The Royal Grammar School

ACCEPTABLE USE OF ICT SYSTEMS AND LEARNING GATEWAY
(POLICY DOCUMENT)

Prepared by:	**Senior Team**
Copy to:	**All RGS Students**
Date:	**June 2017**
Review date:	**June 2018**

Introduction

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

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

This policy encompasses all students and working practices under the responsibility of the Royal Grammar School, including Fraser Youens Boarding House. There are additional specific Boarding House guidelines relating to the use of ICT.

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 may be a criminal offence.

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of the Royal Grammar School's data, the Authorised Learning Gateway User's data and the individuals to whom the Learning Gateway data pertains. In particular, these risks arise from:

- The intentional or unintentional disclosure of login credentials to the Royal Grammar School Learning Gateway system by authorised users
- The wrongful disclosure of private, sensitive, and confidential information
- The exposure of the Royal Grammar School to vicarious liability for information wrongfully disclosed by authorised users

Data Access

This Policy aims to ensure all relevant aspects of the Data Protection Act (1998) and Fair Processing Policy are adhered to.

Scope

This Policy relates to the use by School students of all the School's IT and communication systems, including the Learning Gateway, telephones, mobile telephones, facsimile machines, computers (including laptops and mobile devices), e-mail and the internet. It also relates to the monitoring of all the above by the ICT Management Team.

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 ICT systems will be considered a disciplinary issue. This Policy applies to all students who use the School's ICT 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 ICT staff may look at any files and communications to ensure that the system is being used responsibly
5) ICT 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:

- Use of another person's username and password
- Trespass in the folders, work or files of other people
- Hacking with or without 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
- 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. Outside lessons, your parents bear responsibility for such guidance, as they do with other information sources such as television, telephone, cinema, radio, newspaper, magazine and other potentially offensive media
- 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 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
- Change your password at regular intervals – at least once a term and using a minimum of **eight** characters, including numbers and letters
- Do not use your own name or username as a password, for example *smith123*
- 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 Learning Gateway or school based cloud storage.
- You must not trespass in 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 program. 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 ICT 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 ICT staff immediately
- You may not take 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

Email

- 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 ICT 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 individuals or internet web-sites including social networking sites such as Facebook
- If you receive any such messages from outside the School you must report them to your Form Tutor, your Head of Year or the ICT Manager. You must not forward them either within or outside the School
- If you send emails of the type described above this will be considered a disciplinary offence and treated accordingly

Monitoring

- Searches on the internet and web addresses are monitored. The ICT 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:
    - 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 on the network server. This means that you can access your work from any network station
- To reduce the chances of the server hard disk filling up and crashing the whole network, the amount of disk space for each user is limited to 750MB. Overflowing this limit will cause you to be locked out until you have deleted sufficient files or moved them to a memory stick

- 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 (anyone excluding ICT Management team) attempting to do so will be in breach of the Computer Misuse Act
- An automatic and regular search will be made for any executable or compressed files (including 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, the authorities will be notified and appropriate action will be taken

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 rules. If you attempt to access sites blocked by the Firewall you are in breach of the school policy. Where a site is blocked and is required for school work, the ICT staff may be requested to ask for the site to be unblocked

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 if 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 must not connect or attempt to connect any device such as a laptop, mobile device or a personal music player or any gaming device to the network 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 school work is brought in fully charged. There are no charging facilities at school

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.

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 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.

Royal Grammar School
Amersham Road
High Wycombe
HP13 6QT

Telephone: 01494 524955