Newcastle upon Tyne Royal Grammar School

Junior School E-safety Policy

This policy applies to the Junior School and is published to parents and staff

Updated September 2015 **Author: Rachel Towers**

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.

See also:
- ☐ 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
- ☐ Acceptable Use Policies (staff and students)
- ☐ PSHE Scheme of Work and PDS scheme of work in the Junior School
- ☐ E-safety Policy
- ☐ Computing – Junior School Policy
- ☐ Junior School Mobile Phone Contract

What is e-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.

E-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.

•The e–Safety Policy and its implementation is reviewed annually.
•Our e–Safety Policy has been written by the school, building on e–Safety Policy and government guidance.
•Our School Policy has been agreed by the Senior Leadership Team and approved by governors

WHY IS E-SAFETY IMPORTANT?

Teaching and learning

Activities involving the internet and communications technologies might have been a rarity a few years ago, they are now common place. Coupled with this, pupils have access to these technologies outside of school and potentially through a range of locations; home, libraries, free wifi sites and also through a variety of technologies ranging from mobile phones to portable games machines.

The use of technology also brings many learning benefits and so risks need to be balanced up with the opportunities technology offers, and moderated by the careful and rigorous application of safety measures by schools. All users, be they children or adults are given a clear understanding of what the risks and dangers are, and how these can be safely managed.

Becta in 'Safeguarding Children in a Digital World' comment:
'While it is clear that technology offers children unprecedented opportunities to learn, communicate, create, discover and be entertained in a virtual environment, there are some inherent risks. And whilst most children's confidence and competence in using the technologies is high, their knowledge and understanding of the risks may be low.'

It is this challenge we need to tackle at Ponteland Community Middle School. Our aim is to ensure that pupils are not just safe in school, but are prepared for the outside world and the use of these technologies in the home and community.

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.
•Pupils 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 pupil 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 pupil 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 pupils worldwide;
●vocational, social and leisure use in libraries, clubs and at home;
●access to experts in many fields for pupils 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.

How can Internet use enhance learning?

●The school's Internet access is designed to enhance and extend education.
●Pupils 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 pupils complies with copyright law.
●Access levels to the internet is reviewed to reflect the curriculum requirements and the age and ability of pupils.
●Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
●Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
●Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

●Pupils 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.
●Pupils 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.

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

At the Royal Grammar School Junior School pupils are taught what cyberbullying means and how to report it. DfE and Childnet resources and guidance are used to give pupils practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying. The pupils 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 on line. 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 pupil'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.
Year 3: Screen out the mean
Year 4: The Power of Words
Year 5: Digital Citizenship Pledge
Year 6: What's Cyberbullying?

- 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 policy on anti-bullying, anti cyber-bullying and behaviour and sanctions.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.

1. Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. E-safety forms one aspect of their termly safeguarding discussions.

Designated Safeguarding Lead (DSL)

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, of the current school e-safety policy and practices and they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) and the Safeguarding Code of Conduct. They must report any suspected misuse or problem to the Pastoral Director or Headmaster. They 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 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.

SWGfL BOOST includes access to Whisper, an anonymous reporting app that installs onto a school website and extends the school's ability to capture reports from staff, children and parents(http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper).

Co-ordinator for investigation/action/sanction

- digital communications with students / pupils (email / Virtual Learning Environment) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- 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.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• will be 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.
• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Each year the pupils' observe Internet Safety Day which takes place in February.

Parents / carers:
Parents / carers play a crucial role in ensuring that 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, website and information about national and local e-safety campaigns. Every year the Junior School hosts a dedicated e-safety parents' evening in the autumn term. Those unable to attend will be sent the information as part of the Junior School bulletin and through e-mail.

Parents and carers will be responsible for:
•endorsing (by signature) the Rules for Responsible Use of iPads, computers and the Internet (Acceptable Use Policy) in student planners and the Rules for Blogging;
•signing the RGS standard terms and conditions;
• accessing the school website / VLE / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Every year the parents receive a Programme of Study for 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.

Community Users, Volunteers and 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.

