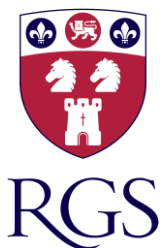




ONLINE SAFETY POLICY JUNIOR SCHOOL



RGS



ONLINE SAFETY POLICY

Newcastle upon Tyne Royal Grammar School

INTRODUCTION

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. Computing lessons in the Junior School. However at the RGS, online safety is a whole school issue and as such will be addressed across the curriculum.

See also:

- E-Safety Policy
- Acceptable Use Policies (staff and students)
- Student Mobile Device Load Agreement
- Safeguarding Policy
- Staff Code
- Mobile Phone Policy
- Managing Allegations Policy
- Anti-bullying Policy
- Anti-cyberbullying Policy
- Behaviour, Rewards and Sanctions policy
- BYOD policy
- Privacy notice
- Acceptable use policies (for staff and students)
- PSHE (including RSE) Policy and PSHE (including RSE) scheme of work in the Junior School
- Computing Policy (Junior School)

WHAT IS ONLINE SAFETY?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the *duty of care* which applies to everyone working with children.

This policy applies to all members of the *school* community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the *School*.

RESPONSIBILITIES

RGS aims to operate in accordance with KCSIE 2024, Filtering and Monitoring Standards for schools and the government recommendations about cyber security.

Our Governors are required to understand the potential harms and risks to our students from the online world, and to consider the number of and age range of our students and those who are potentially at greater risk of harm. The Safeguarding Governor and the DSL will be responsible for ensuring these standards are met.

The Deputy Head Pastoral, as the Designated Safeguarding Lead (DSL), has overall

This policy applies to the Junior school and is published to parents, students and staff

Version: 02 Updated: July 2023 Reviewed: September 2024 Author: R Towers

responsibility for e-safety issues, and ensuring we have appropriate filtering and monitoring on school devices and networks. In conjunction with the Head of Digital Strategy, 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, how our filtering and monitoring systems work and their duties in relation to it, 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 2024, all new staff will complete e-safety training as part of their induction programme, and staff will receive e-safety training each year.

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 Head of Digital Strategy 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 Head of Digital Strategy will ensure filtering is fit for purpose and that software such as Smoothwall and SENSO filtering and monitoring enables the school to carry out effective filtering and monitoring of devices when required. With this in mind, the Head of Digital Strategy 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. Regular review and testing of the filtering and monitoring tools and settings should be carried out, ideally termly, and reported to the governors via the termly Safeguarding Report from the DSL.

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 CODE (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. 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, social media and appropriate use of AI 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

This policy applies to the Junior school and is published to parents, students and staff

Version: 02 Updated: July 2023 Reviewed: September 2024 Author: R Towers

parents understand these issues through parents' evenings, newsletters, letters, the e-safety link on the school website and information about e-safety campaigns. For parents of Y3-6, the school has a subscription to The National College : Wake Up Wednesday guides, which offers a range of information guides and practical skills to be able to have informed and age-appropriate conversations with children about online safety, mental health and wellbeing and climate change. Formerly delivered by National Online Safety, these guides now address wider topics and themes. Advice for parents through webinars, resources and Q&A sessions, on topics that relate to e-safety and digital wellbeing. 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 Smoothwall and Senso software to monitor activity which may be of concern on the school system or school-issued devices, 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 Head of Digital Strategy, 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, Head of Digital Strategy 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 or exploitation of a child
- 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 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 CODE 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.

Our students will be using a school-issued device and will complete a Student Mobile Device Loan Agreement plus an Acceptable Use Policy which gives clear parameters on how they are expected and required to use their devices at anytime (including beyond school-hours). The school also has a BRING YOUR OWN DEVICE (BYOD) POLICY. School cannot monitor or filter what students access via their personal devices using 4G/5G. It is stated clearly in the student acceptable use policy that VPNs are not permitted to be used in school. In the Junior School, mobile phones are required to be switched off and handed to a Form Teacher each morning. In the Senior School, student must comply with the Mobile Phone Policy which clearly lays out our expectations of personal device use (including smart watches/devices), exemption criteria, and also the sanctions for mobile/device use. Bringing mobile devices into school is a privilege not a right, and this privilege may be removed at the school's discretion.

