Rye College Policy

Policy Title:	Online Safety Policy
Leadership Responsibility:	Deputy Headteacher
Review Body:	Head Teacher
Date:	December 2023
Review:	December 2024

Statement of intent

Rye College (the Academy) 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 Academy; therefore, there are a number of controls in place to ensure the safety of students and colleagues.

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 colleagues revolve around these areas of risk. The Academy 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 colleagues.

Objectives

This policy applies to all members of the college community (including colleagues, students, volunteers, families, visitors, community users) who have access to and are users of our technology systems, both in and out of the Academy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off-site and empowers colleagues to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the Academy, but is linked to membership of the Academy.

The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Management Policy.

The Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

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 (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in college'
- DfE (2022) 'Searching, screening and confiscation'
- 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'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following Trust and Academy policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Students' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Safeguarding and Child Protection Policy

- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Remote Education Policy

Roles and Responsibilities

The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the college community, though the day-to-day responsibility for online safety will be delegated to the DSL and Online Safety Lead.

The Head Teacher and senior leaders are aware of the procedures to be followed in the event of a serious online safety allegation being made against a colleague.

The Head Teacher and senior leaders are responsible for ensuring the DSL and Online Safety Lead and other relevant colleagues receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Head Teacher and senior leaders will ensure there is a system in place to allow for monitoring and support of those who carry out internal online safety monitoring. This is to provide a safety net and also support those colleagues who take on important monitoring roles. The Trust undertakes quality assurance through the work of the Compliance Officer.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the Academy.
- Taking day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the Online Safety Policy including understanding the filtering and monitoring systems and processes in place.
- Ensuring all colleagues are aware of the procedures that need to be followed in the event of an online safety incident taking place using My Concern.
- Providing training and advice for colleagues.
- Liaising with the Local Authority, Trust or relevant body.
- Liaising with Schools ICT Support.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Reports to relevant meetings of the Aquinas Advisory Council to discuss current issues, review incident logs and filtering/change control logs.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that Students with SEND face online.
- Ensuring online safety is recognised as part of the Academy's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the Academy's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and colleagues, and ensuring all members of the college community understand this 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 Academy's provision, and using this data to update the Academy's procedures.
- Reporting to the Head Teacher/Trust/Aquinas Advisory Council about online safety on a termly basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the Academy's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Head Teacher/DSL.
- Ensuring that the Academy's filtering and monitoring systems are updated as appropriate.

All colleagues 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 Academy's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Having an understanding of filtering and monitoring (see below).

Be vigilant:

- **Report it** - if you see or suspect inappropriate use of IT equipment to access unsuitable material.
- **Report it** - if through lesson planning, you come across unblocked content that is unsuitable.
- **Report it** - if the system fails for some reason and allows inappropriate content to be shown.
- **Tell the IT team and DSL** - if you are preparing a topic which may lead to unsuitable material being inadvertently accessed or searched for.
- **Tell the IT team and DSL** - if access feels too restricted for the study of a topic or in not allowing students to actively make self-filtering decisions on content.

Smoothwall monitoring:

- **Proactive real-time monitoring** - Captures user activity as it happens, automatically sending potential risks through to the Monitor portal and My Concern.

- **Online and offline monitoring** - Captures activity that may indicate a risk, even outside of the regular web browser such as in a Word Document, Messaging app, or encrypted "dark web" browser.

- **Auto pre-grading** - A 24/7 in-house team of Moderators review captures to minimise false positives and contact you by phone for any urgent risks.

- **Alert notifications** - Alerts are sent in real-time by phone, email, and stored within the intuitive portal for the DSL to review. These also go directly to My Concern.

Students will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from colleagues 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 via informing staff or via yourconcern@ryecollege.co.uk
- Are expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking or use of images and on online bullying.
- Should understand the importance of adopting good online safety practices when using digital technologies out of school and realise the Online Safety Policy covers their actions out of school, if related to their membership of the college community.

Managing online safety

All colleagues 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 has overall responsibility for the Academy's approach to online safety, with support from deputies and the Head Teacher where appropriate, 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 Academy operations in the following ways:

- Colleagues receive regular updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies and tutor time themes on the topic of remaining safe online.
- Rules for use of ICT systems and internet are posted in relevant rooms.

Handling online safety concerns

Any disclosures made by students to colleagues 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 Safeguarding and Child Protection Policy.

Colleagues 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. Colleagues 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 colleague's online behaviour are reported to the Head Teacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Head Teacher, it is reported to the CEO of the Trust.