2. E-Safety Checklist

Action	Completed by:
The Acceptable Use Policy is in place and has been revised to accommodate any developments in technology and its use.	
Governors know that all staff (teaching and non-teaching) and any volunteers or supply staff are familiar with the current e-safety policy and the Acceptable Use Policy.	
e-safety forms part of the induction of all new staff	
Governors know that all new parents/carers have received a copy of the school's AUA.	
Governors know that all parents/carers have signed a copy of the internet access permission form in the child's planner.	
All staff (teaching and non-teaching) and any volunteers or supply staff are in possession of the Levels of E-Safety Infringement (Junior School) to know what to do if an incident occurs.	
All users are compliant with additional AUA's and Terms and conditions contained	

in other services (such as BYOD) and procedures are in place to ensure this happens.	
All users understand the use of e-safety monitoring software where installed.	

Chair of Governing Body:

_____ Date:
(signature)

3. Unsuitable / Inappropriate / Illegal activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and those users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

	Acceptable	Acceptable at times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
child sexual abuse images					**X**
promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation					**X**
adult material that potentially breaches the Obscene Publications Act in the UK					**X**
criminally racist material in UK					**X**
pornography				**X**	
promotion of any kind of discrimination				**X**	
promotion of racial or religious hatred				**X**	
threatening behaviour, including promotion of physical violence or mental harm				**X**	
any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute				**X**	
using school systems to run a private business				**X**	

use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Newcastle upon Tyne LEA and /or Royal Grammar School Newcastle				**X**	
	Acceptable	**Acceptable at times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable and illegal**
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				**X**	
Revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, computer / network access codes and passwords)				**X**	
Creating or propagating computer viruses or other harmful files				**X**	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				**X**	
On-line gaming (educational)		**X**			
On-line gaming (non educational)				**X**	
On-line gambling				**X**	
On-line shopping / commerce				**X**	
File sharing				**X**	
Use of social networking sites apart from Merlin e.g. Bebo, Facebook for older users				**X**	
Use of video broadcasting e.g. Youtube			**X (Staff)**		

4. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	**Allowed**	**Allowed at certain times**	**Allowed with permission**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff permission**	**Not allowed**
Mobile phones may be brought to school	**X***				**X ***			
Use of mobile phones in lessons			**X****					**X**
Use of mobile phones in social time	**X**							**X**
Taking photographs on school camera devices			**X**				**X**	
Taking photographs on personal mobile phones				**X**				**X**
Use of hand held devices e.g. iPads, Kindles in lessons			**X**				**X**	
Use of personal email address in school, or on school network			**X**					**X**
Use of school email for personal emails			**X**					**X**
Use of chat rooms / facilities for personal use				**X**				**X**
Use of instant messaging for personal use				**X**				**X**
Use of social networking sites for personal use				**X**				**X**
Use of blogs	**X**						**X**	

* Allowed only after the Mobile Phone Contract has been signed by a parent. This can be found in the student planner (Junior School).
**Allowed specifically for teaching purposes (BYOD).

5. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of computing, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If apparent or actual misuse appears to involve illegal activity i.e:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school systems. Other activities such as cyber-bullying would be banned from school systems and could lead to criminal prosecution. 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, the school will use the following procedure to protect all those involved and to preserve evidence of a subsequent investigation. At the Royal Grammar School Junior School, like other schools in Newcastle, when an incident occurs it is important that we keep a clear record of what has and is taking place. At RGS we will use the whole school e-safety incident report log.

At least two senior members of staff will be nominated to investigate the report; this is most likely to be the IT Director and the Headteacher, but may include other members of the JS Leadership Team.

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. Use the same computer 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 well as 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 Headmaster 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 the 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 material to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

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

6. Responding to Incidents Reporting Log

E-Safety Incident Report

This E-Safety Incident Report has been compiled by:
Name:
Role:
Date:

When did the incident occur?
Date:
Time:

When was the incident logged?
Date:
Time:

Who is reporting the incident?
Name:
Role:

Who has been informed?	**(✓)**
Class teacher	
Computing Subject Leader (Junior School only)	
IT Director (P Miller)	
Leadership team	
Headteacher	
Parents/Carers	
CEOP	
Child Protection officer	
Police	
Other (please specify)	

Where did the incident occur?	**(✓)**
School (please specify location/s)	
Other	

Who was involved?

What is the nature of this incident?

Incident witnessed by:	**Names:**
Staff	
Pupil	
Parent	
Other	

Has any evidence been collected? If so, what is it and where has it been kept?

