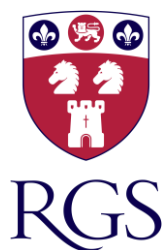


E-SAFETY POLICY



RGS



E-SAFETY POLICY

Newcastle upon Tyne Royal Grammar School

The school recognises that in a digital age it has a duty to ensure that every student is safe in the virtual world. Students use technology in their lives both inside and outside school and whilst this provides huge opportunities for learning, it also poses greater and different risks to young people. We therefore provide a safe online environment within school and teach students about different risks, including bullying, harassment, grooming, identity theft and protection of personal data. We increasingly seek to use technology to deliver exciting and innovative lessons across the curriculum and in doing so seek to demonstrate and educate students in the power, potential and associated responsibilities which come with new technology.

The nature of technological advance means that RGS regularly reviews both its provision of IT and its policies regarding safe use. Specific education for students regarding e-safety is incorporated into PSHE lessons and in other age specific formats e.g. IT lessons in the Junior School and the Computer Science Curriculum in the Senior School. This policy covers both fixed and mobile internet devices provided by the school, as well as all devices owned by students and staff and brought into school, and when students have to work remotely.

RESPONSIBILITIES FOR E-SAFETY

The Deputy Head Pastoral, as the Designated Safeguarding Lead (DSL), has overall responsibility for e-safety issues. In conjunction with the Director of IT Services and the Digital Lead, the Deputy Head Pastoral reviews both the strategic and practical management of e-safety in the school on a continuing basis. This includes making sure that staff are aware of their responsibilities to promote safe IT use in their lessons, procedures if they are concerned about IT misuse, and how to report an e-safety incident.

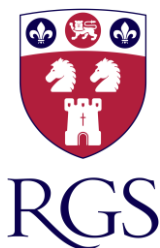
Staff are given updates regarding e-safety as part of their safeguarding briefings during the year.

In line with KCSIE 2021, all new staff will complete e-safety training as part of their induction programme.

The Deputy Head Pastoral will keep a record on CPOMS of e-safety incidents and how they were dealt with. A summary of e-safety incidents and changes in policy is presented to Governors each term as part of the Safeguarding report. In addition, the Deputy Head Pastoral should ensure that staff and students understand that the technology provides additional means for child protection issues to develop through:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyberbullying.

The Director of IT Services has responsibility for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack, and that users may only access the networks and devices through a properly enforced password protection policy. Together with the Deputy Head Pastoral, the Director of IT Services will ensure filtering is fit for purpose and that software such as Smoothwall enables the school to carry out effective monitoring of devices when required. With this in mind, the Director of IT Services and their staff, are also required to keep up-to-date with e-safety technical information in order to carry out effectively their e-safety role and to inform and update others as relevant.



It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that these sites are temporarily removed from the filtered list for the period of study. Any request to do so will be cleared with the Deputy Head Pastoral or Head of the Junior School.

Teaching and support staff are responsible for ensuring that they have an up-to-date awareness of e-safety matters, the current school e-safety policy and practices, and that they have read and understood the **STAFF ACCEPTABLE USE POLICY (AUP)** and the **STAFF BEHAVIOUR POLICY** (staff have confirmed this when they signed their contract of employment). They must report any suspected misuse or problem to the Deputy Head Pastoral or Headmaster. Teaching staff should also promote good e-safety practices in the classroom, for example during research and in the use of software, as part of our whole school approach to safeguarding.

Students are responsible for using the digital technology systems in school in accordance with the **STUDENT ACCEPTABLE USE POLICY**. Each student will sign an acceptable use agreement at the start of each academic year (found in their planner). This makes clear the expectations we have for how they use our IT systems, and how they behave when working online, be that on-site or working remotely.

In addition, students will be taught to understand issues surrounding bullying, plagiarism, use of digital imagery and social media in and outside of school. This is usually, but not exclusively, delivered as part of the PSHE curriculum and IT lessons (in the Junior School). Reflection on specific incidents as part of form or tutor time and in informal conversations with students and parents is also an important part of promoting a whole school approach to e-safety.

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and the school looks for opportunities to help parents understand these issues through parents' evenings, newsletters, letters, the e-safety link on the school website and information about e-safety campaigns. The school encourages parents to share concerns they have about their child's online life, for example gaming and using social media as part of good pastoral care.

UNSUITABLE/INAPPROPRIATE ACTIVITIES

Some internet activity, e.g. accessing child abuse images or distributing racist material, is illegal and is banned from school systems. Other activities, e.g. cyberbullying and harassment, are banned and where allegations are made, investigated in accordance with school policies and reported to the police if it seems that a crime has been committed. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

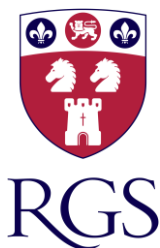
The school uses software to monitor activity which may be of concern on the school system, in addition to appropriate filtering. This covers all Office 365 tools that the students use when working on-site or using them remotely.

In the event of suspicion of serious or criminal IT misuse, for example radicalisation activity, the school will use the following procedure to protect all those involved and to preserve evidence for a subsequent investigation. The investigation will be recorded on CPOMS.

At least two senior members of staff will be nominated to investigate the report; this is most likely to be the Director of IT Services, the Deputy Head Pastoral or Head of the Junior School, but may include other members of the Senior Leadership Team (SLT).

A designated computer will be allocated that will not be used by young people and, if necessary, can be taken off site by the police should the need arise. The same computer will be used for all aspects of the investigation. All sites and content visited are closely monitored and recorded.

The URL of any site containing the alleged misuse will be recorded, as will the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.



