ACCEPTABLE USE OF IT POLICY
(Students)

Date to be reviewed	June 2022
Date of last review	June 2021
Governors Committee accountable for review	Education Committee
Senior Team member accountable for review	DHM

Introduction

This Policy applies to all computers fully or partially owned or operated by the RGSHW, and to any computer and mobile device used on its premises whether connected to the school network. This includes:

- The voice and data networks that connect them
- All devices connected to these computers and networks
- All hardware and software associated with these systems
- The information managed by these systems

This Policy applies to all students of the School, including those in Fraser Youens Boarding House. It aims to ensure that all users are aware of how to use IT responsibly and safely. There are additional specific Boarding House guidelines relating to the use of IT.

The RGSHW is fully committed to ensuring that the application of this policy is non-discriminatory, in line with the UK Equality Act (2010). The RGSHW seeks to implement this policy through adherence to the procedures set out in this document, and through commitment to staff and pupil training.
All information held electronically is secure, and the School fully complies with the Data Protection Act 2018 and the GDPR Act 2018.

This policy should be read in conjunction with other school policies:

- Anti-Bullying Policy
- Behaviour Policy
- Child Protection Policy
- Opportunities and Race Equality Policy
- Pastoral Care Policy
- Preventing Radicalisation Policy
- School Rules
- E-safety Policy

General

The school network and Learning Gateway is a valuable resource that is available to all students, staff, parents and governors via the Internet. Access is not therefore restricted to use at school. To ensure the safe use of this resource, and to help ensure that the system is kept available and in full working order, a series of policies apply. These policies are very similar for each type of user (student, member of staff, parent/guardian, governor). A specific policy has however been produced for each user type, clearly identifying the consequences of misuse. Inappropriate use will not only breach school rules but also may be a criminal offence.

All students must read and sign this policy at the beginning of each year, or after each major revision; their use of both internet and/or email at school is dependent upon this.

Data Access

This Policy aims to comply to all relevant aspects of the GDPR and data protection legislation as amended from time to time. Boys must ensure that they do not hold information of a personal or sensitive nature either on their devices or on USB sticks that are used in conjunction with RGS work. The RGSHW will undertake to educate boys on the scope of information of this nature.
Furthermore, the RGSHW will undertake to limit the use of USB sticks by training all boys to store information in their OneDrive accounts.

Aims and scope

Each individual is responsible for his/her actions.
This Policy relates to the use by RGSHW students of all the School's IT and communication systems. The School provides the IT and communication systems for the purposes of the student's work and the use of these systems at all times is subject to this policy. Any breach of this policy by a student's use of the School's IT systems will be considered a disciplinary issue. This Policy applies to all students who use the School's IT systems.

All individuals are expected to respect and observe policies and procedures governing:

- The privacy of and/or other restrictions placed on data or information
- The ownership of software and/or other assets pertaining to computers or network systems
- The finite capacity of computers or network systems.

The policy and procedures will ensure that:

- All students will be responsible users and will stay safe whilst using the internet and other online technologies for educational, social, and recreational purposes.
- The school endeavours to ensure that IT systems and users are protected from **misuse (whether accidental or deliberate)** that could compromise the safety of individuals or systems.

All students should be aware of the following:

1) Computer storage areas are school property
2) All network activity is monitored and recorded
3) All emails (even when deleted) and their history are logged and archived
4) Members of the IT staff may look at any files and communications to ensure that the system is being used responsibly
5) IT staff can view your computer screen at any time, from anywhere on the school network without you knowing about it

The following are not permitted:

- **BYPASSING OR ATTEMPTING TO BYPASS THE SCHOOL INTERNET FILTERING SYSTEMS BY USE OF PERSONAL HOTSPOTS, VPNs or by any other means. This is considered an extremely serious offence and will be dealt with as such**
- Use of another person's username and password
- Trespass in the folders, work, or files of other people
- Hacking or access with intent to cause damage
- Sending, displaying, accessing, or trying to access any obscene or offensive material
- Using obscene or offensive language
- Harassing, insulting, or attacking others through electronic media
- Violating copyright laws
- Revealing any personal information, the home address or personal phone numbers of yourself or other people to anyone on the internet, unless specifically authorised by parent, carer or teacher
- Downloading games or other executable programs
- Intentionally wasting limited resources or time on unnecessary or unauthorised activities (including playing games)
- Moving or changing any computer or associated equipment unless specifically requested and authorised by a member of staff. Damage caused by unauthorised persons may be considered a criminal offence.
- Commercial activities for profit, excluding Young Enterprise
- Carrying on a private business
- Undertaking financial transactions on behalf of the school unless authorised

