High Tunstall College of Science

Inspire | Support | Achieve

Online Safety Policy

Revised	-	March 2022
Stakeholder Consulted	-	Admissions and Safeguarding Committee
Review Date	-	March 2024
Responsibility for Review	-	Headteacher

Contents:

Statement of intent

High Tunstall College of Science understands that using online services is an important aspect of raising educational standards, promoting student achievement, and enhancing teaching and learning. The use of online services is embedded throughout the college; therefore, there are a number of controls in place to ensure the safety of students and staff.

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 and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect students and staff revolve around these areas of risk. Our college has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following college policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Data Security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Sex, Relationships and Health Education Policy
- Staff Code of Conduct
- Behavioural Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Photography and Video Policy
- Remote Learning Policy
- Student ICT Acceptable Use Policy
- Staff ICT Acceptable Use Policy

2. Roles and responsibilities

The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the designated safeguarding team's remit covers online safety.
- Reviewing this policy on a biennial basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.

- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant college policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the college's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the designated safeguarding team by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the college is keeping students safe.
- Working with the designated safeguarding team and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the designated safeguarding team and governing body to update this policy on an biennial basis.

The designated safeguarding team is responsible for:

- Taking the lead responsibility for online safety in the college.
- Acting as the named point of contact within the college on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the college's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the college's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the college's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Ensuring all members of the college community understand the reporting procedure.

- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the college's provision, and using this data to update the college's procedures.
- Reporting to the governing body about online safety on a termly basis.
- Working with the headteacher and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the headteacher and governing body to update this policy on a biennial basis.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the college's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the college's filtering and monitoring systems are updated as appropriate.
- Working with the designated safeguarding team and headteacher to conduct half-termly light-touch reviews of this policy.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or 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 students may be unsafe online.
- Reporting concerns in line with the college's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Students are responsible for:

- Adhering to the ICT Acceptable Use Policy and other relevant policies.
- Seeking help from college 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.

3. 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.

The designated safeguarding team has overall responsibility for the college'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 students' safety online.

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

Staff receive regular training

- Staff receive regular email updates 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 termly on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by students 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.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a student's online behaviour are reported to the designated safeguarding team, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The college avoids unnecessarily criminalising students, 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 student has taken and distributed indecent imagery of themselves. The designated safeguarding team 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 college's response are recorded by the designated safeguarding team.

4. Cyberbullying

Cyberbullying can include 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
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

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

5. Peer-on-peer sexual abuse and harassment

Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of college and off and online, and will remain aware that students 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.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The college responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the college premises or using college-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the designated safeguarding team, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that students who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The student believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The student does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The student may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the student feel 'special', particularly if the person they are talking to is older.
- The student may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact students are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The designated safeguarding team will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the college and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a student may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting

and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about students with relation to CSE or CCE, they will bring these concerns to the designated safeguarding team without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain students at increased vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any students displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a student relating to radicalisation, they will report this to the designated safeguarding team without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy.

7. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in students, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of college can have a substantial impact on a student's mental state, both positively and negatively. The designated safeguarding team 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 student is suffering from challenges in their mental health. Concerns about the mental health of a student will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. 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 student 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 students in the college, they will report this to the designated safeguarding team immediately.

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

Where the designated safeguarding team's assessment finds an online challenge to be putting students at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant students, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The designated safeguarding team and headteacher will only implement a college-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible.

9. 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 college will factor into its approach to online safety the risk that students 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 student's use of technology and their intentions with regard to using their skill and affinity towards it, the designated safeguarding team 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 designated safeguarding team and headteacher will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that students cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on college-owned devices or on college networks through the use of appropriate firewalls.

10. Online safety training for staff

The designated safeguarding team ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that students 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.

Information about the college's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, the Peer-on-peer Abuse Policy and the Child Protection and Safeguarding Policy.