Concerns regarding a student's online behaviour are reported via My Concern, the safeguarding team investigates concerns with relevant staff members, e.g. the Head Teacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding and Child Protection Policy.

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

The Academy 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 Safeguarding and Child Protection Policy.

All online safety incidents and the Academy's response are recorded on My Concern.

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 Academy 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 colleagues 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.

Child-on-child sexual abuse and harassment

Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Colleagues will understand that this abuse 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 colleagues 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 colleagues 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. Colleagues 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.

Colleagues 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 Academy 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 Academy will respond to these incidents in line with the Safeguarding and Child Protection and Anti Bullying Policies.

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

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.
Colleagues 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 colleagues 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 Academy 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 colleagues have any concerns about students in relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding and Child Protection 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.

Colleagues will be aware of the factors which can place certain students at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Colleagues will be expected to exercise vigilance towards any students displaying indicators that they have been, or are being, radicalised.

Where colleagues 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 in the Safeguarding and Child Protection Policy.

Mental health

Colleagues 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 colleagues 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.

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 colleagues suspect there may be a harmful online challenge or online hoax circulating amongst students in the Academy, they will report this via My Concern.

The 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 Academy 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 Teacher 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 Safeguarding and Child Protection 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 Teacher will only implement an Academy-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.

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 Academy 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. (https://www.nationalcrimeagency.gov.uk/cyber-choices)

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

Online safety training for colleagues

The DSL ensures that all safeguarding training given to colleagues includes elements of online safety, including how the internet can facilitate abuse and exploitation. All colleagues 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.

Online safety and the curriculum

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

- RSHE
- Life Education
- ICT

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.
- 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 Online Media Literacy Report

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 Academy'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 Inclusion Manager/SENCO/Designated Teacher for LAC, will ensure the curriculum is tailored so that students who may be more vulnerable to online harms, e.g., students with SEND and LAC, receive the information and support they need.

The Academy 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 the Academy to help with the delivery of certain aspects of the online safety curriculum. The Head Teacher 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 colleague 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 colleague is concerned about anything students raise during online safety lessons and activities, they will make a report in line with the Safeguarding and Child Protection Policy.

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

Use of technology in the classroom

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

- Computers
- Laptops
- Email
- Cameras
- Smartphones

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.

Use of smart technology

While the Academy recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the Academy 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 Academy's Technology Acceptable Use Agreement for Students.

Colleagues will use all smart technology and personal technology in line with the Academy's Colleague ICT and Electronic Devices Policy.

The Academy 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 Academy'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.
- Recording (visually and / sound only) without all parties' explicit written consent.

Students will not be permitted to use smart devices or any other personal technology whilst in the classroom. Mobile phones should not be used on Academy premises.

Where it is deemed necessary, the Academy will ban students' use of personal technology whilst on site.

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

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

The Academy 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.

Educating parents

The Academy will work in partnership with parents to ensure students stay safe online at college and at home. Parents will be provided with information about the Academy's approach to online safety and their role in protecting their children.

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 will be raised in the following ways:

- Parents' evenings
- Newsletters
- Letters
- Website
- Information about all relevant national or local online safety campaigns and literature
- Information about useful organisations or support services for reporting online safety issues

Internet access

Students, colleagues and other members of the college community will only be granted access to the Academy'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 in their school files as part of the admissions process, for colleagues in their personnel files in HR.

All members of the college community will be encouraged to use the Academy'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.

Filtering and monitoring online activity

The DSL will ensure the Academy's ICT network has appropriate filters and monitoring systems in place. The DSL 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 Head Teacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the Academy 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. (SWGfL) testing tool)

Requests regarding making changes to the filtering system will be directed to the DSL. 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 Management Policy. If a colleague 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 Academy's network and Academy-owned devices will be appropriately monitored. All users of the network and Academy-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 Safeguarding and Child Protection Policy.

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 to ensure they are running correctly, and to carry out any required updates.

Colleagues 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 colleagues will have their own unique usernames and private passwords to access the Academy's systems. All students will be provided with their own unique username and private passwords. Colleagues 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, HR/the Student Hub will be informed.

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

Full details of the Academy's network security measures can be found in the Technical Security Policy.

Emails

Access to and the use of emails will be managed in line with the Trust Data Protection Policy, and Academy Acceptable Use Agreement.

Colleagues and students will be given approved Rye 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, colleagues and students must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the Academy site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Colleagues and students will be required to block spam and junk mail, and report the matter to ICT technicians. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. As part of Life Education students will learn about 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.

