Student Acceptable Use Policy

Action	Policy to be reviewed annually		
	Owner	**Date**	**Completed**
Reviewed	Assistant Head, Teaching, Learning & Innovation	April 2023	✓
Approved	Education Committee	9 May 2023	✓

To be published on the following:	
Staff Portal	✓
Student Portal	✓
School website	✓

ST PAUL'S
GIRLS' SCHOOL

Student Acceptable Use Policy

Who this policy applies to

This policy applies to all students at the school.

What this policy is for

This policy extends the principles and expectations set out in the school's behaviour policy and sets out the rules for online behaviour and the acceptable use of the school network.

Legal framework

- Keeping Children Safe in Education

Other relevant school policies

- Behaviour policy
- Online Safety Policy
- Anti-bullying Policy
- Mobile Phone Policy
- The school's privacy notices

Content of policy

1. Introduction

1.1 The school network and the internet provide valuable tools to support learning and the school recognises that social networks and digital communication are an integral part of how many of us socialise and interact.

1.2 The points below are designed to ensure that the network remains available and safe for the whole school community.

1.3 All users of the network (whether using school or personal equipment on the school network and systems) are expected to use their common sense and follow all laws, rules and regulations.

2. Awareness and acceptance of AUP

2.1 You are required to agree to the terms of this Acceptable Use Policy (AUP) at the beginning of each academic year to indicate that you have read, understood, and accepted the policy, and the policies referred to by the AUP. Access to the school network and IT systems is subject to the terms & conditions outlined in this policy.

2.2 School tutors are expected to explain the AUP to their tutees and to give them the opportunity to ask questions before agreeing. Parents/guardians are asked to familiarise themselves with the school AUP and to reinforce this with students.

3. Enforcement of AUP

3.1 A breach of this AUP and listed policies will be dealt with in accordance with the school behaviour policy. In the case of a serious breach of this policy, parents/guardians may be contacted, and the matter may lead to suspension or further disciplinary action.

3.2 If online activity is found to be illegal, it may lead to a referral to the police and result in prosecution, such as in the case of hacking, data breaches, harassment or the creation and distribution of illegal images.

3.3 Where a member of staff suspects that an electronic device has been, or is likely to be, used to commit an offence or cause personal injury or damage to property, they may confiscate the device for examination by a member of the pastoral team. The member of the pastoral team may examine the device for any data or files where there is a good reason to do so in accordance with the school behaviour policy. They may also request that data is deleted if they think there is a good reason to do so. Parental consent is not needed to search through a student's mobile phone if it has been seized in a lawful 'without consent' search.

4. School Systems and Network

Use of school systems	You must only use school-approved systems. An up-to-date list of approved systems can be provided by the Director of IT upon request.
	You should take all reasonable precautions to prevent others from being able to use your account.
	You should only use your own school login and password to access school systems and equipment.
	You must not make changes to the content on the school network without permission from the owner of that content (Heads of Departments, SMT, or Heads of Year).
	It is forbidden to attempt to bypass the school internet filtering system or use unapproved virtual private networks (VPNs) to this effect.

	No unauthorised attempts should be made to circumvent the school security systems and controls, download or install unapproved software, nor access or delete school data, or damage school IT equipment or systems. This includes school laptops.
	The use of school systems is monitored, filtered and logged.
Passwords & Security	School usernames and passwords must not be shared with anyone else, nor written or recorded where they may be accessed by others.
	Passwords should consist of a minimum of eight characters with at least one capital and alphanumeric character.
	A password set for school systems should not be the same as that used on other personal accounts.
	Computers or laptops must be logged off or locked when unattended (hold down the Windows Key and press 'L'). If you come across a school computer that has been left logged in by another user, you should immediately sign out of the account and not attempt to access their files and data.
Data Storage	Students are provided with personal data storage as part of their login which is accessible from both inside and outside of school. This must be used for schoolwork and school data.
	Advice should be sought from the Director of IT if the need for storage other than on the school network is considered necessary. Encrypted USB drives may be brought into school but should be used with caution as it may include viruses or other malicious software. To ensure that network security is not compromised, the IT team may ask to see such media and may disable it for use on the network if they believe that network security may be or may have been compromised.

