



RUGBY SCHOOL

Online Safety Policy

Advent 2026

1. Aims and Objectives

It is the duty of Rugby School to ensure that every student in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning but also pose great risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use Policy (for all staff, visitors and students), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection Policy
- Code of Conduct;
- Discipline and Rewards Policy;
- Data Protection Policy;
- School Trips Policy
- RSE Policy;
- Acceptable Use of AI;
- Images Policy
- Permanent Exclusion and Required Removal Policy (RS)
- Social Media Policy
- Communications Policy School

- Technical Security Policy (including filtering and passwords)
- Standard Terms and Conditions (Parent Contract)
- Counter-Bullying Policy
- The Guidelines for Life at Rugby School

At Rugby School, we understand the responsibility to educate our students on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving students in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- “staff” includes teaching and non-teaching staff, governors, and volunteers;
- “parents” includes students' carers and guardians; and
- “visitors” includes anyone else who comes to the school.

Both this policy, and the Acceptable Use policies, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by students, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In designing this policy, the school has considered the “4Cs” outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that many students will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some students, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by students, in or out of school, will be dealt with under the school’s Discipline and Rewards Policy, the Counter-Bullying Policy and the Safeguarding and Child Protection Policy as is appropriate in the circumstances.

3. Roles and responsibilities in relation to online safety

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Safeguarding and Child Protection Policy.

3.1. The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the DSL (the school's online safety coordinator) and Senior Leadership Team are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

3.2. Head Master and the Senior Leadership Team

The Head Master is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

3.3. The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child protection at Rugby School. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Head Master and Senior Management Team, and IT staff to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL is the online safety coordinator and will work closely with the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that termly checks are properly made of the system.

The DSL will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. The DSL will document and act upon any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system.

3.4. Technical Services Department

The Technical Services Department have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the DSL.

3.5. Teaching and Operational and Administrative staff

All staff are required to sign and return the IT Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL and Senior Management Team as appropriate.

3.6. Students

Students are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy.

3.7. Parents and carers

Rugby School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about students' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

4. Filtering and Monitoring

In general:

Rugby School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements, and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, students, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Code of Conduct or the Discipline and Rewards Policy, as appropriate. Examples of student mis-use and suggested sanctions are listed in The Guidelines.

The DSL, in liaison with the Director of IT Services, will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding governor and the DSL will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content and adult content. Additional content categories may be added to this list as appropriate. If there is a good educational reason why a particular website, application, or form of content should not be blocked a student should contact the IT Helpdesk, who may then contact the DSL for their consideration.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals to be identified. In line with the school's Data Protection Policy, the IT Staff will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the DSL if they are teaching material which might generate unusual internet traffic activity.

Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the DSL or IT Helpdesk if they believe that appropriate teaching materials are being blocked.

Students:

Students must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to their Housemaster or Housemistress (Hm) or the DSL.

Deliberate access to any inappropriate materials by a student will be dealt with under the school's Discipline and Rewards Policy. Students should be aware that all internet usage via the school's systems and its Wi-Fi network are monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, students should contact a member of the IT Helpdesk for assistance.

5. Education and training**5.1. Staff: awareness and training**

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures.

All staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When students use school

computers, staff should make sure children are fully aware of the agreement they are making to follow the Guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

5.2. Students: the teaching of online safety

Online safety guidance will be given to students on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our students' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating students / pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At Rugby School, the school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via the spiral PSHE curriculum and includes interactive theatre productions, lessons with Tutors, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. From F Block, pupils are formally and informally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Online Safety Coordinator and any member of staff at the school.

From F Block, pupils are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Pupils are taught about respecting other people's information and images (etc.)

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding / Counter Bullying / Sanctions Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

5.3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about students' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges seminars for parents when an outside specialist advises about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

6. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff at Rugby School are permitted to bring in personal devices for their own use.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any student nor to have any images, videos or other recording of any student on their personal devices. Please read this in conjunction with Safeguarding and Child Protection, Acceptable Use, Staff Code of Conduct and School Trips policies.

Students

Information on when students may have their mobile phones are found in The Guidelines.

Students are responsible for their conduct when using school issued or their own devices. Any misuse of devices by students will be dealt with under the School's Discipline and Rewards Policy.