Once this has been completed and fully investigated, the Deputy Head Pastoral, Director of IT Services and Head will judge whether the concern has substance or not. If it does, then appropriate action will be required in line with the RGS [BEHAVIOUR, REWARDS AND SANCTIONS POLICY](#), [SERIOUS DISCIPLINARY ISSUES GUIDANCE](#) and [MANAGING ALLEGATIONS POLICY](#).

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of *grooming* behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material or any act regarded as a hate crime
- Other criminal activity or materials.

In this situation the computer used to investigate the concern will be isolated pending advice from the police.

USE OF SCHOOL AND PERSONAL DEVICES

Staff using either their own or a school device as part of their school role must have a password or device lock so that unauthorised people cannot access the content, and when the device is not being used they must make sure it is locked to prevent unauthorised access. Staff are permitted to use mobile phones during the school day, but are reminded that professional conduct would assume that they would not take personal calls or read messages whilst they were teaching. The [STAFF BEHAVIOUR POLICY](#) makes clear that staff should not share their personal numbers or personal contact details with students or parents (except in circumstances cleared by a member of the SLT) and they should not communicate with students via social media, unless in monitored groups.

The school has a [BRING YOUR OWN DEVICE \(BYOD\) POLICY](#) and students are encouraged to use their own devices as appropriate in lessons. In the Junior School, mobile phones are required to be switched off and handed to a Form Teacher each morning. In the Senior School, students are allowed to keep their phones and devices with them but they must be switched to silent and stored out of sight from the start of morning registration until 4pm, unless a teacher has given permission for phones or devices to be used. The Sixth Form are allowed to use their phones and devices in the Sixth Form Common Room. Mobile phones and devices that are visible between those times will be confiscated for the remainder of the school day. A record is kept of confiscated phones/devices and when a phone/device is confiscated for the third time, parents are asked to come into school to take the phone/device away. Mobile phones and devices remain the responsibility of the child throughout the school day. Bringing mobile devices into school is a privilege not a right, and this privilege may be removed at the school's discretion. It is stated clearly in the student acceptable use policy that VPNs are not permitted to be used in school.

USE OF INTERNET AND EMAIL

There is strong anti-virus and firewall protection on the school network and therefore the network can be regarded as safe and secure. Sometimes the protection will block legitimate sites and staff should contact the IT Department to request a site to be unblocked. Staff should also be aware that attempting to access blocked sites will be recorded on the school systems and that email can also be monitored.

Staff and students are not restricted in their personal use of the IT system, but are expected to adhere to the [ACCEPTABLE USE POLICY](#) and staff should not undertake personal web browsing



whilst supervising or teaching a class.

Staff must immediately report to the Deputy Head Pastoral the receipt of any communications that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature. They should not respond to any such communication.

Students are also encouraged to report similar incidences to a member of teaching staff and to retain screen shots of the relevant and related material to help with investigation.

Any online communications (including posting or sharing links) must not either knowingly or recklessly:

- Place a child or young person at risk of harm
- Bring the School into disrepute
- Breach confidentiality
- Breach copyright
- Breach data protection legislation
- Do anything that could be considered discriminatory.

DATA STORAGE

In accordance with our [PRIVACY NOTICE](#) and [ACCEPTABLE USE POLICY](#), staff should not store personal data on unsecured devices or data storage solutions, for example memory sticks, phones or the cloud.

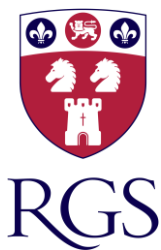
The school provides secure access to documents and data through Office 365, iSAMS, CPOMS and Foldr.

STORAGE OF DIGITAL IMAGES

Whilst there are many benefits to the development of digital imaging technologies, there are also specific dangers as a result of publishing digital images on the internet because they provide opportunities for cyberbullying, stalking or grooming to take place. The school's role is to educate students, staff and parents to be vigilant and to consider these possibilities before they publish their images electronically. The school asks parents or students (if in the Sixth Form) to consent to the use of photographs in certain circumstances, and students are given age appropriate guidance regarding the posting of images.

Staff who take pictures of students for educational purposes should do so within the rules of the [ACCEPTABLE USE POLICY](#), [STAFF BEHAVIOUR POLICY](#) and [PHOTOGRAPHY IN SCHOOL POLICY](#), and take care to ensure students are appropriately dressed. Staff should not keep digital images of students on their own devices, instead downloading any pictures taken of school activities or events to the School One Drive. Where they have a particular reason to keep a record of an activity or event (for example, pictures of a team, play or concert with particularly strong memories or associations for them), they should:

- Ensure they are uploaded to the School One Drive.
- Inform either the Headmaster or the Deputy Head Pastoral what they are intending to keep and why – this should be in the form of an email.
- Label the photo clearly in order to supply an unequivocal context and (for their own protection) to ensure that their purpose in saving images cannot be misconstrued.
- Ensure that their own device is clear of any school-related content – to include in



the *downloads* section of their own devices.

See also:

- ACCEPTABLE USE POLICIES (staff and students)
- SAFEGUARDING POLICY
- STAFF BEHAVIOUR POLICY
- MANAGING ALLEGATIONS POLICY
- ANTI-BULLYING POLICY
- ANTI-CYBERBULLYING POLICY
- BEHAVIOUR, REWARDS AND SANCTIONS POLICY
- BYOD POLICY
- PRIVACY NOTICE
- PSHE POLICY (SENIOR AND JUNIOR)
- ONLINE SAFETY POLICY (JUNIOR SCHOOL)
- COMPUTING POLICY (JUNIOR SCHOOL)

CONTACT DETAILS

Royal Grammar School, Eskdale Terrace, Newcastle upon Tyne NE2 4DX

Tel: 0191 281 5711

General enquiries: hm@rgs.newcastle.sch.uk
or communications@rgs.newcastle.sch.uk

www.rgs.newcastle.sch.uk