What action has been taken?	**(✓)**
Evidence preserved	
Senior Staff informed	
Other action (please specify)	

Will follow up action be necessary?	**(✓)**
Yes (give further details)	
No	

Will a review date be necessary?	**(✓)**
Yes (give further details) Date:	
No	

Signature of person reporting incident?

Name:

Thank you for completing this report.
If you need to record any further information please attach it to this sheet.
Please pass this report to the appropriate person immediately (for Junior School Mr Craig and Mrs Baillie and for Senior School Mrs Baillie and Dr Trafford).

Levels of E-Safety Infringement (Junior School)

The school deals with each incident individually and will respond to each case as deemed appropriate.

An E-Safety Incident Report Form must be completed in any of the following situations (this acts as a guide to follow):

Deliberate breaches of E-Safety	**Actions/Sanctions**
Use of non-educational sites during lessons	**Level 1**
Unauthorised use of e-mail	**☐Inform class teacher** **☐Inform computing subject leader** **☐Remind student of e-safety rules** **☐Inform parents informally (if deemed necessary)**
Unauthorised use of mobile phone/ digital cameras/ other handheld devices	
Unauthorised use of instant messaging/ social network sites/	
Unauthorised downloading/uploading of files	

Repeated Level 1 breaches after reminder given	**Level 2**
Deliberately corrupting or destroying work/data belonging to other pupils	**☐Inform class teacher** **☐Inform computing subject leader** **☐Inform IT Director (P Miller)** **☐Inform Headteacher** **☐Inform parents**
Allowing others to access school network by sharing username and passwords	
Attempting to access or accessing the school network, using another pupil's account	
Attempting to access or accessing the school network, using the account of a member of staff	

Sending an e-mail or message that is of a bullying or offensive nature (one-off incident) Please see bullying policy.	**Level 3**
Deliberately trying to access offensive or pornographic material (one-off incident)	**☐Inform class teacher** **☐Inform computing subject leader** **Note: the computing subject leader should contact the Paul Miller to ensure that appropriate filters are being applied.** **☐Inform Pastoral Director (KW and SB)** **☐Pastoral Director to inform the headteacher** **Note: If the headteacher is not available, inform another one of the designated staff responsible for Child Protection** **☐Inform parent/carer** **☐Remove internet access rights for a period of time** **☐Secure and preserve any evidence** **☐Inform CEOP/police**
Using proxy sites or other means to subvert the school's filtering system	

Continued sending of e-mails or messages that are of a bullying or offensive nature after level 3 sanctions	**Level 4**
Deliberately accessing any material deemed to be offensive, obscene, defamatory, racist, homophobic or violent	**☐Inform class teacher** **☐Inform Computing subject leader** **Note: The Computing subject leader should contact P. Miller to ensure that appropriate filters are being applied.** **☐Inform Pastoral Director/ SLT.** **☐Inform Headteacher** **Note: If the Headteacher is not available inform another one of the designated staff responsible for Child Protection.** **☐Contact with parent/carer** **☐Remove Internet Access rights** **☐Secure and preserve any evidence** **☐Inform police**

	Level 5
Receipt of transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	**☐Inform Headteacher / Pastoral Director immediately.**
Actions which could bring the school into disrepute or breach the integrity of the school	**☐Inform Headteacher / Pastoral Director immediately.** **☐ Suspension**

7. Actions and Sanctions for Pupils and Staff

Pupils **Actions/ Sanctions**

Incidents:	Refer to class teacher	Refer to JSLT	Refer to Headteacher	Refer to Police	Refer IT Director for action	Inform parents/carers	Removal of network/ internet access rights	Warning	Further sanction e.g. detention/ exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X				X			
Unauthorised use of mobile phone/ digital camera/ other handheld device	X	X				X			
Unauthorised use of social networking/ instant messaging/ personal e-mail	X	X				X			
Unauthorised downloading or uploading of files	X	X				X			
Allowing others to access school network by sharing username and passwords	X	X				X			
Attempting to access or accessing the school network, using another pupil's account	X	X			X	X			
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X			
Corrupting or destroying the data of other users		X			X	X			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X				X			
Continued infringements of the above, following previous warnings or sanctions			X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						
Using proxy sites or other means to subvert the school's filtering system		X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material			X			X	X	X	X
Receipt of transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X			X			

