RGS STUDENT IT ACCEPTABLE USE POLICY

Introduction

To whom does this apply?

This policy applies to:

- all students at the Royal Grammar School Guildford.

What is the purpose of this policy?

This policy is designed to safeguard the school community, which includes staff, students, and data, while also upholding the school's reputation. Its purpose is to empower staff, students, and other authorised individuals to carry out their responsibilities with safely and efficiently within the school environment.

Infringement

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

Safeguarding, Security, Internet Filtering and Monitoring

Every device that's connected to, and all data that passes through the school's network, cloud services and apps, may be monitored and filtered.

All data traffic sent to or from any device connected to the school network are subject to several automated safeguarding monitoring systems to allow the school to undertake its safeguarding duty of care to protect all members of the school community.

The purpose of these systems is as follows:

- To protect students and staff against common online threats such as viruses, malware, phishing attacks 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 inappropriate content.

Safeguarding

The school has implemented a comprehensive safeguarding system, Securus, on all school-provided student devices. Securus is designed to detect any inappropriate content or risks that may pose a threat to students. Should any such content or risk be detected, Securus will promptly report this to our Digital Safeguarding leads. It is important to note that Securus operates only during normal school hours. The implementation of this system contributes significantly towards creating a secure digital environment for students.

Malware, Virus, and Phishing Protections

We employ a robust malware, virus, and phishing protection service that monitors all data transmitted and stored within the school's Microsoft 365 service and stored on school provided devices. This service is programmed to take action at the first sign of any suspicious activity. Actions taken may include deleting or quarantining suspicious files and emails, restricting user accounts, or reporting potential threats. This ensures that our digital environment remains safe and secure from external threats.

Web Filtering

The school employs a web filtering system to ensure that students have access to safe and educational online content. This system blocks access to content via the school network that are deemed inappropriate or unsafe for student viewing. It is designed to create a safe online browsing environment by filtering out content that is not conducive to learning. This includes, but is not limited to, websites containing adult content, violence, hate speech, or any other content that goes against our school’s values and guidelines. We encourage students to use the internet as a resource for learning and personal growth, and our web filtering system supports this by providing a safe and focused online environment.

Please report content which has been incorrectly categorised to helpdesk@rgsg.co.uk.

Email Phishing Simulations

As part of our ongoing commitment to digital security, we will be conducting email phishing simulations targeted at our student body. These simulations are designed to mimic real-world phishing attempts that can compromise your personal information and digital security.

The purpose of these simulations is not to “catch people out”, but to educate and prepare them for potential threats. Much like a fire drill prepares staff and students for emergency situations, our email phishing simulations are intended to help you recognize and respond to phishing attempts in a safe and controlled environment.

We encourage students to think of these simulations as “digital fire drills”, designed to keep you safe and well-prepared in the digital world.

Monitoring

The School may monitor, access, log and disclose any data transmitted via the school’s network, cloud services, and hardware without consent, to the extent permitted by law. This includes, but is not limited to:

- Microsoft 365 services: Teams chat, OneDrive, SharePoint etc.
- Telephone calls, voicemail, call history, call recordings and transcriptions.
- The school wireless network and cable network.
- School managed Microsoft Surfaces and other hardware.
- School servers: on-premise and cloud hosted.

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

Monitoring serves multiple purposes. It might be used to verify or gather information related to school operations; to check compliance with the school's policies, standards, and procedures; or to make sure IT systems are working efficiently; for training or quality improvement.

Keep in mind, if you're using the school's apps or services for personal conversations, they may unintentionally be part of the communications that are monitored, intercepted, and 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.

Data deleted by users – including emails, Microsoft Teams chats, and documents – may be archived indefinitely or for specific period as part of compliance processes.

User Accounts & Use of the School System

Your school user accounts give you access to a range of school apps and services. You are also permitted access the school buildings via your finger scan. It also gives you access to some personal information (such as names, email addresses, and chat messages) related to other students and staff.

Use of your school user account requires that you understand and follow points below:

- You are responsible for all activity carried out under any account assigned to you by the school, 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.
- Do not allow any other person to use any user accounts or access codes assigned to you. This includes, another member of your family using your school loaned Surface.
- Ensure that you log off from or lock 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).

Password Policy

See the separate School IT Account Password Policy for details.

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.

Student Leavers and Your Data

- 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.

Use of a Personal VPN (Virtual Private Network) Services & Apple iCloud Private Relay

The use of a VPN and Apple iCloud Private Relay or any technology which masks the identify of a computer, removes 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.

Personal VPN applications and services (for example, NordVPn, ExpressVPN and Surfshark) may not be used on ANY device connected to the RGS network.

When accessing any school digital services, an automated check will be carried out to detect the use of a VPN. If a VPN is detected, or it is believed that a VPN is being used, one or more of the automated actions will be taken without notice:

- You will be denied access to login.
- Your account access will be limited.
- You will be required to use multi-factor authentication.
- Your account will be disabled pending a manual review.
- In extreme circumstances, your account and Surface will be disabled.

Support will not be provided by the IT Services department for any device found to have a VPN installed, until it is removed by the user.

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.

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

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

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.

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 quotas 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.

Use of cameras, microphones, and other recording technology

Students should not make recordings of any staff, students, or other members of the school community without their express permission.

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 directorofit@rgsg.co.uk. 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: **30 June 2023**
Date of next review: **Trinity 2024**