Student Online Safety Policy

September 2019

Responsibility for updating this policy: Deputy Head

New students will be given a talk on the use of laptops and appropriate use of technology in the first few weeks of being at Rugby. They will also be asked to sign to confirm that they are aware of this Acceptable Use Policy, that it is available on Firefly and that they agree to abide by it.

This policy applies to the use of technology on School premises and also any use, whether on or off School premises, which affects the welfare of other students or where the culture or reputation of the School are put at risk.

Rugby School's ICT and related Systems are important and essential assets which need to be appropriately protected. The School is concerned with establishing a framework of acceptable usage and controls, including student responsibilities, in order to safeguard our ICT hardware, systems, infrastructure and data from:

- unauthorised access
- accidental or intentional damage
- interruptions to availability of services
- use for illegal purposes or in contravention of the Guidelines for Life at Rugby School

The aims of this policy are to:

- encourage students to make good use of educational opportunities presented by access to the Internet and electronic communication
- to safeguard and promote the welfare of students by preventing "cyberbullying" and other forms of abuse
- minimise the risk of harm to the assets and reputation of the School
- help students take responsibility for their own e-safety
- ensure that students use technology safely and securely.

Linked Policies

Discipline and Rewards Policy

Anti Bullying Policy

Guidelines for Life at Rugby School

Student Manual

Procedures

Students are responsible for their actions, conduct and behaviour online in the same way that they are responsible at all other times. Use of technology should be safe, responsible and legal. Expulsion is the likely consequence for any student found to be responsible for material on his or her own or another website or social medium or any other electronic material that would be a serious breach of School rules in any other context. Any misuse of the Internet or any electronic media will be dealt with under the Guidelines for Life at Rugby School, the Student Manual and the Discipline and Rewards policies of the School. Examples of misuse and likely disciplinary action and sanctions are set out in the Appendix. Any misuse should be reported to a member of staff as soon as possible.

Students must not use their own or the School's or any other technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-bullying Procedures and other discipline policies. If you think that you might have been bullied or if you think another person is being bullied, talk to a member of staff about it as soon as possible.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's Child Protection Procedures. If you are worried about something that you have seen on the Internet or on social media, talk to a member of staff about it as soon as possible

Sanctions

Where a student breaches any of the School's protocols, the Governors have authorised the Head Master to apply any sanction which is appropriate and proportionate to the breach including, in the most serious cases, expulsion. Other sanctions might include rustication, increased monitoring procedures, detention or the withdrawal of privileges.

Unacceptable use of electronic equipment could lead to confiscation and other disciplinary sanctions in accordance with the rules set out in this policy, the Guidelines for Life at Rugby School, the Student Manual and other School Discipline and Rewards policies. See also the School's policy on the searching of electronic devices in the Appendix to the Discipline and Rewards policy.

E-mail and the Internet

These communications facilities are provided as essential teaching and learning tools and we encourage all our students to use these tools effectively and appropriately in support of their work.

Your Rugby School e-mail account is provided primarily to enable you to communicate with other members of the School.

When using e-mail you must ensure that you do not create, access, or pass on material that is obscene, sexually explicit, pornographic, racist, homophobic, defamatory, hateful, bullying, incites or depicts violence or terrorist acts or is otherwise inappropriate or represents values which are contrary to Rugby School's ethos. Rugby School e-mail is routinely monitored for such activity by the IT Services Department.

All incoming and outgoing electronic data will be monitored for inappropriate content and threats such as computer viruses and other potentially harmful programs.

The use of e-mail services, other than that provided by Rugby School, is not supported from within the School.

The Internet is provided as a resource in support of your studies. All Internet activity is monitored and logged. Attempts to access or download material from obscene, unlawful, violent, abusive or similar sites deemed inappropriate for a School environment will be punishable under the terms of the Guidelines for Life at Rugby School, the Student Manual and the Discipline and Rewards policies.

Students must not use unauthorised VPNs to circumvent the School's monitoring and filtering systems. Any use of such VPNs without the written consent of the IT Services Manager would constitute a serious disciplinary offence and would probably lead to rustication and a final warning.