Staff **Actions/ Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to technical support staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X	X	X
Excessive or inappropriate personal use of the internet / social networking sites/ instant messaging / personal email		X						
Unauthorised downloading or uploading of files		X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X		
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		X			X	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X			X		
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils		X				X		
Actions which could compromise the staff member's professional standing		X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		
Using proxy sites or other means to subvert the school's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X		X	X	X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions		X	X	X		X	X	X

8. Acceptable Use Agreement for Staff

Newcastle upon Tyne Royal Grammar School

Staff Internet, Network and Laptops – Acceptable Use Policy

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

Issued September 2013 **Author: Richard Metcalfe**

With few exceptions, all RGS staff are required to use computers, the school network and the internet in connection with their work. All staff are required to be responsible for their own computer use and RGS employment contracts require all staff to comply with the policy for use of ICT: this document is the current version of that policy. As part of the School's commitment to providing a safe learning environment, we provide a filter service to try and prevent any unsuitable material appearing on the school network. Using these methods, we are as safe as can reasonably be expected. Set out below are the procedures which you as an employee must follow to ensure that this safety is not compromised.

You must:

- ✓ Use the computers to enhance teaching and learning for yourself and the students and/or in connection with the effective running of the School
- ✓ Use the RGS ICT network and equipment in accordance with the School's Data Protection Policy (this is also a contractual requirement)
- ✓ Treat all ICT equipment with care
- ✓ Keep your password safe and report any password that is compromised
- ✓ Only store on the RGS network work related files and information
- ✓ Only install on the RGS network licensed software that is work related
- ✓ Only use installed software in accordance with the licence(s) held for it

You must not:

- × Actively seek to bypass school security measures
- × Access or seek to access any illegal or inappropriate material
- × Download to the RGS network or equipment without permission any files that are not work related
- × Store files on your user area or laptop that are not related to your role in RGS.
- × Seek to send to or download to the School network any material that has not been virus checked
- × Use another person's account at any time.
- × Deliberately damage the computer equipment or use the network in a manner that will prevent others using it.
- × Allow your laptop to be used by any other person other than yourself at any time in or out of school.
- × Use RGS ICT equipment/network/internet access for unreasonable recreational use.
- × Use material for school work without permission from the copyright holder/owner.
- × Use ICT equipment for fraudulent purposes
- × Use or amend images or text that may cause distress or offence
- × Use any IT equipment to harass, bully, abuse or otherwise distress any individual inside or outside school
- × Use iSAMS to share/distribute files or information that is illegal, pornographic or may cause offence or distress.

You must be aware that:

- ✓ The School reserves the right to monitor all users of the network and to check your user area regularly to ensure correct and appropriate usage.
- ✓ You have a responsibility to use the facilities in an appropriate manner.
- ✓ You are totally responsible for your own user space, laptop and/or PDA and any unsuitable material found on it.
- ✓ Any material in your user area that is not work related may be deleted at any time.
- ✓ You are responsible for saving and backing up your own work.
- ✓ You will be personally liable for any fraudulent or criminal activities as a result of e-commerce carried out using the RGS network or equipment.

Reporting of inappropriate use:

- ✓ If you become aware of any inappropriate use of the School's network, in the first instance please contact the RGS Director of IT Services.

- ✓ Please also see the RGS Whistle Blowing Policy in connection with reporting inappropriate use

Dealing with inappropriate use:

- ✓ Minor infringements will be reported by the Director of IT Services to SLT, who will determine the action to be taken
- ✓ Serious cases of inappropriate use may be dealt with through the RGS Staff Disciplinary Procedures
- ✓ If necessary, serious cases of inappropriate use may also be reported to the police and external agencies such as the Information Commissioner.

- The current policy can be viewed in the Staff Handbook or on the RGS staff intranet.
- Please note that this policy may be updated from time to time.
- Changes to the policy will be notified by e-mail to your school mailbox

9. Acceptable Use Agreement for Visitors

Computing and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of Computing. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Pastoral Director as the Designated Safeguarding Lead (DSL).

Royal Grammar School

Agreement regarding use of IT Resources by visitors

This Agreement relates to the IT resources used by a person visiting RGS. Please read the following terms and conditions carefully – their purpose is to ensure that the School complies with legislation and licensing requirements and to protect the RGS network.

Specific conditions

1. IT Resources are provided solely for the purposes of preparing and presenting material relating to teaching and administration at RGS: e.g. Powerpoint presentation or access to web-based information used for teaching, training, display or administration of that particular activity.

