ROCHESTER INDEPENDENT COLLEGE

ONLINE SAFETY
2024/25

Contents

1. Scope of the Online Safety Policy

This Online Safety Policy outlines Rochester Independent College's commitment to safeguarding our college community (including staff, learners, governors, parents, carers, and visitors) both on and off-campus in accordance with statutory guidance and best practice. It also applies to the use of personal digital technology on the college site (where permitted).

This policy is created in line with DfE statutory guidance, including 'Keeping Children Safe in Education' (2024), 'Working Together to Safeguard Children' (2023), and Medway Local Authority guidance. It aims to safeguard and promote the welfare of all RIC community members when using online, mobile and smart technology.

This policy is linked to:
Anti-bullying policy
Behaviour and discipline policy
Safeguarding and child protection policy
Staff code of conduct
Curriculum policies (Computing, PSHE, Citizenship, RSE)
Searching and confiscation policy

2. Process for Monitoring the Impact of the Online Safety Policy

The college will monitor the policy's impact through:

- Logs of reported incidents
- Filtering and monitoring logs
- Surveys/questionnaires from:
    - Students
    - Parents and carers
    - Staff

3. Policy and Leadership Responsibilities

To ensure effective online safeguarding, we must work together to develop safe and responsible online behaviours, learning from each other and from best practices elsewhere, and reporting inappropriate online behaviours, concerns, and misuse as soon as they arise. While this is a team effort, the following sections outline the online safety roles and responsibilities within the college.

3.1 Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safeguarding of the college community, including online.
- The Principal, Senior Vice Principal, and DSL are aware of the procedures to follow in the event of a serious online safety allegation against a staff member.

- The Principal and senior leaders are responsible for ensuring that the DSL, Director of IT, and other relevant staff carry out their responsibilities effectively and receive appropriate training.
- They will receive regular monitoring reports from the DSL.

- They will work with the responsible Governor, the DSL, and Director of IT on all aspects of filtering and monitoring.

3.2 Governors

Governors are responsible for the approval of the Online Safety Policy and reviewing its effectiveness. The Safeguarding Governor or a representative from the Governing Body will:

- Attend regular meetings with the DSL to ensure provisions are in place.
- Regularly receive (collated and anonymised) reports of online safety incidents.
- Ensure the filtering and monitoring provision is reviewed and recorded annually.
- Receive cyber-security training.

- Be a member of the college Online Safety Group

3.3 Designated Safety Lead (DSL)

The DSL will:

- Hold lead responsibility for online safety within their safeguarding role.
- Receive relevant and regularly updated training in online safety.
- Meet regularly with the online safety Governor, Principal, and senior leadership team to discuss current issues and review incidents and filtering and monitoring logs.
- Ensure filtering and monitoring checks are carried out.
- Be responsible for receiving reports of online safety incidents and deciding on referrals by liaising with relevant agencies, ensuring all incidents are recorded.
- Lead the Online Safety Group.
- Promote awareness of and commitment to online safety education across the college and beyond.
- Liaise with curriculum leaders to ensure the online safety curriculum is planned, mapped, embedded, and evaluated.
- Ensure all staff are aware of the procedures to follow in the event of an online safety incident and the need to immediately report those incidents.

- Provide or identify sources of training and advice for staff, governors, parents, carers, and students.

3.4 Curriculum Leads

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme through:

- PHSE and SRE programmes
- A cross-curricular programme
- Assemblies and pastoral programmes
- Drop-down PSHE/RSE teaching days in KS5

- Relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying Week

3.5 Teaching and Support Staff

College staff are responsible for ensuring that:

- They understand that online safety is a core part of safeguarding.
- They immediately report any suspected misuse or problem to the safeguarding team for investigation/action, following college safeguarding procedures.
- All digital communications with students and parents/carers are professional and only carried out using official college systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other college activities (where allowed) and implement current policies regarding these devices.
- In lessons where internet use is pre-planned, students are guided to suitable sites, and processes are in place for dealing with any unsuitable material found.
- Where lessons involve live-streaming or video-conferencing, national safeguarding guidance and local policies are followed.
- There is zero-tolerance for incidents of online bullying, sexual harassment, discrimination, hatred, etc.
- They model safe, responsible, and professional online behaviours in their use of technology, including out of college and on social media.
- They attend regular, annual online safety training with updates throughout the year and understand their responsibilities, including the Staff Acceptable Use Agreement.