11. Online safety and the curriculum

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

- RSE
- Health education
- PSHE
- Citizenship
- Computing

Online safety teaching is always appropriate to students' ages and developmental stages.

Students 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 students learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks students may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix A of this policy.

The designated safeguarding team is involved with the development of the college's online safety curriculum. Students 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.

The college recognises that, while any student can be vulnerable online, there are some students who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. students with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these students receive the information and support they need.

The college 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 students.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for students?
- Are they appropriate for students' developmental stage?

External visitors may be invited into college to help with the delivery of certain aspects of the online safety curriculum. The headteacher and designated safeguarding team decide when it is appropriate to invite external groups into college and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and designated safeguarding team consider the topic that is being covered and the potential that students in the class have suffered or may be suffering from online abuse or harm in this way. The designated safeguarding team advises the staff member on how to best support any student who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a student 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 ensures a safe environment is maintained in which students 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 students raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a student 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.

12. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets

- Email
- Cameras
- VR headsets

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

Students are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

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

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

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

The college recognises that students' unlimited and unrestricted access to the internet via mobile phone networks means that some students may use the internet in a way which breaches the college's ICT Acceptable Use Policy for students.

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.

Students will not be permitted to use smart devices or any other personal technology during college hours. Personal devices must be stored in the student's locker, or with their Head of Year/Student Support Officer if they do not have access to their locker.

Where it is deemed necessary, the college will ban student's use of personal technology whilst on college site.

Where there is a significant problem with the misuse of smart technology among students, the college will discipline those involved in line with the college's Behavioural Policy.

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

The college will consider the 4C's (content, contact, conduct and commerce) when educating students about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

The college works in partnership with parents to ensure students stay safe online at college and at home. Parents are provided with information about the college's approach to online safety and their role in protecting their children. Parents are sent a copy of the ICT Acceptable Use Policy when their child joins the college (and as and when there are updates) and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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 students, 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 is raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources

15. Internet access

Students, staff and other members of the college community may be refused access to the college's internet network if they have not read and signed the ICT Acceptable

Use Policy. A record is kept of users who have signed and returned their ICT Acceptable Use Policy in the college office.

All members of the college community are encouraged to use the college's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

Senior ICT Technician ensures the college's ICT network has appropriate filters and monitoring systems in place. The Senior ICT Technician ensures 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

The Senior ICT Technician undertakes a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the college implements are appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks. ICT technicians undertake frequent checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the Senior ICT Technician. Prior to making any changes to the filtering system, ICT technicians check the suitability of a site. Any changes made to the system are recorded by ICT technicians. Reports of inappropriate websites or materials are made to an ICT technicians immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the designated safeguarding team and ICT technicians, who will escalate the matter appropriately. If a student has deliberately breached the filtering system, they will be disciplined in line with the Behavioural 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 college's network and college-owned devices are appropriately monitored. All users of the network and college-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the designated safeguarding team who manages the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and students are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to ICT technicians.

All members of staff have their own unique usernames and private passwords to access the college's systems. All students are provided with their own unique username and private passwords. Staff members and students are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords expire after 60 days, after which users are required to change them.

Users inform ICT technicians if they forget their login details, who will provide the user with their username and reset their password. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Head of Year is informed and decides the necessary action to take.

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

Full details of the college's network security measures can be found in the Data Security Breach Prevention and Management Plan.

18. Emails

Access to and the use of emails is managed in line with the Data Protection Policy and the ICT Acceptable Use Policy.

Staff and students are given approved college email accounts and are only able to use these accounts at college and when doing college-related work outside of college hours. Prior to being authorised to use the email system, staff and students must agree to and sign the ICT Acceptable Use Policy. Personal email accounts are not permitted to be used on the college site. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and students are required to block spam and junk mail, and report the matter to ICT technicians. The college's monitoring system can detect inappropriate links, malware and profanity within emails – staff and students are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened. Students are taught about phishing emails within the curriculum.