2. All of the points set out in the RGS Code of Conduct for use of Communications and Information Technology (printed on the reverse of this agreement) apply to the use of this equipment.

3. The user of the resource must ensure that it is not used by any third party other than authorised RGS staff.

4. Personal devices must only be connected to the RGS network hardware, as approved by the Director of IT Services.

5. IT resources are to be used while at RGS and only used out of school with the express permission of the Director of IT Services.

6. The user of a resource is responsible for its safe-keeping at all times.

7. The user must not download files from or save files to accessible parts of the RGS network or the internet on this equipment without the express permission of the Director of IT Services.

8. The user must not use IT resources for any purpose which might breach Safeguarding or Data Protection regulations or bring RGS into disrepute.

9. For further information about this policy, please contact the Director of IT Services on extn 313 (DDI 0191 212 8964) or e-mail p.miller@rgs.newcastle.sch.uk .

Member of RGS staff issuing this Agreement (please print) ……

I agree to the conditions of use for IT Resources, as set out above

Signed …… Date……

Two copies of this agreement are to be signed for each visitor: one is to be retained by the member of staff responsible for issuing the agreement, and one by the Director of IT Service

10. Rules for Responsible Use of iPads, Computers and the Internet (Acceptable Use Agreement for 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 not bring USB Flash drives (memory sticks, pen drives etc) into school without permission;
- I will ask permission from a member of staff before using the Internet;
- I will only e-mail 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.

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.

Parent/carer's permission

I give permission for use of computers, iPads and access to the Internet on the terms set out in the above rules.

Signed:…….

Print Name:……..

Pupil's agreement

I agree to follow the Rules for Responsible Use of Computers and the Internet

Signed:…….…..

Print Name: ……

Class: ……

The above agreement is found in each pupil's student planner.

11. 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

Pupil'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).

12. Mobile Phone Contract (Junior School)

The use of mobile phones is part of our daily lives and it is appreciated that students might have the need to bring mobile phones to school with them; however, it is important that, whilst in school, phones are used sensitively and in accordance with the following rules:

The student agrees that:

1. As soon as I arrive in school, I will switch off my phone and hand it in to the designated place in my classroom;
2. I can only use my phone during the school day to contact my parents/guardians and to do so I will request permission from my teacher;
3. If I do use my phone (with permission), it will be switched off and returned to the designated area as soon as I have finished my call;
4. At the end of the school day (3.30pm), or at the conclusion of an after-school club (with the teacher's permission), I can contact parents to update my travel arrangements but I will not contact other students (when not in use, my phone will be in my pocket);
5. I will not play with my phone in late room or anywhere else in school (this includes using the phone as a camera or camcorder);
6. I must not lend my phone to anybody else in school;
7. My phone can only be taken on school trips and sporting fixtures at the discretion of the teacher leading the trip. If permitted to take my phone, I know I must follow rules 1 to 4 and 6 above.

NB: Messages fro parents to students during the school day (8.30-3.45pm) are best directed to the school secretary, Miss Emma Hollins, on 0191 2818955, who will then pass them quickly on to the relevant class teachers and children.

By signing this contract, I agree to abide by the points above.

Pupil's name: Class:

Signed: Date:

Parent's signature:

☐My child currently does not bring a mobile into school, however, if this should change, we agree to the points above.

K. Wall (Pastoral Care)

13. Letter to parents

Dear Parent/Carer,

Welcome to the new academic year. Your child is about to embark upon an exciting new stage in their education and we are very much looking forward to working with and teaching them this year.

Having moved into a higher year group, they have been made aware that this will involve an increased level of learning, responsibility and participation. We will be calling upon them to undertake extra work at home, much of which will be internet based.

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 our students' development but always want them to spend their time online safely. As a parent/carer you can play a significant part in ensuring this.

Just a few simple steps by you can help keep them safe and give young people the awareness to know what to do if they feel uncomfortable about anything they encounter while on the internet.

If you do not wish for your child to be able to access any inappropriate content online, please ensure that their computers, laptops and other devices with internet access are all fitted with parental controls.