Additional Information

- The Internet is provided for you to conduct genuine research and communicate with others. All the sites you visit are recorded. Remember that access is a privilege not a right, and that access requires responsibility at all times
- During lessons, teachers will guide you toward appropriate materials.
- You are required to log on with your own username, which will remain with you throughout your time at school
- You have your own password (for both the school network, Microsoft apps (Teams, Sharepoint), and the VLE) to allow you to log on. You should never reveal your password to anyone else. If you think someone has learned your password, change it immediately.
- Network passwords must never be given to anyone else, unless with the Director of IT's permission. Passwords should be changed at regular intervals – at least once a year and you must use a strong password. A strong password is at least twelve characters long and includes at least three of the four character classes (upper case letters, lower case letters, numbers and symbols); it should not include repeated sequences of letters or numbers. Your password should not be based on your own name or username, for example: smith 123.
- Do not write your password on anything you leave unattended.
- Remember that a school is a public place. Always make sure that you have completely logged off or locked the computer before leaving it unattended. Failure to do so will be considered a contravention of school policy. If an offence has been committed by some other person on your unattended computer, this may be considered as facilitating the Misuse of a Computer, which is a criminal offence. You are never allowed to use another

person's username and password. This is considered a criminal offence under the Computer Misuse Act 1990.

- If you are doing shared work, you must keep a copy of the work in the school's Office 365 cloud storage.
- You must not access or attempt to access the folders, work or files of another person. All unauthorised access is considered a criminal offence under the Computer Misuse Act 1990.
- You must not damage data, computers, computer systems or computer networks. This includes unauthorised access to any files or programs. Damage or unauthorised access may be considered a criminal offence under the Computer Misuse Act 1990.
- Programs may only be installed on a computer by a member of the IT administration department.
- You may not copy software contrary to the provisions of the Copyright, Designs & Patents Act 1988.
- You may not install, copy or transmit obscene material. Doing this may be considered a criminal offence under the Obscene Publications Act 1959/1964.
- Eating, drinking or the use of aerosol sprays near a computer may cause serious damage and are strictly prohibited.
- If a "virus alert" occurs when transferring work files from a memory stick, please inform your teacher and a member of the IT staff immediately. We encourage students not to use USB sticks, but rather to store their work in the cloud.
- You may not take RGSHW owned or provided computer equipment off-site without formal authorisation.
- You should not switch off a computer during the school day unless it has completely locked up or is unlikely to be used again that day.
- E-mail correspondence is not private. Your e-mails can easily be intercepted, copied, forwarded and stored without your knowledge. You must take into account the fact that any e-mail you send may be read by a person other than your intended recipient.
- You should treat any attachments which contain important or confidential material in the same manner as the email in terms of security.
- All messages and files are automatically scanned for viruses before being introduced into the network, but this does not provide a complete guarantee of protection. You should therefore, be very careful opening e-mails and attachments to e-mails from unknown sources. If you have any doubts about opening an e-mail or attachment, you should speak to a member of the IT team.
- You must not under any circumstances send messages or attachments, which are:
  - Abusive, including the use of foul language
  - Malicious
  - Discriminatory in any sense for example concerning sex, sexual orientation, age, race, religion, gender or disability
  - Defamatory about any other person or organisation bullying or intimidating in content.

  This applies either within the School or outside the School and to individual or internet websites, and to all social networking platforms. If you receive any such messages from outside the School you must report them to your Form Tutor, your Head of Year or the IT Manager. You must not forward them either within or outside the School. If you send

emails of the type described about this will be considered a disciplinary offence and treated accordingly.

Monitoring

- Searches on the internet and web addresses are monitored. The IT technicians will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.
- iPad use is constantly being monitored via the Mobile Device Management software. You must not remove this software from your iPad under any circumstances.
- Monitoring of the content of emails or telephone calls is not routinely carried out but may be carried out in some circumstances, such as: o Where the school has reasonable grounds to believe that a student is breaching this or any other policy of the school
    - For the purpose of assisting in the investigation of wrongful acts
    - To comply with any legal obligations
    - For the purpose of defending or prosecuting any legal action brought against the school.

File Security

- You have your own area for storing work in the cloud – OneDrive and SharePoint. This means that you can access your work from any network station
- You are not permitted access to work station and network drives other than those provided at login, nor are you permitted to alter or save files outside your own area (except in the authorised shared areas)
- You may not boot up network stations from a USB stick or CD. Unauthorised users attempting to do so will be in breach of the Computer Misuse Act
- An automatic and regular search will be made for any executable program and zip files stored in user areas. These will be noted, automatically logged against the user and the user notified. If the user cannot provide a satisfactory reason for them, appropriate action will be taken, including informing the appropriate authorities as deemed necessary.