- They attend induction training for online safety, ensuring they fully understand the college online safety policy and acceptable use agreements.

3.6 Director of IT and Operations

The Director of IT and Operations is responsible for ensuring that:

- They are aware of and follow the college Online Safety Policy and Technical Security Policy.
- The college's technical infrastructure is secure and not open to misuse or malicious attack.
- The college meets (at a minimum) the required online safety technical standards as identified by the DfE, local authority, or other relevant body.
- There is clear, safe, and managed control of user access to networks and devices.
- They keep up to date with online safety technical information to effectively carry out their role and inform and update others.
- Technology use is regularly and effectively monitored to report any misuse/attempted misuse to the safeguarding team.

- Monitoring systems are implemented and regularly updated.

3.7 Students

The college acknowledges, learns from, and uses students' skills and knowledge in digital technologies to shape the online safety strategy and contribute positively to their personal development. Their contribution is recognised through:

- Student feedback and opinion.
- Appointment of digital leaders.
- Learner representation in the Online Safety Group.
- Contributions to the online safety education programme e.g. peer education, online safety campaigns.

- Designing/updating acceptable use agreements.

Students are responsible for:

- Using the college's digital technology systems in accordance with the student acceptable use agreement and Online Safety Policy.
- Understanding the importance and process of reporting abuse, misuse, or access to inappropriate materials.

- Adopting good online safety practices when using digital technologies outside of college, as the Online Safety Policy covers actions related to their membership of the college.

3.8 Parents and Carers

The college will provide information and awareness to parents and carers through:

- Regular communication, awareness-raising, and engagement on online safety issues, curriculum activities, and reporting routes.

- Encouraging students to pass on online safety messages learned in lessons.
- Letters, newsletters, and the website.
- High-profile events/campaigns e.g., Safer Internet Day.
- Reference to relevant websites/publications highlighted through the student support app.
- Publishing the Online Safety Policy on the college website.
- Providing a copy of the students' acceptable use agreement.

- Parent representation in the Online Safety Group.

Parents and carers are encouraged to support the college by:

- Reinforcing online safety messages provided to their children.
- Supporting the safe and responsible use of their children's personal devices in and out of college (where allowed).

- Reporting incidents of online misuse by students via phone (01634 828115) or email (DSL@rochester-college.org.uk). Each incident will be considered against local and national guidance, as well as the contextual information of each student involved. Reports to additional safeguarding agencies will be made as appropriate.

3.9 Online Safety Group

The Online Safety Group includes:

- Director of Safeguarding and Pastoral (DSL)
- Director of IT and Operations
- Director of PSHE
- Governors
- Parents and carers

- Students

Members will assist the DSL with:

- Producing, reviewing, and monitoring the college Online Safety Policy/documents.
- Producing, reviewing, and monitoring the college filtering policy and requests for filtering changes.
- Mapping and reviewing the online safety education provision, ensuring relevance, breadth, progression, and coverage.
- Reviewing network/filtering/monitoring/incident logs, where possible and appropriate.

- Monitoring improvement actions identified through the 360-degree safe self-review tool.

4. Reporting and Responding, including Policy breaches

The college will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of the college, impacting the college, which will require intervention. The college will ensure that any online safeguarding concerns are reported and responded to in line with our Safeguarding and Child Protection Policy.

Most incidents will likely involve inappropriate rather than illegal misuse. It is important that incidents are dealt with promptly and proportionately. Incidents will be dealt with through normal behaviour/disciplinary procedures with regard to the Safeguarding and Child Protection Policy. If an online safeguarding concern arises, students or college devices may be searched in line with the College's Searching and Confiscation Policy. Indecent images of children should not be intentionally viewed or copied. Devices suspected of containing illegal content must be reported to the police. Staff may delete harmful data if necessary.

