (or more often as required), up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Working with Trust ICT leads to ensure online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping learners safe.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that learners with SEND face online.
- Ensuring that there are appropriate filtering and monitoring systems in place and current
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT team.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to any occasions of remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by learners and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about key online safety issues including sharing of inappropriate imagery.
- Working with the Headteacher and governing board to update this policy on an annual basis.

The ICT team will be responsible for:

- Providing technical support in the development and implementation of the Trust's online safety policies and procedures.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT team and service providers
- Implementing appropriate security measures

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use / have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that learners may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Learners will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

2. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

It is important to acknowledge that to over block content can be more harmful and the reason for filtering needs to be fully understood. See the following guidance Navigating the Latest Changes in DfE Filtering and Monitoring Standards for Schools and Colleges

The DSL has overall responsibility for their school's approach to online safety, with support from deputies and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about learners' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive updates including regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by learners to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that learners displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action. If the concern is about the Headteacher, it is reported to the LGB Chair of Governors.

Concerns regarding a learner's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and ICT Technician, and manages concerns in accordance with relevant policies e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

If the concern is regarding a staff member the IT team will consult with the Headteacher (or if the concern is regarding a member of shared services the Director that line manages that person) as it may be that there was a legitimate reason for the staff member being on a particular site. The HT /Director may decide if the case is to be managed using the Disciplinary Policy.

Where there is a concern that illegal activity has taken place, the DSL will contact the police.

Each school will avoid unnecessarily criminalising learners, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a learner has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded on CPOMS.

3. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain learners can be more at risk of abuse and/or bullying online, such as LGBTQ+ learners and learners with SEND.

Cyberbullying against learners or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with our Anti-bullying Policy.

4. Child-on-child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that learners are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

All staff will be aware of potential risks through annual online safety training, DSL annual update training and identified National college modules, but will specifically be aware of risks relating to Grooming and Exploitation, Child sexual exploitation (CSE) and child criminal exploitation (CCE)and Radicalisation – as referenced in the Child protection and Safeguarding Policy.

5. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a learner's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a learner is suffering from challenges in their mental health. Concerns about the mental health of a learner will be dealt with in line with the Child Protection and Safeguarding Policy.

6. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the learner and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst learners in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to learners, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing learners.

- Not inadvertently encouraging learners to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger learners but is almost exclusively being shared amongst older learners.
- Proportional to the actual or perceived risk.
- Helpful to the learners who are, or are perceived to be, at risk.
- Appropriate for the relevant learners' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting learners at risk of harm, they will ensure that the challenge is directly addressed to the relevant learners, e.g. those within a particular age range that is directly affected or individual learners at risk where appropriate.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing learners' exposure to the risk is considered and mitigated as far as possible. Support will be gained from ICT at Trust level.

7. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that learners with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a learner's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that learners are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

In addition, the school will use clear curriculum coverage to raise awareness for learners and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber crime. The school will implement it's cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges'.

8. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that learners are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

9. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSHE/PSHE
- ICT

Online safety teaching is always appropriate to learners' ages and developmental stages.
Learners are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours learners learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks learners may face online are always considered when developing the curriculum.

The DSL will be involved with the development of the school's online safety curriculum. Learners will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO, will work together to ensure the curriculum is tailored so that learners who may be more vulnerable to online harms, e.g. learners with SEND and CLA, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from learners.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of learners. Lessons and activities will be planned carefully so they do not draw attention to a learner who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which learners feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything learners raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a learner makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

10. Use of technology in the classroom

A wide range of technology will be used during lessons, including computers, laptops, emails and cloud based resources.

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that learners use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Learners will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

11. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Learners will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the Trust's ICT Acceptable Use Policy.

Staff will use all smart technology and personal technology in line with the school's ICT Acceptable Use Policy.

The school recognises that learners' unlimited and unrestricted access to the internet via mobile phone networks means that some learners may use the internet in a way which breaches the school's acceptable use of ICT agreement for learners and that is why mobile phones are not permitted to be used on the school site unless for educational purposes.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Learners (up to and including Year 11) will not be permitted to use smart devices or any other personal technology whilst on the school site. Where there is a significant problem with the misuse of smart technology among learners, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating learners about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

12. Educating parents

The school will work in partnership with parents to ensure learners stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents can access the Acceptable Use Agreement at the beginning on the school and Trust website and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it. All learners will sign to accept the Acceptable Use Policy at the start of joining school and periodically thereafter.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of learners, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources

13. Internet access

Learners, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Policy. All learners will sign to accept the Acceptable Use Policy at the start of joining school and periodically thereafter.

All members of the school community will be encouraged to use the school's internet network as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

14. Filtering and monitoring online activity

The Trust Board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The filtering and monitoring systems the school implements will be appropriate to learners' ages, the number of learners using the network, how often learners access the network, and the proportionality of costs compared to the risks. ICT will undertake termly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the ICT helpdesk. Prior to making any changes to the filtering system, ICT and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT. Reports of inappropriate websites or materials will be made to ICT immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT, who will escalate the matter appropriately. If a learner has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

15. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by The Trust ICT team. Firewalls will be switched on at all times. Firewalls will be reviewed to ensure they are running correctly, and to carry out any required updates.

Staff and learners will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks.

All members of staff will have their own unique usernames and private passwords to access the school's systems. All learners will be provided with their own unique username and passwords. Staff members and learners will be responsible for keeping their passwords private.

Users will inform the ICT Team if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time.

Users will be required to lock access to devices and systems when they are not in use.

16. Emails

Staff and learners will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and learners must agree to the ICT Acceptable Use Policy. Staff are to avoid the use of personal email accounts on the school network unless needed to facilitate their work, and never to communicate with any learner attending the school. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Any emails sent between staff and learners should always be school -related, of a professional nature and should not take place outside of school hours or during holidays.

Staff members and learners will be required to block spam and junk mail, and report the matter to ICT. The monitoring system can detect inappropriate links, malware and profanity within emails – staff and learners will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

All staff will complete training on the appropriate use of ICT and potential harm including:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

17. Generative artificial intelligence (AI)

The school will take steps to prepare learners for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to learners' age.

We will ensure the IT system includes appropriate filtering and monitoring systems to limit learner's ability to access or create harmful or inappropriate content through generative AI. We will ensure that learners are not accessing or creating harmful or inappropriate content, including through generative AI.