Security and Confidentiality

It is essential that our computer systems and data are secure. To help achieve this Rugby School requires students to be aware of the need to protect IT equipment and data from actions and misuse which could affect the confidentiality, integrity and availability of our systems and data.

Security of IT applies to the use of the IT hardware and facilities which are either supplied by Rugby School or in the use of personal equipment authorised for use on the systems (both on and off the premises).

4G

Accessing the Internet on a School laptop or other device using a 4G connection presents a major threat to Rugby School's network security. The use of such connections is prohibited.

Passwords

At the core of all data security is the passwords you may require to access the network and related systems. If you have been issued with a name/password to access resources on the network:

- The password should be changed at the first opportunity (if the system permits)
- Passwords must be a minimum of 6 characters and should include letters and numbers
- Personal passwords should never be shared with friends
- Students have the responsibility to safeguard their passwords and change them regularly to avoid breaches in security and immediately if they suspect they may have been compromised.
- Students are entirely responsible for all activity that occurs using their log-in and must, therefore, safeguard their credentials.

Security of Hardware

Access to IT systems must only be made via your authorised user account and password.

Accounts should never be left open whilst unattended and users must always log off when finished. This will then require a password to be entered before the computer can be used again and guard against unauthorised access.

At the end of the working day you must log out of your computer and shut down for security.

You must not use another person's account for any reason. Impersonating another person online is a serious offence and would probably result in rustication and a final warning.

Portable devices must be secured (in a locked cupboard or by a 'Kensington' type security cable) when not in use (even in a locked room).

You must not attempt to move, re-configure, or alter the cabling on computer hardware or peripherals without the authority and assistance of an IT Technician. To ensure compatibility with, and the security of, our systems, personal and other equipment which has not been purchased through the School Laptop Scheme or the IT Department may only be connected to computer systems or the network (wired or wireless) with the prior authority of the Information Systems Manager and inspection/configuration by an IT Technician. The equipment may be required to meet minimum standards before connection is undertaken.

To avoid potential conflicts or interference with School systems, software which has not been purchased through, or provided by, the IT Department may not be installed on School computer systems without the authority of the Information Systems Manager.

General

Students are welcome to use their own laptops and mobile devices but these should only be connected to the School's network. Please contact the IT Services for further information. See the Guidelines for Life at Rugby School and the Student Manual for the rules about the use of mobile electronic devices including mobile phones.

All activity on the School's computing facilities is monitored which will alert IT Services to any breaches of this policy.

For reasons of safety and security and so students pay attention to their surroundings and those around them, the use of mobile devices is prohibited when moving around the campus. A Minor will be awarded to any student who uses his / her mobile device when moving around the streets that run through the School campus or around the School buildings.

Social Media

Social media are powerful allies and appropriate use is encouraged. Inappropriate use of social media, by whatever means, will be dealt with severely, under the terms of the School's Anti-bullying Policy and under the terms of this AUP. Such misuse may include, although is not restricted to, impersonating another person online, malicious or defamatory posts or messages and any action which is designed to undermine or defame another member of the School community.

Youth Produced Sexual Imagery (Sexting)

Students must not send indecent images of themselves, or other students, to another person, whether they are at Rugby School or not. Doing so may constitute a criminal offence. If students commit such an act, it is likely that the local statutory authorities will be consulted and a School disciplinary sanction will be applied. Local statutory authorities include the Police Service and the Warwickshire Safeguarding Children Board, although this list is not exhaustive.

Monitoring and review

The Deputy Head has responsibility for reviewing this policy and in doing so, will consider any e-safety incidents that have occurred.

Authorised Compliance and Risk Committee:	
Date:	**25 September 2019**

Appendix Examples of misuse and disciplinary action and sanctions

The information below is intended to indicate potential reactions. The SMT reserves the right to adjust these punishments according to the severity of the misdemeanour.