The Leadership Team will review incidents, learn lessons, and update policies as needed. Confidentiality and official reporting procedures must be respected. Complaints and whistleblowing procedures will be communicated to all.

5. Online Safety Education Programme

Online safety is a focus in all areas of the curriculum. The curriculum is broad, relevant, and provides progression, with opportunities for creative activities, provided in the following ways:

- A planned online safety curriculum for all year groups, matched against a nationally agreed framework.
- Lessons matched to need, including age, developmental stage, SEND, EAL, and building on prior learning.
- Context-relevant lessons with agreed objectives leading to clear and evidenced outcomes.
- Effective planning and assessment addressing learner need and progress.
- Incorporating relevant national initiatives and opportunities (e.g., Safer Internet Day and Anti-bullying Week).

- Addressing vulnerability as part of a personalised online safety curriculum (e.g., for victims of abuse and SEND).

6. Appropriate filtering and monitoring

Filtering internet content is important for preventing users from accessing illegal or inappropriate material. While the filtering system cannot provide a 100% guarantee, it is one element in a larger strategy for online safety and acceptable use.

Monitoring user activity on college devices is crucial for providing a safe environment. Unlike filtering, it does not stop users from accessing material but allows review of user activity. The

college uses Securly for filtering and monitoring, sending instant alerts to the safeguarding team for prompt action and recording the outcome.

- RIC will do all we reasonably can to limit student's exposure to online risks through college provided IT systems and will ensure that appropriate filtering and monitoring systems are in place. We are compliant with the DFE filtering and monitoring standards 2023
    - If students or staff discover unsuitable sites or material, they are required to make staff members aware who will alert our Director of IT, Peter Holl.
    - The DSL receives live monitoring updates through Securly when a risk has been identified through the system.
    - The Principal, DSL and Director of IT have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
    - All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation.
    - Filtering breaches or concerns identified through our monitoring approaches will be recorded and reported to the DSL who will respond as appropriate.
    - Any access to material believed to be illegal will be reported immediately to the relevant agencies, such as the Internet Watch Foundation and the Police.
    - When implementing appropriate filtering and monitoring, RIC will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
    - Boarding students accessing our onsite wifi will be subject to the same filtering and monitoring processes. We recognise that there are risks associated with students bringing content on site via their 4G/5G devices. Students will be encouraged to report any concerning content seen on peers' devices and through ongoing education we will continue to support students' individual needs. Any concerns will be responded to appropriately by the DSL.
    - This is reviewed by Governors, the safeguarding team and IT Director at least annually.
- Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of RIC's approach to online safety.
    - Students will use appropriate search tools, apps and online resources.
    - Internet use will be supervised by staff as appropriate to students' age and ability.
    - Students will be directed to use age/ability appropriate online resources and tools by staff.
    - Students will be taught explicitly the risks, consequences and support available for online safety.

7. Technical Security

The college's technical systems will be managed to meet recommended technical requirements, including those from Dukes Education, local, and national policies. Responsibilities include:

- SLT overseeing technical security, with delegation to identified roles.
- Clearly defined access rights to college technical systems and devices, reviewed annually.
- Implementing password policies and procedures (consistent with National Cyber Security Centre guidance).
- Ensuring the security of usernames and passwords.
- Keeping administrator passwords for college systems in a secure password manager..
- Regular reviews and audits of technical systems' safety and security.
- Securely locating servers, wireless systems, and cabling, with restricted physical access.
- Implementing appropriate security measures to protect systems and data, regularly tested.
- Maintaining rigorous and verified back-up routines, with air-gapped copies on-site.
- Ensuring all software is adequately licensed and updated.
- Providing a system for reporting technical incidents/security breaches.
- Regulating the use of college devices outside college and personal devices on the college network.
- Ensuring data protection and encryption at rest and in transit.
- Implementing mobile device security and management procedures.

- Providing appropriate access for guest users based on risk profiles.

