



SoundSkool Music

Online Safety Policy

Last Review Date	1 September 2025
Review Date	26 August 2026
Reviewed By	Simon Gordon
Amendments Made Since Last Review Date	



Contents

Statement of intent	3
1. Legal framework.....	4
Roles and responsibilities.....	5
2. Managing online safety	6
3. Cyberbullying	8
4. Child-on-child sexual abuse and harassment.....	8
5. Grooming and exploitation	9
6. Mental health.....	10
7 Online hoaxes and harmful online challenges	10
14....Internet access	14
15. Filtering and monitoring online activity	15
16. Network security.....	15
17. Emails	16
18. Generative artificial intelligence (AI).....	17
19. Social networking	17
20. The college website.....	17
21. Use of devices.....	17
22. Remote learning.....	18
23. Monitoring and review	18

Statement of intent

SoundSkool 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 (Use and Access) Act 2025
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for colleges and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education 2025'
- DfE (2023) 'Teaching online safety in college'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2025) '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 college policies:

- Social Media Policy
- Cyber-security Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Photography and Images Procedure
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy

Roles and responsibilities

The Governance board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the 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.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant college policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Head of College will be 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 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 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.
- Working with the DSL and Governance board to update this policy on an annual basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the college.
- 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,
- 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.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff, and ensuring all members of the college community understand this procedure.
- Understanding the filtering and monitoring processes in place at the college.

- 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 college.
- 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 college's provision, and using this data to update the college's procedures.
- Reporting to the Governance board about online safety on a termly basis.
- Working with the Head of College and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the Head of College and Governance board to update this policy on an annual basis.

All staff members will be 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 will be responsible for:

- Adhering to the Acceptable Use Agreement 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.

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.

The DSL/Head of College has overall responsibility for the college's approach to online safety and will ensure that there are strong processes in place to handle any concerns about students' 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 college operations in the following ways:

- Staff and practitioners 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

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 student 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 students displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

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 Head of College, who decides on the best course of action in line with the relevant policies. If the concern is about the Head of College, it is reported to the chair of governors.

Concerns regarding a student's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Head of College and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Head of College 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 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 college's response are recorded by the DSL.

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

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.

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 college, 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
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a college culture that normalises abuse and leads to students becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of 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 will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other students taking "sides", often leading to repeat harassment.

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

5. 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, e.g. 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 DSL 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 online.
- 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 DSL 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, as outlined in the Prevent Duty Policy. 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 DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

6. Mental health

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 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 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.

7 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 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 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 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 Head of College 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 DSL's assessment finds an online challenge to be putting students at risk of harm, 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 individual students at risk where appropriate.

The DSL and Head of College 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 c
- 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 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 Head of College will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. 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 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.

11. Online safety and the curriculum

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

- PSHE
- Music Business

Online safety teaching is always appropriate to students'

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
- 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 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 DSL will be 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

Relevant members of staff, e.g. the SENCO will work together to ensure the curriculum is tailored so that students who may be more vulnerable to online harms, e.g. students with SEND 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 will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students.

External visitors may be invited into college to help with the delivery of certain aspects of the online safety curriculum. The Head of College and DSL will 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 DSL will 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 DSL will advise the staff member on how to best support any student who may be especially impacted by a lesson or activity. Lessons and activities will be 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 will ensure 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 will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras

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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Students will be 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.

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 acceptable use of ICT agreement 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 whilst in the classroom.

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 Behaviour 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 4Cs (**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....Internet access

Students, staff and other members of the college community will only be granted access to the college's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access on the encrypted college cloud.



All members of the college community will be 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.

15. Filtering and monitoring online activity

The Governance board will ensure the college's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's ['Filtering and monitoring standards for colleges and colleges'](#). The Governance board will ensure 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

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 college's safeguarding needs.

The Head of College and CEO will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the college implements will be 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 will undertake monthly 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 Head of College. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician 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 technicians, who will escalate the matter appropriately. If a student 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 college's network and college-owned devices will be appropriately monitored. All users of the network and college-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.

16. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will



review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

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

All members of staff will have their own unique usernames and private passwords to access the college's systems. Students in class, year or key stage and above will be provided with their own unique username and private passwords. Staff members and students will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after **90** days, after which users will be required to change them.

Users will inform ICT technicians 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. If a user is found to be sharing their login details or otherwise mistreating the password system, the Head of College will be informed and will decide the necessary action to take.

Users will be 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 Cyber-security Policy.

17. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Student Confidentiality Policy and Staff and Volunteer Confidentiality Policy.

Staff and students will be given approved college email accounts and will only be 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 Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the college site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and students will be 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 will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. ICT technicians will organise an annual assembly where they explain what a phishing email and other malicious emails might look like – this assembly will include information on the following:

- 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

18. Generative artificial intelligence (AI)

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

The college will ensure its IT system includes appropriate filtering and monitoring systems to limit student's ability to access or create harmful or inappropriate content through generative AI.

The college will ensure that students are not accessing or creating harmful or inappropriate content, including through generative AI.

The college will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The college will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

19. Social networking

The use of social media by staff and students will be managed in line with the college's Social Media Policy.

20. The college website

The Head of College will be 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 will be managed in line with the College Website Policy.

21. Use of devices

Staff members and students will be issued with college-owned devices to assist with their work, where necessary. Requirements around the use of college-owned devices can be found in the college's Device User Agreement.

The use of personal devices on the college premises and for the purposes of college work will be managed in line with the Staff ICT and Electronic Devices Policy and Students' Personal Electronic Devices Policy.

22. Remote learning

All remote learning will be delivered in line with the college's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

23. Monitoring and review

The college recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the Head of College conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

The Governance board, Head of College and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is 31 August 2026.

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

Online harms and risks – curriculum coverage

[The table below contains information from the DfE’s ‘Teaching online safety in colleges’ guidance about what areas of online risk colleges should teach students about. You can use this to assist your college in developing its own online safety curriculum; however, you must develop your curriculum in line with your local needs and the needs of your students.]

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	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> That age verification exists and why some online platforms ask users to verify their age <input type="checkbox"/> Why age restrictions exist <input type="checkbox"/> That content that requires age verification can be damaging to under-age consumers <input type="checkbox"/> What the age of digital consent is (13 for most platforms) and why it is important 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Health education <input type="checkbox"/> Music Business
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> What a digital footprint is, how it develops and how it can affect students’ futures <input type="checkbox"/> How cookies work <input type="checkbox"/> How content can be shared, tagged and traced <input type="checkbox"/> How difficult it is to remove something once it has been shared online <input type="checkbox"/> What is illegal online, e.g. youth-produced sexual imagery (sexting) 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business

<p>Disinformation, misinformation and hoaxes</p>	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Disinformation and why individuals or groups choose to share false information in order to deliberately deceive <input type="checkbox"/> Misinformation and being aware that false and misleading information can be shared inadvertently <input type="checkbox"/> Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs <input type="checkbox"/> Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons <input type="checkbox"/> 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 <input type="checkbox"/> How to measure and check authenticity online <input type="checkbox"/> The potential consequences of sharing information that may not be true 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Fake websites and scam emails</p>	<p>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 will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> How to recognise fake URLs and websites <input type="checkbox"/> What secure markings on websites are and how to assess the sources of emails <input type="checkbox"/> The risks of entering information to a website which is not secure <input type="checkbox"/> What students should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email <input type="checkbox"/> Who students should go to for support <input type="checkbox"/> The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business

<p>Online fraud</p>	<p>Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> What identity fraud, scams and phishing are <input type="checkbox"/> That online fraud can be highly sophisticated and that anyone can be a victim <input type="checkbox"/> How to protect yourself and others against different types of online fraud <input type="checkbox"/> How to identify 'money mule' schemes and recruiters <input type="checkbox"/> The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal <input type="checkbox"/> The risk of sharing personal information that could be used by fraudsters <input type="checkbox"/> That children are sometimes targeted to access adults' data <input type="checkbox"/> What 'good' companies will and will not do when it comes to personal details <input type="checkbox"/> How to report fraud, phishing attempts, suspicious websites and adverts 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Password phishing</p>	<p>Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Why passwords are important, how to keep them safe and that others might try to get people to reveal them <input type="checkbox"/> How to recognise phishing scams <input type="checkbox"/> The importance of online security to protect against viruses that are designed to gain access to password information <input type="checkbox"/> What to do when a password is compromised or thought to be compromised 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business

<p>Personal data</p>	<p>Online platforms and search engines gather personal data – this is often referred to as ‘harvesting’ or ‘farming’. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> How cookies work <input type="checkbox"/> How data is farmed from sources which look neutral <input type="checkbox"/> How and why personal data is shared by online companies <input type="checkbox"/> How students can protect themselves and that acting quickly is essential when something happens <input type="checkbox"/> The rights children have with regards to their data <input type="checkbox"/> How to limit the data companies can gather 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Persuasive design</p>	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> 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 to encourage them to spend money or generate advertising revenue <input type="checkbox"/> How notifications are used to pull users back online 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Privacy settings</p>	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> How to find information about privacy settings on various sites, apps, devices and platforms <input type="checkbox"/> That privacy settings have limitations 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business