Any cyber-attacks initiated through emails are managed in line with the Data Security Breach Prevention and Management Plan.

19. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and students are not permitted to use social media for personal use during lesson time. Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during college hours may result in the removal of internet access or further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the college. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff are not permitted to communicate with students or parents over social networking sites and are reminded to alter their privacy settings to ensure students and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or student, and thus are connected with them on social media, e.g. they are friends with a parent at the college, they will disclose this to the designated safeguarding team and headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the college.

Students are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the college community on social media are reported to the designated safeguarding team and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behavioural Policy.

Use on behalf of the college

The use of social media on behalf of the college is conducted in line with the Social Media Policy. The college's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the college's social media accounts.

All communication on official social media channels by staff on behalf of the college is clear, transparent and open to scrutiny.

20. The college website

The headteacher is responsible for the overall content of the college website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and students is not published on the website. Images and videos are only posted on the website if the provisions in the Photography and Video Policy are met.

21. Use of devices

College-owned devices

Staff members may be issued with the following devices to assist with their work:

- Laptop
- Tablet

Students are provided with college-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

College-owned devices are used in accordance with the ICT Acceptable Use Policy. Staff and students are not permitted to connect college-owned devices to public Wi-Fi networks. All networked college-owned devices are password protected.

ICT technicians review all college-owned devices which are on site on a termly basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. Staff are responsible for applying updates to college owned devices which they use off site, or alternativity should return the device to college on a termly basis to ensure updates can be applied. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Cases of staff members or students found to be misusing college-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

Personal devices

Personal devices are used in accordance with the ICT Acceptable Use Policy, Students Code of Conduct Policy and Staff Code of Conduct Policy. Any personal electronic device that is brought into college is the responsibility of the user.

Personal devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff are encouraged to take photos and videos of students using college equipment; however, they may use their own devices such as a mobile phone. Staff who use their personal device, to take images or videos of students, must

ensure these images are uploaded to the appropriate platform in college and deleted from the personal device within 48 hours. Further information can be found in the Photography and Video Policy.

Staff members report concerns about their colleagues' use of personal devices on the college premises in line with the Allegations of Abuse Against Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

Students are not permitted to use their personal devices during lesson time or when moving between lessons. If a student needs to contact their parents during the college day, they must speak to their Head of Year/Student Support Officer. The headteacher may authorise the use of mobile devices by a student for safety or precautionary use.

Where a student uses accessibility features on a personal device to help them access education, e.g. where a student who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Students' devices can be searched, screened and confiscated in accordance with the Behaviour Policy. If a staff member reasonably believes a student's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

22. Remote learning

All remote learning is delivered in line with the college's Remote Learning Policy.

The college will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The college will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The college will ensure that all college-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the college will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.

- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The college will not be responsible for providing access to the internet off the college premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the college.

23. Monitoring and review

The governing body, headteacher and designated safeguarding team will review this policy on a biennial basis and following any online safety incidents.

The next scheduled review date for this policy is March 2024.

Any changes made to this policy are communicated to all members of the college community.

Appendix A: Online harms and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect students' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong,	This risk or harm is covered in the

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
	misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	following curriculum areas: • RSHE/PSHCE • Computing • Tutor Time
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What students should do if they are harmed, targeted, or groomed as a	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
	result of interacting with a fake website or scam email • Who students should go to for support	
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
	• How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How students can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	• Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • How adverts seen at the top of online searches and social media have often come from companies	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
	paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	• Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing • Tutor Time
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Tutor Time

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
	• That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Tutor Time
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
	• The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching students about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	
Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if students would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That students should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
	• The risks of grooming	
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour • That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people students do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what students are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for students to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
	anxiety, depression and other mental health issues • That isolation and loneliness can affect students and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE • Computing
Suicide, self-harm and eating disorders	Students may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for students and should take care to avoid giving instructions or methods and avoid using language, videos and images.	This risk or harm is covered in the following curriculum areas: • RSHE/PSHCE