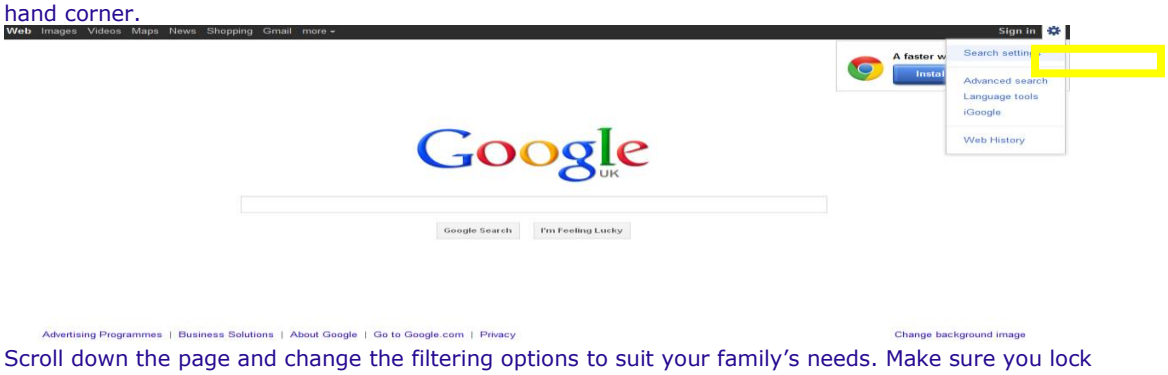
You can find free downloadable versions online or you can contact your internet service provider (such as BT, Talk Talk, Sky) for more information.

As a **minimum**, please set parental controls on your search engines, youtube account and the mobile phone your child uses.

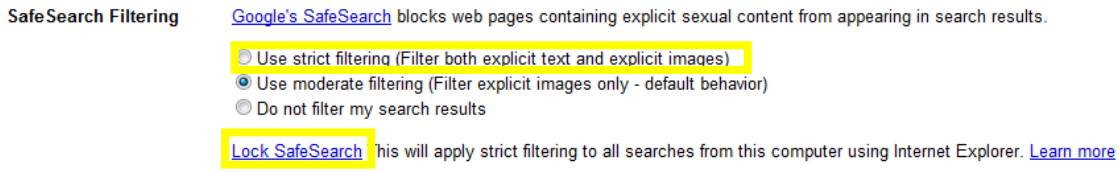
One of the most popular search engines in the world is Google. You can visit Google's informative safety centre for **simple** step by step guides - www.google.com/familysafety/tools

Here are a few options available to you; they truly are simple to set, promise.

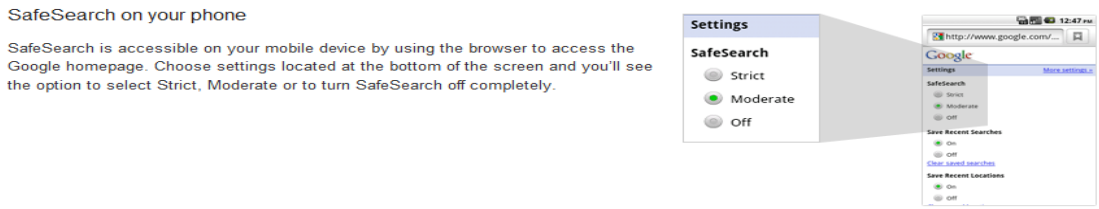
Visit the Google home page – www.google.co.uk and click on the 'search setting' tab in the top right hand corner.



Scroll down the page and change the filtering options to suit your family's needs. Make sure you lock the safe search; otherwise these settings can easily be changed without your knowledge.



You can also set this on your child's smart phone;



Please be aware that no filter is 100% accurate. CEOP advice that you talk to your child about the sites they use. Why don't you discuss:

- Their favourite online sites
- What they enjoy most, the fun aspects of being online?
- What they think can go wrong?
- How would they react if things got out of control?

Let them know that you understand that situations happen online and that seeing 'adult' material can make them feel uncomfortable. Make sure they know that you are there to help.

Visit The Child Exploitation and Online Protection Centre (CEOP) parents' information website for more information - www.thinkuknow.co.uk/parents

Please remember if you are concerned that an adult has made inappropriate contact with your child you can report this directly to CEOP, either by visiting the site www.ceop.police.uk/safety-centre or clicking the button:

Look out for CEOP's future parent and carers updates.

Key safety rules used in the Junior School

Childnet SMART rules have been written especially for young people to remind them how to be careful online. Please spend time looking through them and discussing them with your child/children. A copy of these rules can be found in your child's student planner.