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 IDT 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 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 or phones.

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

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 CODE and PHOTOGRAPHY IN SCHOOL POLICY, and take care to ensure students are appropriately dressed. Staff should not keep digital images of s

students on their own devices, instead downloading any pictures 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 on their own devices, instead of downloading an 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.

STUDENTS

The School is committed to educating its students as responsible digital citizens, prepared to embrace the developing technological world with skill and awareness for their own safety. To this end, students are given guidance so they are responsible for using the school computing systems in accordance with Rules for responsible use of iPads, computers and the internet (*Acceptable Use Policy*), which they will be expected to sign before being given access to school systems. There will be a separate Acceptable Use Policy (AUP) which includes Microsoft 365 and other online applications. This is signed for by pupils and regularly discussed in computing lessons. In addition;

- They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They are expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices.
- They should also know and understand school policies on the taking/use of images and on cyber bullying.
- They understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety policy covers their actions out of school, if related to their membership of the school.

Computing and RSE -Curriculum Coverage

Primary

Online relationships

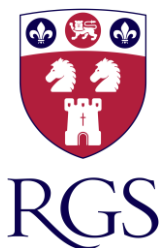
Pupils should know:

- that people sometimes behave differently online, including by pretending to be someone they are not
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- how information and data is shared and used online

Being safe

Pupils should know:

- what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- about the concept of privacy and the implications of it for both children and adults; including that it is not always right to keep secrets if they relate to being safe
- that each person's body belongs to them, and the differences between appropriate and inappropriate or unsafe physical, and other, contact
- how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- how to recognise and report feelings of being unsafe or feeling bad about any adult
- how to ask for advice or help for themselves or others, and to keep trying until they are heard,
- how to report concerns or abuse, and the vocabulary and confidence needed to do so
- where to get advice, for example family, school or other sources



Each year, the students observe Internet Safety Day which takes place in February. In addition, there are Online Safety assemblies and reminders of key online safety messages in both the computing and PSHE curriculum.

PARENTS/CARERS

Parents/carers play a crucial role in ensuring their children understand the need to use the internet/mobile devices in an appropriate way. The School looks for opportunities to help parents understand these issues through parents' evenings, newsletters, letters, the website and information about national and local 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. Every year, the Junior School hosts a dedicated e-safety parents' evening. Those unable to attend will be sent the information as part of the Junior School bulletin and through email. As a part of the digital schools membership, parents receive regular online safety updates via the RGS website, as well as parental guides. In addition, parents can access free parenting courses via the National College website.

Every year, Junior School parents receive a *Sharing the curriculum guide which contains the computing* which explains the e-safety topics being covered throughout the Junior School. This understanding is then built upon in PSHE lessons in the Junior School and in lessons in the Senior School.

Parents and carers are encouraged to support the School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events;
- Access to the parents' sections of the website;
- Their children's personal devices in the School.

Parents and carers have access to additional help throughout the year via the Digital Schools Membership.

COMMUNITY USERS, VOLUNTEERS & SUPPLY STAFF

Users who access school computing systems/website as part of the extended school provision, as a volunteer or supply staff, will be expected to sign the agreement regarding use of IT Resources by visitors before being provided with access to school systems.

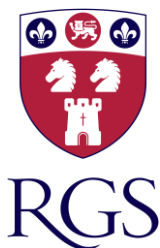
WHY IS E-SAFETY IMPORTANT

While regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the School to recognise and avoid online safety risks and build their resilience.

The School uses a number of approaches to support the school community to stay safe online.

NATIONAL COLLEGE MEMBERSHIP

As part of our ongoing commitment to keeping children safe; promoting digital resilience and



keeping the whole school community regularly informed of the latest developments in online safety, the RGS is a National College Member (formerly National Online Safety). This membership provides: regularly updated online safety messages (accessed via the RGS website and through the Junior School bulletin); curriculum resources and advice. It is constantly updated to reflect the ever changing digital world.

