Staff acceptable use of IT policy

This policy applies to staff, peripatetic teachers and coaches, volunteers and any adult accessing school IT facilities in order to provide services to the School.

Action	**Policy to be reviewed annually**		
	Owner	**Date**	**Completed**
Review	Helen Semple	April 2019	✓
Reported	Education Committee	7 May 2019	✓
Approved	Board of Governors	25 June 2019	✓

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

Minor updates to reflect staffing changes made in August 2019

1.1 St Paul's Girls' School seeks to embrace the use of IT to enhance teaching and learning and the school's administrative processes. The aim of this policy is to ensure that:

- Information is readily available to the relevant users throughout the School
- Confidentiality is always maintained
- The integrity of the information is maintained
- Data access and use conforms to regulations in regard to the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.
- Undesirable consequences associated with breaches of information security are avoided. This includes but is not limited to; bad publicity, fraud and illegal use of personal data.
- Staff understand their responsibilities online to ensure the welfare and safeguarding of pupils.
- Staff understand the boundaries of acceptable behavior, to mitigate the risk of inappropriate communication taking place between staff and pupils and of having misplaced allegations being made against staff.

1.2 This policy applies when using school computers, using your own device connected to the school's wireless network and when representing St Paul's. Keep in mind that even when using social media and public blogs and forums you may still be seen as representing the school.

1.3 All staff and people offering services at the school who access school IT systems are required to read and comply with this policy. Failure to comply with the policy may lead to an investigation and hearing under the school's disciplinary policy, or other appropriate action.

1.4 This policy is also written in conjunction with *Keeping Children Safe in Education 2018 (Annex C).*

2. Responsible use of IT

2.1 Staff are expected to use School IT systems responsibly and primarily for the purposes of their job (see section 7 – Use of school IT facilities for personal use).

2.2 Staff should be aware that access to the network and use of systems such as email and the internet are not regularly monitored but may be reviewed in accordance with section 10 of this policy and staff access of blocked sites will be logged automatically by the system.

2.3 Staff must not attempt to browse internet sites or access content that is illegal, offensive or indecent. This includes content that is pornographic or that promotes violence, religious extremism or discrimination.

2.4 Staff must not upload or post aggressive or offensive material to the internet (for example material that is racist, sexist or in any way discriminatory or liable to incite violence or hate crimes) and must not upload or post any material to the internet that is likely to bring the school into disrepute.

3. Data protection and the GDPR

3.1 Staff should understand their responsibilities when accessing, using and sharing school data and only do so according to school policies and data protection legislation (refer to the Data Protection and Confidentiality Agreement which you signed when you joined the School and can be found on the Portal).

3.2 Unless otherwise stated all data and information relating to your work at the school (for example personal information relating to staff or pupils, work submitted by students, internal examinations, financial data or confidential minutes) must only be stored and processed on school computers and systems (e.g. iSAMS, the Portal, school email, CPOMS, school provided cloud storage and network drives).

3.3 Personal email should never be used for School work. When working from home staff should use school access to cloud storage or encrypted USB drives.

3.4 Staff should always ensure that their work cannot be overseen in a public space and should be particularly mindful when using systems containing sensitive personal information (e.g. medical, safeguarding, and SEN information) on iSAMS, email etc. in the presence of students, parents or visitors, particularly if the computer is connected to a projector.

3.5 If a member of staff is aware that school data, particularly staff or pupils' personal information, has been or could be accessed by an unauthorised source (e.g. due to loss of equipment containing data, unauthorised access to a school system, or information that has been transmitted to a third party in error), **they must inform the Director of IT and eLearning and the Bursar immediately who will decide whether the Information Commissioner's Office needs to be notified**. The school needs to notify the ICO of a reportable breach within 72 hours and swift action may enable a breach to be contained. It is therefore crucial that breaches are reported without delay, even during the school holidays.

3.6 Data stored on the school network is backed up regularly. Staff should, however, ensure that data on removable media and portable devices is also backed up.

3.7 When leaving a computer staff must make sure that they have logged off or that the computer is locked (hold down the Windows Key and press 'L').

4. IT security

4.1 The security of the School's IT systems is the responsibility of all staff and staff should follow the advice and guidance specified by the IT department (please see http://portal.spgs.org/itsupport/help/security).

4.2 Staff must only log onto school IT systems (including the Portal and email) using their own username and password.

4.3 Staff must not share their username and password with anyone else and should be aware that the IT department will never ask them for their password.

