School Acceptable Use Policy

Action	Policy to be reviewed annually		
	Owner	Date	Completed
Reviewed	Ellis Whitcomb	May 2021	✓
Approved	Board of Governors	23 June 2021	✓

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

ST PAUL'S
GIRLS' SCHOOL

1. Introduction

1.1 This policy extends the principles and expectations set out in the school behaviour policy (for students) and the staff code of conduct (for staff) and should be read by staff, students and parents/guardians in conjunction with the following:

- Online Safety Policy
- Anti-bullying Policy
- Mobile Phone Policy
- The school's privacy notices
- AUP Staff Supplement (staff only, including teaching and non-teaching staff, governors, and regular volunteers)

1.2 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.

1.3 Any large computer network is a highly complex system requiring a considerable amount of upkeep and maintenance. The points below are designed to ensure that the network remains available and safe for the whole school community. 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 school standards, rules and regulations and the law of the land.

1.4 At St Paul's we aim to encourage a sense of responsibility for ourselves and others and this encompasses not just how we behave in the real world but also how we communicate online and use technology responsibly.

1.5 When using the school network, systems, and equipment, users should be aware that our network, school systems and internet access is logged and filtered to avoid access to harmful or offensive material.

1.6 The rules and guidelines set out below should be followed when using school equipment and systems, when using your personal device in school and for school matters, and when representing St Paul's in general. Keep in mind that, even when using personal social media, private/public blogs, and online forums, you may still be representing the school and, therefore, guidelines for such situations are included in this policy despite being discouraged for schoolwork.

2. 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 the school AUP and listed policies will be dealt with in accordance with the school behaviour policy or staff code of conduct and may lead to disciplinary action. In the case of students, parent/guardians will be contacted. In the case of a serious breach of this policy, an investigation into misconduct may lead to suspension or further disciplinary action.

3.2 For staff and students, if online activity is found to be illegal it may lead to 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 or staff code of conduct. 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 though a student's mobile phone if it has been seized in a lawful 'without consent' search, and its use is prohibited by the school rules, or is reasonably suspected of being, or likely to be, used to commit an offence.

4. School Systems and Network

	To be followed by Staff & Students	**Information for Parents/Guardians**
Use of school systems	Approved school core systems include: ▪ Microsoft Office 365 (Outlook, Teams, OneNote, OneDrive and Sharepoint portal pages for example and the Microsoft productivity suite: Word, Excel, PowerPoint etc) ▪ Zoom cloud meetings (using school logins) ▪ School portals ▪ iSAMS ▪ CPOMs An up-to-date list of approved systems can be provided by the Director of IT upon request.	Parent/guardian resources are made available on the parent portal through their individual logins. Parents/guardian logins must not be shared, including with students, and are subject to the same security expectations as student account logins and passwords (outlined in this policy). Parents/guardians should only use the email accounts registered with the school for school communications.
	Each user of school information systems and equipment is responsible for their individual account and that they should take all reasonable precautions to prevent others from being able to use their account.	
	Only the user's own school login and password should be used to access school systems and equipment.	
	Software must not be downloaded or installed on school equipment without explicit, written permission from the Director of IT.	
	Changes should not be made to 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, nor use unapproved virtual private networks (VPNs) to this effect.	
	No unauthorised attempts should be made to circumvent the school security systems and controls, nor access or delete school data, nor damage school IT equipment or systems.	
	The use of school systems is monitored 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.	
	The school has a password policy which requires a certain level of complexity 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.	
	The school will never send an email requesting its members' school passwords or account details.	
	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 the account and not attempt to access their files and data.	
Data Storage	Students and staff are provided with personal data storage as part of their login which is accessible from both inside and outside of school and are therefore required to make use of this technology for schoolwork and school data. The use of USB storage or other storage devices is no longer supported, and the facility will be disabled.	
	Advice should be sought from the Director of IT in the event that 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 the media 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.	
Use of school printers	The use of school printing services must be in accordance with the following: o Consideration on the environmental impact and cost implications of printing. o Defaults are black & white and duplex (double sided printing) which can be overridden at time of print/copy. o Reasonable print quotas may be imposed. o Printouts must not be left unattended on photocopiers/printers/scanners.	
	Limited personal printing is permitted in exceptional cases and on an occasional basis.	