360 DEGREE SAFE ONLINE SAFETY SELF REVIEW TOOL



As a school we use the 360 degree safe an online, interactive self-review tool which allows schools to review their online safety policy and practice, to ensure that we constantly review our online safety provision for the whole community.

SWGFL DIGITAL LITERACY & CITIZENSHIP

At RGS, we use a variety of schemes to help teach students digital literacy and citizenship skills. SWGFL schemes of learning are based on Common Sense Media's digital literacy and citizenship curriculum, which empowers learners to think critically, behave safely, and participate responsibly in our digital world. These 21st-century skills are essential for children and young people to harness the full potential of technology for learning.

EDUCATION FOR A CONNECTED WORLD A FRAMEWORK TO EQUIP CHILDREN & YOUNG PEOPLE FOR A DIGITAL LIFE

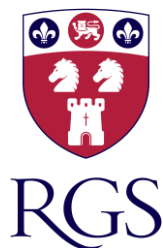
Education for a Connected World is a tool which enables the development of teaching and learning as well as guidance to support children and young people to live knowledgeably, responsibly and safely in a digital world.

It focuses specifically on eight different aspects of online education:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

The framework aims to support and broaden the provision of online safety education, so that it is empowering, builds resilience and effects positive culture change. The objectives promote the development of safe and appropriate long term behaviours and supports educators in shaping the culture within their setting and beyond.

WHY IS INTERNET USE IMPORTANT?



The rapid developments in electronic communications are having many effects on society.

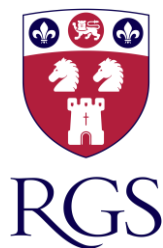
- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The internet is a part of everyday life for education, business and social interaction.
- The School has a duty to provide students with quality internet access as part of their learning experience.
- Students use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.
- The purpose of internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

HOW DOES INTERNET USE BENEFIT EDUCATION?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the internet including increased student attainment.

Benefits of using the internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between students worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for students and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with Northumberland County Council and DfE;
- Access to learning wherever and whenever convenient



APPENDIX A

HOW CAN THE INTERNET USE ENHANCED LEARNING?

The school's internet access is designed to enhance and extend education.

- Students are taught what internet use is acceptable and what is not, and given clear objectives for internet use.
- The school ensures that the copying and subsequent use of internet-derived materials by staff and students complies with copyright law.
- Access levels to the internet is reviewed to reflect the curriculum requirements and the age and ability of students.
- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and ability.
- Students are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students are taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

HOW WILL STUDENTS LEARN HOW TO EVALUATE INTERNET CONTENT?

- Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. This is taught as part of the discrete digital literacy and citizenship lessons within computing lessons, as well as part of certain computing lessons throughout the year.
- Students use age-appropriate tools to research internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and is viewed as a whole-school requirement across the curriculum.

HOW WILL CYBERBULLYING BE MANAGED?

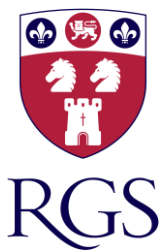
Cyberbullying can be defined as: *"The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone"* DCSF 2007.

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policies on anti-bullying and anti-cyberbullying.

There are clear procedures in place to support anyone in the school community affected by cyberbullying.

Junior School students are taught what cyberbullying means and how to report it. DfE and Childnet resources and guidance are used to give students practical advice and guidance on cyberbullying: www.digizen.org/cyberbullying.

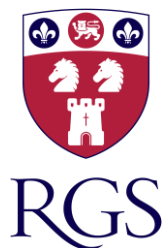
Students start in Year 3 by looking at the adventures of Kara, Winston and the Smart Crew, and are introduced to the SMART rules, which reinforce simple rules that they must abide by in order to keep themselves safe online. These SMART rules posters are displayed in all



rooms around the Junior School and are referred to throughout the year and throughout the year groups. The rules are displayed in each student's planner. These resources are used in both computing and PHSE lessons.

