Royal Grammar School

E Safety Policy

Introduction

At the Royal Grammar School we use technology and the Internet extensively across all areas of the curriculum and as such safeguarding and applying appropriate controls/restrictions are essential. Online safeguarding (E-Safety), is an area that is constantly evolving and as such this policy will be reviewed at least annually by the Governing Body.

The primary purposes of this policy are:

- To empower the whole school community with the knowledge to stay safe and reduce risk.
- To ensure that risks are clearly identified, assessed and mitigated in order to reduce any potential harm to students and staff, and any liability for the school.

This document provides a guide for adults working in our school about acceptable and desirable conduct to protect both adults and students. It also includes guidance for students and parents on E-Safety issues. It refers to and complements other policies and guidance at The Royal Grammar School with which all staff, volunteers and visitors must be familiar and work in accordance to. The policies include in particular:

- Child Protection Policy
- Staff Code of Conduct. ‘Guidance for Safe Working Practices for the Protection of Children and Staff’
- Preventing Radicalisation Policy
- Behaviour Policy
- Acceptable Use of ICT Systems Policy and Internet Safety
- Anti-Bullying Policy
- Equal Opportunities and Race Equality Policy
- Health and Safety
- Staff Handbook
- Guidance on Photography and Recording images of RGS students
- Mobile Phone Guidance
- Additional Boarding Guidance papers to boarding staff.

You should also be aware of the following documents:

- *Keeping Children Safe in Education (September 2016).* ***All staff should read, understand and comply with their roles and responsibilities laid out in Part 1 of this document.***
- *Working together to safeguard children (March 2015).*
- *What to do if you're worried a child is being abused (March 2015)*
- *Guidance for safer working practice for adults who work with children and young people (October 2015).*

All of the above policies and documents can be found on SharePoint on the network at school.

The guidance in this document is also applicable to all adults working in Fraser Youens Boarding House.

It is the aim of the School to ensure that staff/adults do not place themselves in situations of vulnerability in their professional duties. To help staff/adults in this we would advise that the points in this document are heeded. This list is not intended to be definitive and we understand that professional judgment will be needed in dealing with situations that arise.

1. Teaching and Support Staff

All adults working in our school should know the name of the Designated Safeguarding Lead (Mrs Dawn Booth – Assistant Head) and the Additional Designated Safeguarding Leads (Mr Scourfield and Mrs Herath) be familiar with our Child Protection Policy and understand their responsibilities to safeguard and protect children and young people.

All staff should be aware of the school policies and documents on E-Safety available on **SharePoint** which set out our expectations relating to:

- Creating a safer online environment
- Giving everyone the skills, knowledge and understanding to help children and young people stay safe online.
- Inspiring safe and responsible use and behaviour
- Use of mobile phones both within school and on school trips/outings
- Use of camera equipment, including camera phones
- What steps to take if you have concerns and where to go for help
- Staff use of social media as set out in the Staff Code of Conduct. 'Guidance for Safe Working Practices for the Protection of Children and Staff.'

The E-Safety Officers (Named DSL and ADSLs) will:

- Keep up to date with the latest risks to children using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Senior Team.
- Advise the Senior Team and governing body on all significant E-Safety matters.
- Engage with parents and the school community on E-Safety matters at school and/or at home.
- Liaise with IT technical support and other agencies as required.
- Retain responsibility for the E-Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical E-Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose.
- Make themselves aware of any reporting function with technical E-Safety measures, i.e. Internet filtering reporting function.

And with support from the ICT technicians will ensure that:

- Anti-virus software is fit-for-purpose, up to date and applied to all capable devices.
- Software updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly and have been applied correctly.
- Passwords are applied correctly to all users.
- The ICT System Administrator password is changed on a regular basis.

All staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headmaster.
- Any E-Safety incident is reported to the E-Safety Officers within 24 hrs and appropriate action will be taken. If staff are unsure, the matter should be raised with the E-Safety Officers who will make appropriate decisions.