Any cyber-attacks initiated through emails will be managed in line with the Emergency Contingency Plan.

Social Networking

The use of social media by colleagues and students will be managed in line with the Academy’s Social Media Policy.

The College website

The Head Teacher 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.

Use of devices

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

The use of personal devices on the Academy premises and for the purposes of Academy work will be managed in line with the Trust’s policy.

Remote learning

All remote learning will be delivered in line with Academy guidelines.

Monitoring and review

The Academy recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the Head Teacher conduct annual reviews of this policy to evaluate its effectiveness.

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

December 2023 DDo

EQUALITIES

We recognise that our students bring with them a wide variety of behaviours influenced by life experiences outside college. We aim to respond to each case professionally, objectively and compassionately. We are sensitive when working with children and families with specific needs and experiences and we continuously seek ways to promote successful partnerships. The basis of differentiation will vary dependant on the needs of each case but we will take into account the views of parents and families, colleagues and external agencies together with any Statement of Special Educational Need or Education, Health and Care Plan.

We will also ensure compliance with the Trust's Equality Policy taking into account students with protected characteristics and making reasonable adjustments for students with a disability within the meaning of the Equality Act 2010. Both the college and Trust respects the Public Sector Equality Duty (PSED) that requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations between different people when carrying out their activities. By following the Trust's Equality Policy, the college seeks to eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by such legislation.

DATA PROTECTION

Rye College [The Academy] processes personal data in accordance with the data protection principles embodied in the General Data Protection Regulations (GDPR) and the Data Protection Act 2018. The Academy complies with the requirements of the data protection legislation as detailed in the Trust Data Protection Policy.

All colleagues are aware of the principles of data protection and will not process personal data unless necessary. The Academy safeguards the personal data it collects through the operation of the Trust's data protection policy and processes and the IT policy. In addition, the Academy has taken steps to ensure that all its contracts that process data have the GDPR compliant provisions.

Appendix A

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.

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 will include 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 will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include 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 will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive	This risk or harm will be covered in the following curriculum areas: • Key Stage 3 ICT

	• Misinformation and being aware that false and misleading information can be shared inadvertently • Malinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g., releasing private information or photographs • 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	• Life Education • RSHE
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 will include 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 result of interacting with a fake website or scam email • Who Students should go to for support • 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	This risk or harm will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim	This risk or harm will be covered in the following curriculum areas: • Key Stage 3 ICT

	• How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts	• Life Education • RSHE
Password phishing	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: • 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 will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following: • How cookies work • 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	This risk or harm will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE

	• How to limit the data companies can gather	
Persuasive design	• 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: • 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 • How notifications are used to pull users back online	This risk or harm will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE
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 will include the following: • How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include the following: • 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 • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some	This risk or harm will be covered in

	cases, can be illegal. Teaching will include 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	the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE
Radicalisation	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: • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include 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 • 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	This risk or harm will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE

Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include 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 will be covered in the following curriculum areas: - Key Stage 3 ICT - Life Education - RSHE
Fake profiles	Not everyone online is who they say they are. Teaching will include 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 will be covered in the following curriculum areas: - Key Stage 3 ICT - Life Education - RSHE
Grooming	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: - Boundaries in friendships with peers, in families, and with others - Key indicators of grooming behaviour - The importance of disengaging from contact with suspected grooming and telling a trusted adult - How and where to report grooming both in college 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.	This risk or harm will be covered in the following curriculum areas: - Key Stage 3 ICT - Life Education - RSHE

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 will include the following: • What the risks of carrying out livestreaming are, e.g., the potential for people to record livestreams and share the content • 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 • The risk of watching videos that are being livestreamed, e.g., there is no way of knowing what will be shown next • The risks of grooming	• Key Stage 3 ICT • Life Education • RSHE
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include 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, e.g., revenge porn or people trafficked into sex work	This risk or harm will be covered in the following curriculum areas: • RSHE
Unsafe communication	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: • 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	This risk or harm will be covered in the following curriculum areas: • Key Stage 3 ICT • Life Education • RSHE

	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	
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to ‘unrealistic’ online images. Teaching will include 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 - That ‘easy money’ lifestyles and offers may be too good to be true - The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm will be covered in the following curriculum areas: - RSHE
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 will include 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 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	This risk or harm will be covered in the following curriculum areas: - Health education

	- Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: - 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	This risk or harm will be covered in the following curriculum areas: - RSHE
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following: - Strategies for positive use - How to build a professional online profile	This risk or harm will be covered in the following curriculum areas: - RSHE
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.	