RGS STUDENT IT ACCEPTABLE USE POLICY

Introduction

To whom does this apply?

This policy applies to:

- all students of the Royal Grammar School Guildford.

What is the purpose of this policy?

This policy exists to protect school employees, pupils, data, and the school's reputation. It is designed to enable staff, students, and other authorised individuals to perform their roles effectively and efficiently while working at the school. It should be read in conjunction with all other related school policies.

Infringement

Breaches of the policy will be dealt with under the School's standard Disciplinary Policy or in serious cases reported to the Police.

Monitoring of Technology

IT Services staff may inspect any IT equipment or services owned, leased or provisioned by the school at any time without prior notice.

The Royal Grammar School may monitor, access, log and disclose telephone calls, emails, instant messaging, and any other data transmissions involving its employees, pupils, or contractors passing through the School's internal network or School provided cloud services, without consent, to the extent permitted by law.

This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of School IT; for quality control or training purposes, or to prevent or detect crime.

Please note that personal communications using school hardware, networks or services may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All data traversing the school network and cloud services, including Internet activity, is logged by the school. These logs may be reviewed and stored at the discretion of the Director of IT, Bursar, or Head.

Internet Filtering

The school has in place a filtering & monitoring system which checks for viruses and suspicious emails, denies access to most undesirable and inappropriate sites on the Internet, and maintains a list of banned sites which is updated on a regular basis.

All devices connected to the school network, either by cable or wireless, have their internet filtered based on the user authenticated on the device. For example, a Sixth Form student may have greater internet access than a First Form student.

The purpose of school web filtering is as follows:

- To protect students and staff against common online threats such as viruses and scams.
- To enable the school to meet its safeguarding duty of care to protect staff and students.
- To protect the school network from security breaches, online risks and to prevent access to services which may have a negative impact on the functioning of the school network.
- To limit access to content which may cause disruption in the classroom.

While there are some restrictions in place, it is the intention of the school to provide as broad access as possible to online services.

You can report a service to be accessible or blocked by emailing the website to helpdesk@rgsg.co.uk and providing your reasoning that access should be enabled. Likewise, if you find that you can access content which you considered inappropriate, please email helpdesk@rgsg.co.uk.

Please be aware that:

- Internet access within the school and the use of cloud and remote services will be logged and may be monitored for inappropriate use.
- All internet sites accessed within the RGS network are logged with date and time of access.
- The accessing and use of inappropriate and indecent materials from the internet or via e-mail will result in disciplinary action being taken.

Use of VPN Services (Virtual Private Network)

VPN applications and services may not be used on devices when connected to the RGS network.

The use of a VPN limits the school's ability to carry out due diligence and safeguarding to ensure students are protected from common threats such as online bullying and limiting access to inappropriate material.

Devices detected using a VPN may have their access to the school network limited or disabled.

Email Filtering

All email traffic is filtered before it reaches your school mailbox. This is done for the following reasons:

- To prevent the spread of viruses, hoax emails, phishing emails and other spam content.
- To prevent inappropriate content being sent or received.

User Accounts

Your user accounts give you access to confidential student and staff information, school data assets, and other information which may have a financial or reputational value to the school. School policy requires that you understand and follow points below:

- You are responsible for all activity carried out under any account assigned to you, whether accessed via school IT equipment, your own personal device, or a remote computer. This includes logon accounts, door access codes and finger scans, and email accounts.
- You are required to follow the school's IT Account Password Policy – see separate policy.
- Do not allow any other person to use school user accounts or access codes assigned to you.
- Ensure that you log off from your machine completely when you are going to be away from the computer for an extended period.
- Do not access, load, store, post or send any material that is, or may considered to be illegal, libellous, pornographic, obscene, defamatory, intimidating, or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.
- Students who have left the school will have their accounts deactivated on their final school day unless IT Services are directed otherwise by the Director of Studies.
- Accounts inactive – not logged into either in school or remotely -- for more than 20 school days will be disabled unless there are extenuating circumstances, for example, long term sickness communicated to IT Services by the Head of Year.
- Any account inactive and disabled for more than 3 months, and any associated data, will be deleted.

Personal Use of School IT Systems

Limited and reasonable personal use of the School's IT systems by students is allowed if it is not excessive and does not:

- interfere with normal work or the work of others or teaching and learning
- involve more than minimal amounts of working time
- involve the school in significant expense
- expose the School to legal action or risk bringing the School into disrepute
- relate to running a private business

Password Policy

Your password should always be secure and kept private. You are responsible for any activity taken under your user account. See the School IT Account Password Policy for more information.

Storing & Transferring Personal, Sensitive, or Confidential Information Using Removable Media

For the protection of the school network and services, the use of USB storage is disabled on most school computers. Instead you should use your school provided OneDrive account.

Email and School Social Media Accounts

All users are provided with an @rgsg.co.uk email account.

Email is classified as a legal document which can be used by the school or requested as part of legal action.

Email should be treated as inherently insecure. As with any form of correspondence be aware of the language used. Do not open or forward any email or attachment from an unrecognised source or that you suspect may contain inappropriate material or viruses.

Do not respond to emails that request personal details unless you are confident the source is genuine. In general companies will not request personal data via email. Staff should not provide personal contact details to pupils and should only contact pupils for professional reasons.

Users must not send, forward, print or transmit in any form any offensive, obscene, violent, dangerous or inflammatory material via email. Users are not permitted to send or forward chain letter emails, jokes, spam etc. If you are concerned about any email that you may have received, contact IT Services (helpdesk@rgsg.co.uk).

Copyright Infringement

Royal Grammar School students will respect all digital copyright rights including:

- the rights of owners of third-party material used in teaching
- the rights of students in all material they create in and for school
- the rights teachers have in material they created prior to being employed at the school and in material created while employed at the school

Printing and Photocopying

Printers and photocopiers are available across the school for students to use. Printers and photocopiers may only be used for school related work.

Students are limited to 80 printed pages per month. Quotas renew on the 1st of each calendar month.

Students are expected to collaborate to use their printer quota's in the most efficient way possible, but under exceptional circumstances, for example, course work, or exam preparation, students may request their teacher to apply for an extension to their quota with the Director of IT.

Computer Misuse

The Computer Misuse Act 1990 makes it illegal to:

- Gain unauthorised access to a computer's software or data (hacking), including the illegal copying of programs
- Gain unauthorised access to a computer's data for blackmail purposes
- Gain unauthorised access to a computer's data with the intention of altering or deleting it, including planting viruses
- Copy programs illegally (software piracy)

Any type of hacking (defined as attempt to gain access to folders, databases, or other material on the network to which one is not entitled) is an extremely serious offence. To

comply with the Computer Misuse Act 1990 any user who indulges in hacking or is found with hacking software/paraphernalia on their computer or network account will face disciplinary action.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Director of IT. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the IT Services department.

Reviewed by: **Director of IT**
Date of last review: **Trinity 2021**
Date of next review: **Trinity 2022**