Access to Software

- All users receive desktop icons and start-menu-shortcuts to all the main application programs and common utilities
- You are guided onto the network via shortcuts set up for each of the curriculum subjects and chosen at log on. This provides shortcuts/icons to programs that are relevant to the study of that subject as well as any shared documents provided by the subject teachers. You have read-only access to these shared documents but may copy them for your own use. Attempts to modify these are in breach of the Computer Misuse Act
- You can only access software and other resources as made available to you through these subject shortcuts. For example, students do not have access to the Staff areas. Access to certain resources such as Internet software may also be removed for certain network users, where found to be necessary
- Use of the main software packages is continually audited for each user

- Sites visited on the Internet are also audited and filtered by the Network's Firewall in accordance with Bucks Local Authority and School rules. If you continue to attempt to access sites blocked by the Firewall or you attempt to bypass the Firewall, you are in breach of the school policy. Where a site is blocked and is required for schoolwork, the IT staff may be requested to ask for the site to be unblocked via your subject teacher.

Computer and other equipment not provided by the School.

- If you bring a laptop, mobile device, personal music player, and/or any related or similar equipment onto School premises, you must ensure its security at all times. Never leave these items unattended in public places such as changing rooms. You should lock items away in your locker or hand them to appropriate staff. The school accepts no responsibility for the loss of these items
- If any equipment described above is lost or stolen, you must immediately report the incident to your Form Tutor or Head of Year
- You may only connect your laptop, or mobile device to the network, wirelessly with your credentials. You must not tether any devices to any 4G/5G connections which are not supplied by the school. You must not connect any or a personal music player or any gaming device without express authority from the ICT Manager. You should be aware that the school has in place measures to prevent this. Any breach of this rule will be treated as a disciplinary offence and will be treated accordingly
- You should ensure that any personal device used in school for schoolwork is brought in fully charged. There are no charging facilities provided at school, and students should not attempt to plug in devices to the school electrical circuits

Access to Printers

You should manage printing sensibly and not waste either ink or paper.

Consequences

1. Violations of the above rules will result in a temporary or permanent ban on your use of the school network. The more serious breaches, or repetitive breaches, will result in more significant consequences
2. The more significant consequences will be in line with our behaviour management policies and will include detentions, formal warnings and exclusions
3. Specifically, any student who tries to bypass the RGS internet filtering system will be in breach of the School's ICT policy and will face severe sanction
4. When applicable, the police or local authorities may be involved.

Appendices

Computer Misuse Act 1990

The "Computer Misuse Act 1990" covers three offences:

- Simple hacking, that is the unauthorised entry to computer facilities via a computer
- Unauthorised access with criminal intent, that is hacking with the intention of perpetrating a more serious crime and covers facilitating access to others
- Unauthorised amendment or damage to data and covers among other things the introduction of viruses and time bombs

Anyone convicted of an offence under this act can expect a fine of an unlimited amount plus a prison sentence ranging up to a maximum of 5 years.
Anyone suspecting that an offence has been committed should refer the matter to the Headmaster.

Obscene Publications Act 1959 and 1964

The "Obscene Publications Act 1959 and 1964" states that an article shall be deemed to be obscene if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.
It is an offence to publish an obscene article or to have an obscene article in ownership, possession or control with a view to publishing it or, where the data is stored electronically, to transmit that data.

The Telecommunications Act 1984

The "Telecommunications Act 1984" makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character' and is a criminal offence which is punishable by a custodial sentence.

Copyright, Designs & Patents Act 1988

The "Copyright, Designs & Patents Act 1988" provides the same rights to authors of computer programs as literary, dramatic and musical authors have to their works. Those rights extend for the life of the author and for fifty years after the author's death.

Software is generally not sold outright to the purchaser. Instead the purchaser is granted the right to use it as laid down in the user licence. It is normally expected that only one person at a time will have access to and use the software concerned. A network licence may be purchased, normally at a reduced rate, for a defined number of users. A site licence may be available to cover all (unlimited) users within the premises.

It is thus illegal to make copies of software without the copyright owner's consent, or to duplicate software loaded on a hard disk for use on any other personal computer unless allowed for under the licence.

Anyone convicted of an offence under this act can expect a fine of unlimited amount plus a prison sentence ranging up to a maximum of 2 years.