5. Online Behaviour, Safety and Social Media

	To be followed by Staff and Students	**Additional requirements specifically applicable to students**
Online Behaviour – General Principles	All communication with students, staff, or others associated with the school are responsible, appropriate, and sensible.	Students must understand that online activity has real-world consequences.
	Online activity, both in school and outside of school, should be respectful and must not cause the school, its staff, students, or others distress, nor bring the school into disrepute.	Online content must not be generated using the St Paul's name, or branding, nor that can be construed to be generated or published by the school, without explicit and written consent from the Director of Communications and only with a supervising member of staff. This includes social media posts, whether public or private facing, website pages, online channels, or apps.
	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).	Copyright must be respected and it must be understood that submitting work downloaded directly from the internet without proper acknowledgment may invalidate my academic work and the assessment of my work (see the plagiarism policy).
	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 to harass, insult, attack, discriminate, prejudice, threaten or cause offense to students, staff or others (whether inside or outside the school). Such action may be viewed as cyberbullying, which is strictly forbidden.	
	School rules and policies still apply when posting content anonymously~~;~~	
Online Safety – General Principles	Personal details must not be published online of students or members of staff without their permission.	You are encouraged to seek advice if you are concerned, uncomfortable or upset by something that may have happened to you or other members of the school community online, or by something you yourself may have done. If anything online causes discomfort, concern, or distress

		this should be shared with an appropriate member of staff (via parents or tutors) without being blamed.
	Retaliation or reply to offensive emails or messages should be resisted, but such communications should be reported and blocked.	Personal information should not be shared online such as 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.
	Staff and students should be aware that people online may be untruthful about their identity, intentionally seek to cause them harm or to spread violent or extremist views through radicalisation.	Students should avoid excessive or addictive online and digital behaviour.
	Those who seek to promote terrorism or religious extremism may attempt to contact or recruit young people via the internet and such activity must be reported.	Students should know how to report a concern to a designated safeguarding lead (DSL), appropriate members of staff, parent or a trusted third party, for example the Police (Child Exploitation and Online Protection unit, CEOP). See section on *further information* at the end of this policy.
Social Media and online channels	While social media is not permitted for schoolwork without authorisation by the Director of Communications, the school expects profiles for its staff and students to be checked regularly and set to the highest levels of privacy for the benefit of its wider community.	Students are expected to inform parents/guardians of all social media platforms being used for personal use and for parents/guardians to check the appropriate age-restrictions and privacy settings are in place and that the school is not being represented or brought into disrepute.
	Staff and students must not run online network spaces, pages, blogs or channels that could be confused with school approved channels. (See Online Safety Policy relating to public facing online resources)	Students must be aware that that social media or online channels that can be identified as associated with school-aged students can attract unwelcome attention and can endanger accounts associated with these channels through follow-lists and related activity.
		Only verified contacts should be added to friends/follower lists and caution should be exercised when communicating with contacts that are only known to you online (informing a member of staff responsible for online safety, via a parent if appropriate). Be aware that it is very easy to impersonate an account name online – check, before accepting and never accept from strangers.
	Staff and students must not attempt to contact each other through social media or non-school-approved channels.	Students should understand that being asked for secrecy by online contacts can support/encourage grooming and that,

		therefore, to remove secrecy by sharing online experiences with friends and family can prevent online harm and abuse
	Staff and students should be aware that people online may be untruthful about their identity, intentionally seek to cause them harm or to spread violent or extremist views through radicalisation.	Students must be aware that entering online chat, forums and channels can expose the individual or school community to strangers.
		Students must not arrange to meet someone in person who they only know online without a parent/guardian being present.
Email	School email addresses should be used for login and registration for all school matters. Home or personal email addresses must not be used	No 'spamming' or bulk emailing.
	Email folders must be regularly checked and emails that are no longer needed deleted.	Privacy should be respected when messaging or communicating with others and that messages/communications should not be re-sent or forwarded without the consent of those involved.

6. Online Resources

To be followed by Staff and Students	**Additional requirements specifically applicable to students**
When using approved online resources, the conditions of approval must be followed.	Do not use images of yourself for profile pictures.
Only school email addresses should be used to create online accounts.	If the online resource includes access to a forum, blog, or other type of chatroom, this must not be used unless specifically approved.
Only the minimal personal data required should be entered. For example, if it is optional to enter yours or the student's date of birth, do not enter it.	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).
All users should be aware that any online resource approval process may be fallible if third-party resources change without warning or notification. In view of this users should apply the best of their judgment on accessing resources, reporting any concerns using the online reporting form (to report safeguarding, data protection or technical concerns).	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 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, students should	When online video clips are used, such as YouTube, only the recommended clip should be viewed and not any other linked clips (unless specifically approved).

speak to their tutor, or a parent and staff should speak to their HoD.	