The School recognises that mobile devices are sometimes used overnight or at other times by students for medical purposes or as an adjustment to assist students who have disabilities. Where a Middle School student needs to use a mobile device for such purposes, the student's parents or carers should arrange a meeting with the Housemaster / Housemistress (Hm) to agree how the school can appropriately support such use. The Hm will then inform the House team, the student's teachers and other relevant members of staff about how the student will use the device at school.

7. Online Communications

Staff

Any digital communication between staff and students or parents / carers must be professional in tone and content. Under no circumstances may staff contact a student or parent / carer / recent alumni (i.e. students over the age of 18 who have left the school within the past three years or parents of recent alumni using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with students or parents / carers and recent alumni. Under no circumstances may staff contact a student or parent / carer and recent alumni using a personal telephone number, email address, or other messaging system nor should students, parents and recent alumni / their parents / carers be added as social network 'friends' or similar. Staff should refer to the Code of Conduct for further guidance if necessary.

Staff must immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT Staff.

Students

All students are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work. Students should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work purposes, students should contact the IT Helpdesk for assistance.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to their Hm or the DSL.

8. Use of social media

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices or whilst teaching.

When accessed from staff members' own devices / off school premise, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Rugby School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
 - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
 - using social media to bully another individual; or
 - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Code of Conduct or Safeguarding and Child Protection Policy.

Students

The school expects students to think carefully before they post any information online or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by students very seriously and incidents will be dealt with under the Discipline and Rewards, Safeguarding and Child Protection Policy and Counter-Bullying policies as appropriate.

9. Data protection

Please refer to the Data Protection policy and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and students are expected to save all data relating to their work to their school laptop or to the school's central server as per the IT Acceptable Use Policy.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or students should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the school.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the IT team in accordance with the Data Protection Policy and IT Acceptable Use Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Director of IT Services.

10. Password security

Students and staff have individual school network logins, email addresses and storage folders on the server. Staff and students are regularly reminded of the need for password security.

All students and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every 6 months;
- not write passwords down; and
- not share passwords with other students or staff.

11. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the

internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites) and follow the School's Images policy.

12. Artificial Intelligence

Any usage by students of generative AI tools such as ChatGPT is only permitted in the circumstances outlined in the Academic Policy.

In particular, personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.

It may be important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, students should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from the DSL, the Head of Wellbeing or the San team.

Rugby School will evaluate the benefits and risks of any proposed use of generative AI by staff or students, with particular regard to risks associated with safeguarding, data protection and the possibility of bias and discrimination. Any approved use of AI will be kept under review and the School will remain alert to the possibility of unauthorised use.

13. Misuse

Rugby School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Child Protection and Safeguarding and Behaviour policies.

14. Complaints

As with all issues of safety at Rugby School, if a member of staff, a student or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the DSL in the first instance, who will undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection Policy and reported to the school's DSL, in accordance with the school's Safeguarding and Child Protection Policy.

Policy Author: ELS

Date last reviewed by the Governing Body: June 2026

Date of next review by the Governing Body: June 2027

Appendix A

Examples of student incidents are outlined in the below table, along with a possible response. However, each incident will be reviewed on a case-by-case basis and the sanction will be dependent on the seriousness of the offence.

Examples of Student Incidents	Issue a Minor	Issue a behaviour detention	Restriction of technology and network/internet access	Further sanction e.g. gation/rustication/exclusion
Unauthorised use of non-educational sites during lessons	X			
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X			
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device		X		
Unauthorised downloading or uploading of files		X	X	
Deliberately accessing or trying to access material that could be considered illegal (see list in “User Actions” section).				X
Deliberately manipulating media to misrepresent a person or their actions				X
Allowing others to access School network by sharing username and passwords			X	X
Attempting to access or accessing the School network, using another student’s account, or the account of a member of staff.			X	X
Corrupting or destroying the data of other users			X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X	X
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School			X	X
Using proxy sites or other means to subvert the School’s filtering system			X	X
Deliberately accessing or trying to access offensive or pornographic material			X	X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X	X
Sharing (including 'showing') video, photographic or audio recordings of others with the result to humiliate, mock or offend.			X	X
Making covert video or audio recordings or taking photographs of others without their knowledge or consent.			X	X