In addition, discrete lessons dedicated to cyberbullying are taught throughout the Junior School using the SWGFL Digital Literacy and Citizenship lesson plans as well as lessons from Education For A Connected World, Cyber First and Natterhub.

In the Senior School, PSHE and RSE lessons continue to build on the anti-bullying message and further opportunities in assemblies and presentations help to embed the messages.



APPENDIX B

JUNIOR SCHOOL DOCUMENTS

ACCEPTABLE USE POLICY (AUP) JUNIOR SCHOOL

All users are responsible for good behaviour when using the school's equipment, network, email, internet and when using Office 365. All pupils are given access to these to support their work; email and Microsoft Teams is provided to allow appropriate communication with others. Please remember that access is a privilege, not a right, and that access requires responsibility. It is your responsibility to follow this AUP (Acceptable Use Policy). Misuse of the AUP may result in suspension of network access or other information service privileges, and possible disciplinary action.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my personal safety:

- I understand that what I do online will be supervised and monitored and that I will not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share them with anyone else and never allow anyone else to use them.
- I will only use my own login and password when using a computer, unless sharing a computer under direct instructions from a member of staff.
- I will use my school email for school purposes.
- I will only use my Office 365 account for school work.
- I will be aware of "stranger danger" when I am online.
- I will not share personal information about myself or others when online.
- I will not create Teams without the permission and inclusion of a supervising member of staff. The school withholds the right to remove any groups it deems unsuitable or offensive.
- I will not use social media in school unless as part of a lesson under direct instruction from a member of staff.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to a teacher.
- I will report any suspicious emails immediately to a teacher.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission. I will use technology sensibly and with respect.
- I will use (where possible) the Surface Go/ iPad I have been assigned to
- I will not alter the settings on any devices.
- I will not try to install any software, applications or programs.
- I will tell an adult if a device is damaged or is not working correctly.
- I will only use the devices to do things that I am allowed to do. I am not allowed for example to use it for online gaming etc.
- I will respect others, and not touch another person's device while they are using it (including the power button, screen, keyboard, digital pen, headphones and mouse).
- I will not use any device to record, video or take photographs of any member of the school community without explicit permission from a member of staff.
- I will only use software and applications my teacher has asked me to use.
- I will only download files (e.g. Micro:bit files) when asked to do by a teacher.
- I will not use computing resources for any form of illegal activity, including, but not limited to, software and music piracy (downloading and listening to music that you have not paid for).
- I will not use Virtual Private Networks (VPNs) to access the school network.
- I will always logout of school devices after use.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me. I will be polite.
- I will make sure that all my communication with everyone is responsible, sensible and polite.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- Where work is protected by copyright, I will not try to download copies (including music and videos).
- I will observe copyright laws and acknowledge sources of information. This means do not copy text from the internet (put it in your own words) and do not add images that are protected by copyright to your work.
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions.

If there is anything in the above policy that you do not understand, please seek clarification from your Computing teacher.

I understand that my use of computing resources including internet, Office 365 and school email will be automatically logged, including using keylogging software, and that the record of my use may be examined from time to time, and without notice, to ensure that I am making proper use of these resources and for the safeguarding of all members of the school community.

I also understand that any data storage space provided belongs to the school and that this may also be examined from time to time, and without notice, and inappropriate data deleted and reported.

This policy applies to all school-owned computing devices (desktop PCs, laptops, iPads, Surface devices), any device which is used to access the school network (including personal devices using Wi-Fi) and any other personal device in use on-site during the school day. You will be required to agree to this policy at the beginning of each academic year. Your form supervisor, class teacher (Junior School) or Computing teacher will explain how to do this.

WHAT IF THINGS GO WRONG?

If I misbehave or make a poor choice:

You must immediately report your error to your teacher who will deal with the issue.

If someone's behaviour online upsets me:

You must report this to whoever you feel most comfortable sharing this with: a teacher, Head of Pastoral (Mrs Wall), parent, or another responsible adult.