7. Using Your Own Devices in School

To be followed by Staff and Students	**Additional requirements specifically applicable to students**
For staff, the Senior School and VI, the school permits the use of personal laptops/tablets (BYOD) under conditions outlined in the policies listed above and in which students may use their own personal devices for schoolwork.	The school network is configured to provide safeguarded, secure, and robust systems to support teaching & learning at school. The condition for bringing personal devices onsite is that individuals must only access the internet through the school WiFi using their school login and password.
Rules, policies and guidelines applying to school equipment also apply to personal devices when brought to school.	*The use by students of personal data plans, for example 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.	For MIV – V, students are expected to conduct their schoolwork through their school 1:1 laptops: • Laptops are required in all lessons. • Laptops are expected to be charged overnight. • Laptops should be looked after, properly maintained, clearly labelled, and kept in a protective sleeve. • Faults in laptops are expected to be reported to IT immediately, and a reserve laptop signed out from the library. • Laptops should be restarted at least once per week to allow critical updates to take place (it is encouraged to do this overnight while on charge, to avoid delays in school during upgrades) (the majority of IT support requests are overcome by a restart and system update). • Students are expected to manage their battery status and notify teachers when they need to connect to charge their laptops in good time during lessons.
The use of personal devices in school is entirely at the owner's risk and it is up to individuals to ensure that their device is not damaged, lost or stolen.	Conditions for the use of mobile phones by students is set out in the Mobile Phone policy, but for clarity: no mobile phones, nor headphones of any sort, are to be used in corridors or common parts except where explicitly permitted for each year group.
The IT department is available to support connection to the school network and access to school systems such as the portal and email but cannot provide support for personal devices or services.	Devices must only be used in lessons for educational purposes as directed by class teachers.

Nothing that is inappropriate or potentially illegal may be downloaded or saved onto devices brought into school, and all students and staff must be aware that sharing, publishing, or transmitting such material may be a crime and a matter, therefore, for the police.	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.
	Personal devices must not be used to capture images or recordings without the express permission of the individual(s) being photographed/recorded and should be deleted if requested. See section below.
	Failure to follow these rules may result in the confiscation of devices and the individual or group withdrawal of permission to use personal devices in school.

8. Policy for Students on the Capture, storage and publication of images/recordings

8.1 Staff guidance on the use of images of students is set out in the AUP Staff Supplement.

8.2 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.

8.3 The capture, storage, and publication of images/recordings during break and for personal reasons must follow the principles that the image/recording/posting:

- is taken with the consent of those involved
- is not clandestine
- is for legitimate and appropriate purposes only
- is not published to social media or the internet in any form that is recognisably associated with the school, nor without the express consent of those involved
- is deleted and/or removed if requested
- is within the rules and guidelines of school policies.

For total clarity:

- images and recordings captured in school premises and on school business (e.g., school trips) must not be held on personal devices (e.g., mobile phone photo/video libraries), except where authorised in writing by an appropriate member of staff
- particular care should be taken if recording images of anyone in clothing other than normal school dress (e.g., sports kit or costume drama). It is never acceptable to record images where students may not be fully dressed (e.g., backstage in drama productions or changing rooms or sports venues).

9. Parental/guardian responsibility for students

9.1 Technical barriers can never entirely protect a student from harmful online content. Parents should be aware that whilst the school network and IT facilities are configured to support a safe and secure environment in which to learn, the same protection is not in place when using other networks, including those at home and personal data plans.

9.2 Students' mobile phone contracts are not (and cannot be) the responsibility of the school. Smart phones are likely to have an internet connection (sometimes referred to as a data, 3G, 4G or 5G connection, for example) which may not have any content filtering in place and could, therefore, be used for unconstrained access to the internet.

9.3 Parent/guardians are expected to ensure that internet access and social media usage through personal devices and mobile contracts is appropriate to the student's age and should also be responsible for giving guidelines to students about the amount of time spent using their devices.

9.4 Whilst the school takes the actions described above to ensure that the school community understands the importance of safe behaviour online, the school cannot be held responsible for inappropriate online behaviour that bypasses the school network. In light of this, **parent/guardians must also be responsible for ensuring that students they are responsible for use technology in a safe and secure way and behave responsibly when online.** The full range of school disciplinary procedures will be considered in the event of any breach of this policy or the school behaviour policy.

9.5 Both the school and parents have a responsibility to ensure that students have the knowledge and confidence to know what to do if they encounter content or receive communications that make them feel uncomfortable, worried or upset and are able to share their concerns in an open and supportive environment.

10. Further information

10.1 The school recognises that technology is constantly evolving, and that social media has become an integral part of how young people socialise and interact. This can be a confusing and daunting area for parents to get to grips with and it can be difficult to understand how your daughter is using the internet.

10.2 We encourage you to familiarise yourself and to explore some of the online resources for parents given below.

- CEOP (Child Exploitation & Online Protection Command) - https://www.thinkuknow.co.uk/
- NSPCC ChildLine - http://www.childline.org.uk/explore/onlinesafety
- BBC Webwise - BBC - WebWise
- Childnet - http://www.childnet.com/parents-and-carers
- ParentZone https://parentzone.org.uk/