<p>Targeting of online content</p>	<p>Much of the information seen online is a result of some form of targeting. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts <input type="checkbox"/> How the targeting is done <input type="checkbox"/> The concept of clickbait and how companies can use it to draw people to their sites and services 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>How to stay safe online</p>		
<p>Online abuse</p>	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The types of online abuse, including sexual harassment, bullying, trolling and intimidation <input type="checkbox"/> When online abuse can become illegal <input type="checkbox"/> How to respond to online abuse and how to access support <input type="checkbox"/> How to respond when the abuse is anonymous <input type="checkbox"/> The potential implications of online abuse <input type="checkbox"/> What acceptable and unacceptable online behaviours look like 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Radicalisation</p>	<p>Students are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> How to recognise extremist behaviour and content online <input type="checkbox"/> Which actions could be identified as criminal activity <input type="checkbox"/> Techniques used for persuasion <input type="checkbox"/> How to access support from trusted individuals and organisations 	<p>All areas of the curriculum</p>

<p>Challenges</p>	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal <input type="checkbox"/> How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why <input type="checkbox"/> That it is okay to say no and to not take part in a challenge <input type="checkbox"/> How and where to go for help <input type="checkbox"/> The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Content which incites violence</p>	<p>Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> That online content (sometimes gang related) can glamorise the possession of weapons and drugs <input type="checkbox"/> That to intentionally encourage or assist in an offence is also a criminal offence <input type="checkbox"/> How and where to get help if they are worried about involvement in violence 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Fake profiles</p>	<p>Not everyone online is who they say they are. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> That, in some cases, profiles may be people posing as someone they are not or may be 'bots' <input type="checkbox"/> How to look out for fake profiles 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business

<p>Grooming</p>	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Boundaries in friendships with peers, in families, and with others <input type="checkbox"/> Key indicators of grooming behaviour <input type="checkbox"/> The importance of disengaging from contact with suspected grooming and telling a trusted adult <input type="checkbox"/> How and where to report grooming both in college and to the police <p>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.</p>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Livestreaming</p>	<p>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 will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content <input type="checkbox"/> That online behaviours should mirror offline behaviours and that this should be considered when making a livestream <input type="checkbox"/> That students should not feel pressured to do something online that they would not do offline <input type="checkbox"/> The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next <input type="checkbox"/> The risks of grooming 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business

<p>Pornography</p>	<p>Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> That pornography is not an accurate portrayal of adult sexual relationships <input type="checkbox"/> That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour <input type="checkbox"/> That not all people featured in pornographic material are doing so willingly, e.g. revenge porn or people trafficked into sex work 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Unsafe communication</p>	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with <input type="checkbox"/> How to identify indicators of risk and unsafe communications <input type="checkbox"/> 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 <input type="checkbox"/> What online consent is and how to develop strategies to confidently say no to both friends and strangers online 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Wellbeing</p>		
<p>Impact on confidence (including body confidence)</p>	<p>Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The issue of using image filters and digital enhancement <input type="checkbox"/> The role of social media influencers, including that they are paid to influence the behaviour of their followers <input type="checkbox"/> That 'easy money' lifestyles and offers may be too good to be true <input type="checkbox"/> The issue of photo manipulation, including why people do it and how to look out for it 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business

<p>Impact on quality of life, physical and mental health and relationships</p>	<p>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 will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> How to evaluate critically what students are doing online, why they are doing it and for how long (screen time) <input type="checkbox"/> How to consider quality vs. quantity of online activity <input type="checkbox"/> 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 <input type="checkbox"/> That time spent online gives users less time to do other activities, which can lead some users to become physically inactive <input type="checkbox"/> The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues <input type="checkbox"/> 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 <input type="checkbox"/> Where to get help 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Online vs. offline behaviours</p>	<p>People can often behave differently online to how they would act face to face. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business

<p>Reputational damage</p>	<p>What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Strategies for positive use <input type="checkbox"/> How to build a professional online profile 	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business
<p>Suicide, self-harm and eating disorders</p>	<p>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.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> RSHE <input type="checkbox"/> PHSE <input type="checkbox"/> Music Business