8. Safe Use of Mobile and Smart Technologies

RIC recognises the importance of mobile and smart technology in daily life. Users must:

- Protect their devices from loss, theft, or damage.
- Use passwords/PINs to prevent unauthorised access.

Sending abusive or inappropriate messages is forbidden and will be addressed according to anti-bullying, behaviour, and safeguarding policies.

Devices must not contain offensive, derogatory, or illegal content.

8.1 College-Provided Mobile Phones and Devices

Staff may be issued work phones for student/parent communication. College-provided devices must be protected by passwords/PINs and used only by authorised staff/students in accordance with the Acceptable Use Policy (AUP) and staff code of conduct. Activity on these

devices may be monitored for safeguarding purposes; an asset log is kept which shows what device staff and students have been assigned.

8.2 Staff Use of Mobile and Smart Technology

Staff must use personal devices in line with the law and college policies (confidentiality, child protection, data security, staff code of conduct, AUP). Personal devices should be kept secure and switched off or on silent during lessons. Bluetooth or other communication forms should be disabled. Personal devices are not to be used during teaching periods unless in emergencies. Content on personal devices must align with professional roles and behaviour expectations. Staff will only use college-provided devices to take photos/videos of students, work with students during lessons, and communicate with students/parents/carers. Policy breaches will be addressed according to the Safeguarding and Child Protection Policy. Illegal content on personal devices will be reported to the police and LADO.

8.3 Students' Use of Mobile and Smart Technology

Students will be educated on safe use of mobile and smart technology and behaviour expectations. Mobile phones and personal devices can be used on-site but not during lessons unless approved by staff. Devices must be kept secure and not taken into examinations. Breaches will be addressed according to anti-bullying, behaviour, and safeguarding policies.

8.4 Visitors' Use of Mobile and Smart Technology

Visitors must use personal devices appropriately and model positive behaviour. Access to technology for visitors working with students must be approved by the DSL. Staff will address any concerns about visitors' use of technology.

9. Social media

The college implements comprehensive measures to mitigate risks associated with social media use, focusing on protecting personal information and educating learners on responsible online behaviour. This includes training on acceptable use, understanding age restrictions, recognising social media risks, adhering to digital and video images guidance, importance of checking settings, data protection, and the correct procedures for reporting issues. Clear reporting guidelines outline responsibilities, procedures, and consequences, while risk assessments address legal concerns.. College staff are instructed not to discuss or reference personal matters or opinions related to the college community on social media, to maintain privacy settings on personal accounts, and to act as positive role models online. Official college social media accounts require senior leader approval, and clear user behaviour codes, alongside systems for handling abuse and disciplinary actions. The college also proactively monitors public social media for mentions and encourages direct communication from parents/carers with concerns, guiding them towards the college's complaints procedure for unresolved issues.

10. Digital and Video Images

The college will inform and educate users about the risks of digital imaging technologies and implement policies to reduce potential harm:

- Using live-streaming and video-conferencing services in line with safeguarding guidance.
- Educating staff and students about the risks associated with taking, using, sharing, publishing, and distributing images.
- Ensuring staff are aware of students whose images must not be taken/published.
- Allowing parents/carers to take personal use videos and images at college events while respecting privacy.
- Allowing staff to take digital/video images to support educational aims, following college policies for sharing, storage, distribution, and publication.
- Taking care to ensure students are appropriately dressed in shared digital/video images.
- Prohibiting students from taking, using, sharing, publishing, or distributing images of others without permission.
- Selecting photographs for publication carefully and complying with the Online Safety Policy.
- Not using students' full names in association with photographs on websites or blogs.
- Obtaining written permission from parents or carers before taking and using students' photographs.
- Informing parents/carers of the purposes, storage, and retention of images in line with the Data Protection Policy.

- Securely storing images in line with the college retention policy.

11. Computer Misuse and Cyber Choices

All key staff are responsible for safeguarding young people from computer misuse and are aware of the risks of committing cyber crimes as a safeguarding issue.

