Newcastle upon Tyne Royal Grammar School

E-safety Policy

This policy applies to the whole school and is published to parents

Updated June 2015 **Author: S Baillie**

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 the 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. 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.

See also:

- Acceptable Use Policies (staff and students)
- Safeguarding Policy
- Safeguarding Code of Conduct
- Procedure for reporting a concern about an adult working at the school
- Anti-bullying policy
- Anti-cyber bullying Policy
- Behaviour and Sanctions Policy
- BYOD Policy
- Data Protection Policy
- PSHE Scheme of Work and PDS scheme of work in the Junior School
- Junior School e-safety Policy
- Computing – Junior School Policy
- Junior School Mobile Phone Contract

Responsibilities for E-safety

The Pastoral Director as the Designated Safeguarding Lead (DSL) has overall responsibility for e-safety issues. In conjunction with the Director of IT Services the Pastoral Director 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.

The Pastoral Director will keep a record 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 Pastoral Director 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 on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

The IT Director 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 Pastoral Director the Director of IT Services will ensure filtering is fit for purpose and that Mobile Device Management (MDM) enables

the school to carry out effective monitoring of devices when required. With this in mind, the IT Director and his 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 those sites are temporarily removed from the filtered list for the period of study. Any request to do so will be cleared with the Pastoral Director 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 Safeguarding Code of Conduct (staff have confirmed this when they signed their contract of employment). They must report any suspected misuse or problem to the Pastoral Director or Headmaster. Teaching staff should also promote good e-safety practices in the classroom, for example during research and in the use of software.

Students are responsible for using the digital technology systems in school in accordance with the Student Acceptable Use Policy. 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 look for opportunities to help parents understand these issues through parents' evenings, newsletters, letters, 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. cyber-bullying 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.

In the event of suspicion of 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 using the whole school incident report sheet.

At least two senior members of staff will be nominated to investigate the report; this is most likely to be the IT Director, the Pastoral Director 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 Pastoral Director, IT Director 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 Rewards and Sanctions policy and Procedure for Reporting Concerns about an Adult Working with Children.

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
- 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 us 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 Safeguarding Code of Conduct makes clear that staff should not share their personal numbers with students or parents (except in circumstances cleared by a member of 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 with them but they must be at least switched to silent and stored out of sight during lessons unless a teacher has given permission for phones to be used. Mobile phones which "go off" in lessons will usually be confiscated for the remainder of the school day. Mobile phones remain the responsibility of the child throughout the school day.

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 Pastoral Director or the e-safety manager 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 Data Protection Policy and Acceptable Use Policy staff should not store personal data on unsecured devices or data storage solutions, for example memory sticks. Memory sticks should only be used for the storage of non-confidential material such as worksheets and presentations. Student reports, assessments and personal information should be accessed via secure links such as Citrix and iSAMS.

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 to consent to the use of photographs of their children 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 and take care to ensure students are appropriately dressed. Staff should not routinely keep digital images of students on their own devices, instead downloading any pictures taken of school activities or events onto the school server (usually the central N-drive folder Event Photos). 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 onto the school server;

•inform either the Bursar or the Designated Safeguarding Lead (Pastoral Director) what they are keeping and why - this should at least be in the form of an email, but is likely to start with a conversation; and

•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.