	Offence	First offence	Second offence	Further offences
R1	Insecure password or computer (leaving a laptop or desktop logged on, unattended, or unsecured).	Network account password changed by IS Manager.	Network account restrictions. 1 week gating.	Network account restrictions. Gating (2 weeks). Letter home (Deputy Head).
R2	Unauthorised connection of hardware to the network (wired or wireless).	Warning and inspection and configuration by IS staff.	Restriction of network account until the equipment is inspected and configured.	Confiscation of equipment.
R3	Altering the software or hardware configurations of School equipment without authorisation.	Saturday detention.	1 week gating and letter home.	Rustication and final warning.
R4	Misuse or abuse of the network resources.	Saturday detention.	1 week gating and letter home.	Rustication and final warning.
R5	Sharing of inappropriate personal electronic/digital resources, such as pirate movies, pornography etc.	Restriction of account and Inspection and wiping of affected devices. Referral to Deputy Head. Possible action taken under the Child Protection and Safeguarding, Anti-bullying and Discipline and Rewards policies.		
R6	Deliberate distribution of computer viruses or similar malicious programs.	Restriction of account and Inspection and wiping of affected devices.	1 week gating and letter home.	Rustication and final warning.
R7	Attempting to gain access to unsuitable Internet site.	Restriction of account and Inspection and wiping of affected devices.	More severe restrictions on Internet access for 1 month. Saturday detention. Letter home.	Rustication and final warning.
R8	Use of abusive, offensive, racist, homophobic, defamatory, aggressive or vulgar language in emails, messaging, online posts or other means of electronic communication.	Will be dealt with under the Anti-bullying and Discipline and Rewards policies. Punishments range from gating to rustication and final warning.		
R9	Use of webcams or any other device to record still or video images of students or staff without their prior consent.	Will be dealt with under the Anti-bullying and Discipline and Rewards policies. Punishments range from gating to rustication and final warning.		

R10	Storage of inappropriate files: a) in network space b) on laptop drive c) on other storage device	Gating (1 week). Referral to the Deputy Head if very serious. Deletion of files	Gating (2 weeks). Referral to the Deputy Head. Letter home (Deputy Head)	Rustication and final warning.
R11	Impersonation of another person online or an e-mail. The use of another person's social media account.	Sanctions will reflect the severity of the offence and its consequences and may, in extreme cases, include expulsion. The Head Master reserves the right to act accordingly		
R12	Distribution of inappropriate material (e.g. via e-mail attachments) including unauthorised images/movies.	Letter home from Deputy Head. Gating (1 week).	Gating (2 weeks) with warning of rustication. Letter home from Deputy Head.	Rustication and final warning
R13	Attempting to gain access to unauthorised network areas or resources ('hacking'); possession of software which could be used to aid unauthorised access. Use of a VPN to circumvent system restrictions.	Letter home. Account restrictions. Possibly rustication.	Rustication and final warning.	Probable expulsion
R14	Intimidation, harassment or bullying by use of emails, text messaging, recorded images or any means of electronic communication.	Students should be aware that depending on circumstances the use of any form of electronic communications to intimidate, degrade or bully any member of the community, could result in immediate rustication and a Final Warning, or in extreme cases expulsion. The School Anti-bullying and Discipline and Rewards policies will also apply.		
R15	Sharing or distribution of recorded or live images or videos, or the use of such images to intimidate, harass or bully.	Students should be aware that depending on circumstances the use of any form of electronic communications to intimidate, degrade or bully any member of the community, could result in immediate rustication and a Final Warning or in extreme cases expulsion. The School Anti-bullying and Discipline and Rewards policies will also apply.		
R16	Bringing the School into disrepute through inappropriate use of electronic media.	Sanctions will reflect the severity of the offence and its consequences and may, in extreme cases, include expulsion. The Head Master reserves the right to act accordingly.		
R17	Using a mobile device in the street or around the campus	A Minor should be issued. If the offence becomes frequent, the device may be confiscated by the Hm.		
R18	Production, distribution or sharing of youth produced sexual imagery of any kind.	The local statutory services will be consulted and a sanction applied. The severity of the sanction will be decided by the Deputy Head or Head Master, but will be on a scale from gating to expulsion, depending on the seriousness of the offence and its effect on others. The statutory authorities may also take action against the perpetrators.		