- Staff are made aware of the safeguarding risks of computer misuse and complete annual training.
- Students agree to the Student Acceptable Use of IT Agreement, outlining acceptable online behaviours and explaining that some online activity is illegal.
- Acceptable computer use is reinforced across the curriculum, with opportunities to discuss acting within moral and legal boundaries online.
- Any breach of the AUP or suspected cybercrime activity will be referred to the DSL for consideration as a safeguarding risk.
- The DSL may refer to the local Cyber Choices programme or seek advice if unsure about referral criteria.

- Parents can report potential cybercrime directly to the local Cyber Choices team but are encouraged to make college-based concerns through the DSL.

12. Policy Monitoring and Review

RIC will review this policy annually or following updates to national/local policies or technical infrastructure. Internet use and online safety mechanisms will be regularly monitored to ensure consistent policy application. Any issues identified will be addressed in action plans.

Created/Updated	**Author**	**Approved by**	**Date**
September 2024	KS, PH and Online Safety Group	AB	September 2024

12. Appendix 1 - Staff Acceptable Use Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use RIC IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for students, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the Internet personally. However, the AUP will help ensure that all staff understand RIC expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that college systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

- I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within RIC both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.
- I understand that RIC Acceptable Use of Technology Policy (AUP) should be read and followed in line with the college Safeguarding and Child Protection policy and staff Code of Conduct and the Use of Mobile and Smart Technology Policy.
- I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the college ethos, college staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of college devices and systems

- I will only use the equipment and Internet services provided to me by the college, for example college provided laptops, tablets, mobile phones, and Internet access, when working with students.
- I will only communicate with learners and parents/carers using official college systems.

Data and system security

- To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

    - I will use a ‘strong’ password to access college systems.
    - I will protect the devices in my care from unapproved access or theft.
- I will respect college system security and will not disclose my password or security information to others.
- I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to IT Department.
- I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the Director of IT.
- I will ensure that any personal data is kept in accordance with the Data Protection legislation.
- Any data being removed from the college site, such as via email or on memory sticks or CDs, will be suitably protected using encryption and passwords.
- I will not keep documents which contain college related sensitive or personal information, including images, files, videos, and emails on any personal devices.
- I will not store any personal files on the college IT system.
- I will ensure that college owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I will not attempt to bypass any filtering and/or security systems put in place by the college.
- If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT Department as soon as possible.
- If I have lost any college related documents or files, I will report this to the Director of IT and college Data Champion as soon as possible.

Classroom practice

- I have read and understood the college mobile and smart technology policy.
- I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where students feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) or an Assistant Designated Safeguarding Lead (ADSL) as part of planning online safety lessons or

activities to ensure support is in place for any students who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with students is appropriate.
- I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL.
- I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them without permission.

Mobile devices and smart technology

- I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff code of conduct and the law.

Online communication, including use of social media

- I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the Safeguarding and Child Protection policy, Staff code of conduct and the law.
- I will take appropriate steps to protect myself and my reputation, and the reputation of the college, online when using communication technology, including the use of social media.
- I will not discuss or share data or information relating to students, staff, college business or parents/carers on social media.
- My electronic communications with current and past students and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via college approved and/or provided communication channels and systems, such as a college email address, user account or telephone number.
    - I will not share any personal contact information or details with students, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past students and/or their parents/carers.
    - If I am approached online by current or past students or parents/carers, I will not respond and will report the communication to the Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or Principal.

- I will only use social networking sites in college in accordance with the college's policies. This means that I will ensure that my account will be set to private and not feature any information or photos of our students.

Policy concerns

- I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
- I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the college into disrepute.
- I will report and record any concerns about the welfare, safety or behaviour of students or parents/carers online to the DSL in line with the college Safeguarding and child protection policy.
- I will report concerns about the welfare, safety, or behaviour of staff online to the Principal, in line with college Safeguarding and child protection policy.

Policy Compliance and Breaches

- If I have any queries or questions regarding safe and professional practice online, either in college or off site, I will raise them with the DSL and/or the Principal.
- I understand that the college may exercise its right to monitor the use of its information systems, including Internet access and the interception of messages/emails on our systems, to monitor policy compliance and to ensure the safety of students and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
- I understand that if the college believes that unauthorised and/or inappropriate use of college systems or devices is taking place, the college may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
- I understand that if the college believes that unprofessional or inappropriate online activity, including behaviour which could bring the college into disrepute, is taking place online, the college may invoke its disciplinary procedures as outlined in the staff code of conduct.