5. Online Behaviour, Safety and Social Media

Online Behaviour – General Principles	Online activity, both in school and outside of school, should be respectful, responsible, appropriate and sensible and must not cause the school, its staff, students, or others distress, nor bring the school into disrepute.
	Students must understand that online activity has real-world consequences.
	Access should not be attempted to internet sites or content that is illegal, violent, or considered offensive (for example material that is racist, sexist or that promotes violence, hate, terrorism, religious extremism, radicalisation, or discrimination), or that undermines fundamental British values (democracy, the rule of law, individual liberty, and mutual respect for and tolerance of those with different faiths and beliefs, and for those without faith).
	Aggressive or offensive material must not be uploaded to, or downloaded from, the internet at any time (for example material that is racist, sexist or in any way discriminatory or liable to incite violence or hate crimes).
	No distribution by email or online posts of indecent, obscene, or offensive information, material, or images on the network or internet that may (or has the intent to) harass, insult, attack, discriminate, prejudice, threaten or cause offence to students, staff or others (whether inside or outside the school). Such action may be viewed as cyberbullying, which is strictly forbidden and will be sanctioned appropriately.

	Online posts outside of official school-controlled outlets must not be generated using the St Paul's name, or branding. Nor should posts be construed as generated by, published for, or speaking on behalf of the school, without explicit and written consent from the Director of Communications. Posts should only be published by a supervising member of staff i.e., the relevant supervising member of staff for that channel. This includes social media posts, whether public or private facing, website pages, online channels, or apps.
	School rules and policies still apply when posting content anonymously~~.~~
Online Safety – General Principles	Personal information should not be shared online such as a home address, location, telephone number, password or any other personal information while online, without the permission of a member of staff responsible for your online safety. You must also not share the personal details of any other students or members of staff without their permission.
	Retaliation or reply to offensive emails or messages should be resisted, but such communications should be reported and blocked.
Social Media and online channels	Students must not attempt to contact staff through social media or non-school-approved channels.
Email	School email addresses must be used for login and registration for all school-related matters. Home or personal email addresses must not be used to create accounts for school-related matters or to communicate directly with staff.
	Messages/communications should not be re-sent or forwarded without the consent of those involved and care should be taken to not disclose personal contact information (e.g., personal student email addresses) when forwarding messages to staff.

6. Online Resources

When using approved online resources, the conditions of approval must be followed.
Only school email addresses should be used to create online accounts.
Only the minimal personal data required should be entered. For example, if it is optional to enter your date of birth, do not enter it.
The content or terms of use of approved resources may change without warning or notification. You should therefore apply your judgment when accessing resources and report any concerns using the online reporting form accessed via the portal.
When using online resources, it is your responsibility to use that resource responsibly and abide by any Terms of Use of that resource. If you need any help with understanding what these are, you should speak to your tutor or a senior member of staff.
For external accounts relating to school matters, do not use images of yourself for profile pictures.
If the online resource includes access to a forum, blog, or other types of chatroom, this must not be used unless specifically approved.

When (and only if) chatrooms associated with these accounts are approved for use, the other guidelines set out in this policy must be followed (for example, do not give out personal information, do not post anything that will cause others offence and distress, and report any messages that cause you offence).
Be aware that any links in a recommended online resource that leads to a third-party website may not necessarily have been approved and should not be followed without seeking advice from the appropriate member of staff.
When online video clips are used, only the specified clip should be viewed and not any other linked or recommended clips (unless specifically approved).

7. Using Your Own Devices in School

During lessons, devices must only be used for educational purposes as directed by class teachers.
Devices must not be used to record lessons without the teacher’s explicit and written (or email) permission, agreed by the appropriate Head of Department for school or educational purposes.
For MIV – VI, students are expected to conduct their schoolwork through their school 1:1 laptop.
For students in the Senior School, the school permits the use of personal laptops/tablets (BYOD) under conditions outlined in the policies listed above.
Rules, policies and guidelines applying to school equipment also apply to personal devices when brought to school.
When on school premises, students must only access the internet through the school WiFi using their school login and password. The use by students of personal data plans, e.g., tethered 4G/5G mobile networks, for access to the internet while in school is expressly forbidden.
The use of mobile phones in student toilets or changing rooms is forbidden. This is to protect the privacy and welfare of other students.
Additional conditions for the use of mobile phones by students are set out in the Mobile Phone policy.

8. Capture, storage and publication of images/recordings

The capture, storage, and publication of images or recordings for schoolwork must only be done on school devices, with school approval and following the instruction of the member of staff leading the activity. Imagery accidentally captured to the personal storage area of personal devices must be deleted permanently and immediately from the device. The only permissible exception to this is the use of mobile phones, providing permission has been granted, to scan written work to upload to a digital platform (e.g., OneNote or MS Teams).