Try to keep a copy or screen shot of any communications that made you feel uncomfortable, was offensive, discriminatory, threatening or bullying in nature.

SANCTIONS RELATING TO USE OF TECHNOLOGY AND DEVICES:

Any breaches of the AUP and the Student Behaviour Policy could lead to any of the usual sanctions to be applied. (see our Rewards & Sanctions Policy and Child Friendly Sanctions Technology)

Click [here](#) to complete the acceptance form. By submitting the form you agreeing to adhere to the terms and conditions set out in the policy above.

Simpler version to use with younger Junior School pupils.

The school has iPads, computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will use only my own login and password when using a computer;
- I will use the computers only for schoolwork and homework;
- I will only use my school email and Office 365 account;
- I will ask permission from a member of staff before using the Internet;
- I will only e-mail and Teams message people a teacher has approved;
- The messages I send will be polite and sensible;
- I will not give my home address or phone number;

- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive a message I do not like;
- I understand that the school can check my computer files and the Internet sites I visit.
- I will take great care with all Computing equipment and report any damage immediately to my teacher.
- I will always log out of school devices after use.
- I know that if I break the rules I might not be allowed to use a desktop PC/ Surface Go or iPad.

iPad Specific rules

- I will not access other people's files on the iPads;
- I will always hold the iPad with two hands;
- I will always keep food and drink away from the iPads;
- I will remember to turn off my iPad screen when the teacher is talking;
- I will only use the apps my teacher has given me permission to use.

The above agreement is found in all Junior School Computing Teams.

WHAT IF THINGS GO WRONG?

If I misbehave or make a poor choice:

You must immediately report your error to your teacher who will deal with the issue.

If someone's behaviour online upsets me:

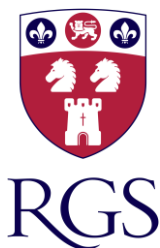
You must report this to whoever you feel most comfortable sharing this with: a teacher, Head of Pastoral (Mrs Wall), parent, or another responsible adult.

Try to keep a copy or screen shot of any communications that made you feel uncomfortable, was offensive, discriminatory, threatening or bullying in nature.

SANCTIONS RELATING TO USE OF TECHNOLOGY AND DEVICES:

Any breaches of the AUP and the Student Behaviour Policy could lead to any of the usual sanctions to be applied. (see our Rewards & Sanctions Policy and Child Friendly Sanctions Technology)

In Junior School computing lessons, you will be given a link to a Form to complete the acceptance form. By submitting the form you agreeing to follow the rules stated in this policy.



RULES FOR BLOGGING

Blogging is great fun, and an amazing way to share our ideas and what we're learning with other people. But to make sure that Our Blog is fun AND safe, we need to **FOLLOW THE BBG (BASIC BLOG GUIDELINES)**:

- **ONLY USE FIRST NAMES** when blogging or commenting. All student work will also be referred to by first names only.
- **DO NOT PROVIDE ANY PERSONAL DETAILS** in a post or comment, such as address or family information.
- Parents and others related to students should also refrain from using full names. Please just use first names, or maybe just go with *Steven's Mum*, or *Lucy's Grandad*!
- **ALWAYS WRITE IN FULL SENTENCES**, think about spelling and punctuation.
- **SHOULD THE AWESOME ABILITY TO WRITE OUR OWN BLOG POSTS BE ABUSED**, or the BBGs not be followed in any way, **WE WILL HAVE TO TAKE AWAY THOSE PRIVILEGES**. But I'm sure that won't have to happen!
- Remember to **COMMENT ON OTHER PEOPLE'S POSTS**. See commenting guidelines for how to do this, and to get ideas on good commenting protocol.
- Our blog is a public space, with other people looking at our work, so **ALWAYS BE PROUD OF WHAT YOU'VE WRITTEN OR COMMENTED**.

Parent/carer's permission

I give permission for my child to write blogs for the school website as set out in the above rules.