13. Appendix 2 - Student Acceptable Use of IT (AUP)

Computing Facilities

Rochester Independent College provides all students with access to computing and IT facilities through personal, password-protected accounts, offering:

- Access to student PCs, Macs, and laptops
- Secure and backed-up personal file storage
- Shared network drives and resources
- Filtered and monitored Internet access
- College applications (including Google GSuite, Adobe Creative Cloud)
- Shared printers

Interpretation

- College Computers: All PCs, Macs, and laptops owned by the College.
- Programmes: Any executable software, including games and application software.
- Local and Network Drives: Local C:\ drive; network drives such as the “Google Drive” G:\
- Virus: Malicious software designed to cause harm or disruption.
- Inappropriate Content: Pornography, illegal/illicit behaviour, anything deemed inappropriate by the College.
- MAC Address: Unique number identifying a network adapter or interface.

Agreement

You must behave responsibly and safely, including online, following these rules:

College Computers

- Use College computers without disturbing, offending, or disrupting others.
- Behaviour bringing the College’s reputation into disrepute is a serious breach.
- Do not alter the configuration or hardware of College computers.
- Files on College systems can be viewed and monitored by staff.
- Do not install any programmes, including games. If you need any extra programs for academic purposes, please contact the IT office or email itstudentsupport@rochester-college.org.uk.
- Audio/video/image files are only for academic purposes; inappropriate content will be removed.
- Files associated with your student account are deleted 28 days after leaving the college.

- Virus scan any files introduced onto College computers; report any viruses immediately. - you may access support from the IT office to do this if needed. Any virus found must be reported to the IT Office immediately.
- You are liable for costs of replacement/repair of equipment damaged through misconduct, this includes software damage.

- Abuse of College computing facilities may result in restricted or removed access.

Personal Account

- Do not share your login details; you are responsible for actions on your account.

- Do not leave yourself logged in at an unattended machine.

Internet

- Do not seek out inappropriate content or materials which could be offensive to others.
- The College monitors and records internet use for compliance and legal purposes.
- Chat rooms or instant messaging clients are not allowed, except for boarding students in their accomodation.
- Peer-to-peer file sharing or data transfer, VPN, TOR, or Proxy Bypass software are forbidden.
- Hosting internet services on the RIC internet connection is forbidden.

- Internet access is a privilege and must not be abused.

Printing

- Use College printing facilities only for academic work and homework.

- Personal printing requires staff permission and must not be excessive or inappropriate.

Personal Computing Equipment

- The College does not support or accept liability for personal computing equipment.
- Access to the network and internet with personal equipment requires approval and inspection.
- Personal networking equipment is not permitted.

- Do not share the College network or internet connection.

Mobile Devices and Smart Technology

- Year 7-9 students must hand in mobile phones during registration and will have them returned at the end of the day.

- Students must use mobile phones responsibly, following safeguarding and behaviour policies.
- Personal devices are brought to the college at the owner's risk.
- Devices are not permitted in tests or exams.
- The College has the right to search and examine any device suspected of unauthorised use.
- Users should adhere to age limits and terms and conditions for app purchases.
- The non-consensual use of images is not permitted.

Student Behaviour

Students must:

- Treat computing facilities and equipment with respect and report any concerns to a member of staff
- Not log on with anyone else's details.
- Use technology responsibly and appropriately.
- Not use technology to bully, harass, offend, or embarrass others.
- Not post pictures without permission.
- Not contact people they don't know.
- Not share Wi-Fi details.
- Report online bullying or contact from unknown individuals to staff.
- Not plagiarise from the internet.
- Not upload or download illegal or offensive material.

The College will take disciplinary action for breaches, including removing access to computing facilities and/or the internet. Serious or repeated breaches may invoke the college's disciplinary procedures.