2. Students

- The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use of ICT Systems and Learning Gateway for Students, the School Rules, the Behaviour Policy, the Valuables Policy and the iPad Agreement **(All available on the School VLE).**
- All students sign and agree to the Use of ICT Systems and Learning Gateway for Students before being granted any access to the school network, ICT equipment or services.

- Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the school Behaviour Policy.
- E-Safety is embedded into the curriculum – students will be given the appropriate advice and guidance by staff, in all subject areas across the curriculum.
- All students will be fully aware of how they can report areas of concern whilst at school or home.

3. Parents/Carers

- All parents/carers should be aware of the school policies and documents on E-safety which are available on the **school website /About/policies and procedures.**
- Parents play the most important role in the development of their children and as such the school will support parents in accessing resources to acquire the skills and knowledge they need to ensure the safety of children outside the school environment.
- Through parent information evenings (e.g. Childnet to Year 7), school newsletters and the availability of free online training courses (Think U Know) the school will keep parents up to date with new and emerging E-Safety risks, and will involve parents in strategies to ensure that students are empowered.
- Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such all parents will sign the Acceptable Use of ICT Systems and Learning Gateway for Students before their son can be granted any access to the school network, ICT equipment or services. All parents receive guidance on photography or recording of images of RGS students. A list of students whose parents have indicated that they would not like their son’s image recorded will be held by the Admissions Office and E-Safety officers.

4. Network and Device Management

The Royal Grammar School uses a range of devices including desktop PCs, laptops and tablets. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering

We use a web filter that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites. The IT Manager and E-Safety Officers are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Senior Team.

Email Filtering

We use Microsoft Office 365 which aims to prevent any infected email being sent from the school or being received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. The system is also used to filter certain words and can be used for monitoring.

Passwords

All staff and students will be unable to access the network without a unique username and password. Staff and student passwords should be changed if there is a suspicion that they have been compromised. The ICT Leader will be responsible for ensuring that passwords are changed as and when required.

Anti-Virus

All capable devices will have anti-virus software. This software will be updated regularly with new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the IT Manager if there are any concerns.

5. Email

All school employees and students are issued with a school email account, the address ending with:

@rgshw.com

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is expected to be used for professional work-based emails only. The use of personal email addresses for the purposes of contacting students is not permitted.

Students are permitted to use the school email system too, and as such are all issued with a RGS email account and their own approved email address. Students should use this email account only for school based activity as laid out in Acceptable Use of ICT Systems and Learning Gateway for Students that they have signed on entry to the school.

6. Photos and Videos

All parents receive guidance on photography or recording of images of RGS students. A list of students whose parents have indicated that they would not like their son’s image recorded will be held by the Admissions Office and E-Safety officers. A list of students who are not permitted to be photographed will be available to all staff with reminders sent out periodically. This list will also be kept by the E-Safety Officers and the Admissions Officer.

Students may not take photos or video footage for personal use anywhere on the school site unless they have written permission from a member of the Senior Team. Any photos or video footage taken in lessons (to enhance a practical activity etc.) must be deleted once their purpose has been fulfilled.

Photographs with names directly identifying the student will not be published by the school without the express permission of the appropriate individual.

7. Social Networking

Any use of social media services in school must be in accordance with the ICT Acceptable Use Policy for Staff.

8. Copyright

Should it be brought to the school's attention that there is a resource which has been inadvertently uploaded, either to the school website or school/department authorised social networking sites, and the school does not have copyright permission to use that resource, it will be removed within one working day.

9. Reporting E-Safety Incidents

Any E-Safety incident must be brought to the immediate attention of the E-Safety Officers. The E-Safety Officers will assist in taking the appropriate action to deal with the incident, liaise closely with the relevant staff to ensure the appropriate resolution of the incident and to complete and maintain any necessary documentation.

All staff should make themselves aware of the procedures and the responsible staff involved in the process.

10. Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues, and the regular distribution of E-Safety information to staff, students and parents.

The school will ensure that aspects of E-Safety for students are firmly embedded into the curriculum.

Whenever ICT is used in school, staff will ensure that students are made aware of the safe use of technology and risks as part of the students' learning and understanding. Subject Leaders should be able to demonstrate where and how the awareness of risk is imparted to students in lessons.