Signed: _____

Print name: _____

Student's agreement

I agree to follow the Rules for Blogging

Signed: _____

Print name: _____

Class: _____



The poster above can be found in all the Junior School planners and is located in all classrooms (similar version in Senior School).

Parents Online Safety

You will be aware the Internet hosts many exciting opportunities for education. The online world is a wonderful place for young people to explore, with unprecedented opportunities for learning and creativity, but just like the real world there are risks and dangers they should be aware of and which we should all act to protect them from. As a school we encourage the use of technology as an important part of your child's development but always want them to spend their time online safely. As a parent/carer you can play a significant part in ensuring this.

Top Tips for Parents:

1. Talk to your child, early and often
2. Explore the online world together
3. Know who your child is talking to online
4. Set rules and boundaries
5. Make sure content is age-appropriate
6. Use parental controls to filter, restrict, monitor and report content
7. Teach your child how to use privacy settings and reporting tools



Gaming Advice

PEGI (Pan-European Game Information)
www.pegi.info

Common Sense Media
www.commonsensemedia.org/game-reviews

Family Gamer TV (YouTube Channel)
<https://www.youtube.com/user/familygamertv>

- Use a gaming name
- Take regular breaks
- Lifestyle balance
- Get involved
- Use parental controls
- Where is device situated
- Reporting/Blocking
- Age rating/content descriptor
- Online element?
- Communication?
- Commerce?



Social Networking Advice

See websites on reverse...

Worth a watch:

The Social Dilemma
[Netflix](#)

The Instagram Effect
[BBC iPlayer](#)

- Minimum age 13+ years
- Sharing personal information
- Digital footprint
- Cyberbullying and grooming
- Live streaming dangers
- Instagram and Snapchat likely to inspire feelings of inadequacy.
- 7 in 10 Instagram users feel worse about their body image



Mobile Phones

UK Safer Internet Centre

<https://saferinternet.org.uk/guide-and-resource/parents-and-carers/phones>

- Is the phone registered as child user?
- Are geotagging/location services disabled?
- Is the phone Bluetooth enabled and visible?
- Use the parental controls
- Does the provider offer data capping?
- Beware when using public Wi-Fi

Password Manager apps



SecureSafe

(free to manage up to 50 passwords)



Dashlane Password Manager

(free to manage up to 50 passwords)

- Mix of letters, numbers, symbols
- Use a pass phrase not a password
- Do not reuse same password

Have I Been Pwned?

haveibeenpwned.com

Advice & Guidance

Internet Matters

www.internetmatters.org
LITTLE DIGITAL HELPS TOOLKIT



Childline

www.childline.org.uk

Childnet

www.childnet.com/parents-and-carers

Net Aware

www.net-aware.org.uk

Parent Zone

parentzone.org.uk

BBC Action Line

www.bbc.co.uk/actionline

CEOP (report Grooming)

www.thinkuknow.co.uk/parents

NSPCC (Cyberbullying advice)

www.nspcc.org.uk/keeping-children-safe

Anti-Bullying Alliance (Cyberbullying advice)

anti-bullyingalliance.org.uk

Young Minds (Mental Health support)

www.youngminds.org.uk

Family Lives (Wellbeing support)

www.familylives.org.uk



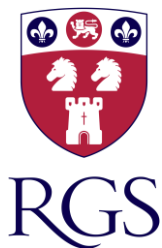
Parents/Carers Checklist

- ☐ I have enabled parental controls on my child's devices
- ☐ I know what games and websites my child uses
- ☐ My child plays age-appropriate games
- ☐ I know which social networking sites my child uses
- ☐ I know who my child talks to online
- ☐ I use different, strong passwords for different sites
- ☐ We have agreed family rules (eg online conduct, down time, contacts etc)
- ☐ I know where to get support and report any concerns
- ☐ My child knows how to report concerns and where to get additional support

Need to Report?

1. Report in online service
2. Contact school
3. NSPCC (ChildLine)
4. CEOP (Grooming)
5. Internet Watch Foundation (Illegal Content)





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