4.4 The School has a password policy which requires a certain level of complexity. Passwords should not be written down or stored in a location where they could be accessed by others. A password set for school systems should not be the same as that used on other personal accounts.

4.5 Staff must not make changes to the configuration of school IT equipment, including downloading or installing software, without first consulting the IT department.

4.6 Staff must not attempt to circumvent the school's IT security controls (including through the use of VPNs) or seek to gain unauthorised access to data.

4.7 Staff should not attempt to bypass the school's internet filtering system.

4.8 All IT equipment and software purchased for school use should be approved in advanced by the IT Department to ensure compatibility and security. Departmental IT requests should be submitted to IT through the usual bidding process before purchase.

5. Use of email (see also Appendix A)

5.1 The content of an email may constitute another person's personal data and therefore be disclosable under a subject access request in accordance with the GDPR. Similarly, any email may need to be disclosed in the case of legal action. Staff should therefore assume that the content of any email may be seen by others including the subject of the email.

5.2 Staff should remain mindful that email is not a secure form of communication. Other forms of communication should be considered for sending confidential or sensitive information, for example by sending such information in a password protected attachment or in an encrypted message. If in doubt, staff should seek advice from the IT department.

5.3 Consideration should be given to the number of emails sent, ensuring that all methods of online communication (e.g. the Portal) are used appropriately as an alternative. The total maximum size for attachments to an email is 25Mb, if you need to send larger files seek advice from the IT department.

5.4 Staff are asked to observe certain protocols so that the use of email does not become a disruption in the day to day working life of colleagues. The School's Email Protocol is attached at Appendix A.

6. Safeguarding and conduct with pupils

6.1 Staff should understand their responsibilities with regard to safeguarding (see the Safeguarding (Child Protection) policy) and understand that these also apply when using IT.

6.2 If you suspect that illegal content has been accessed using a school computer, or that a school system such as email has been used inappropriately contact the Director of IT and eLearning immediately. Do not attempt to access the content yourself as this could corrupt any evidence.

6.3 Pupil data, including photographs and audio/video recordings must only be stored on school systems and not posted/shared publicly without following school guidelines on the use of social media. Permissions are required from pupils (and parents) in certain circumstances and therefore staff should always assume that images and videos of pupils should not be shared publicly without prior permission and guidance from the communications team.

6.4 In accordance with the Staff Code of Conduct, staff should not give out their personal mobile, email or home telephone numbers to a pupil. School phones should be used on trips to avoid staff having to give out their personal phone number to pupils. If staff are

required to communicate with pupils using their own device, communication should be via the school email system. VMTs may give personal email addresses to parents as they are providing private lessons under the terms of the VMT handbook.

6.5 Photographs or audio/video recordings of students should only be taken using school equipment. Staff must not use their own cameras or phones or store photographs or audio/video recordings on their own computer or memory cards. School cameras are available to loan from the IT department.

6.6 Staff should always avoid any online (as well as offline) conduct that could be interpreted as a sexual advance or "grooming" and avoid words or expressions or any behaviour online (as well as offline) that could be interpreted as having any sexual innuendo.

6.7 Guidelines on the use of social media are outlined in the School's Social Media policy (see Appendix B).

7. Use of school IT facilities for personal use

7.1 It is understood that staff may occasionally need to use the School's IT facilities for personal, non-school related use. Such use should be kept to a minimum so as not to interfere with work and responsibilities and limited to break times or outside of school hours. Staff should also remain mindful that information or messages sent through school facilities may be attributed to the school. Personal views should be stated as such.

7.2 Staff may use printers and photocopiers for personal items on an occasional basis. However, these facilities are provided to users primarily for school related work.

7.3 Staff should not save personal files on the school network such as personal photos, music files etc. Disciplinary action may be taken if it is established that school IT facilities have been used to excess for personal use.

8. Use of personal devices in school

8.1 Staff may use their own personal devices (laptops, tablets or smartphones) in school on the understanding that the security of the device is their own responsibility and that the School accepts no liability if the device is lost, damaged or stolen.

8.2 Staff should be mindful of setting an example when using their mobile phones in the School and should not use their mobile phones for personal use during lessons or meetings.

8.2 Personal devices may be connected to the School's wireless network (called "SP-BYOD") in order to access the internet and school systems (see monitoring section below for details of how the school monitors access).

8.3 Personal devices should be password protected and have up to date antivirus software and security updates.

8.4 The IT department will help staff connect their device to the school's wireless network and access school systems such as the Portal and email but cannot provide support for the device.

8.5 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.

9. Social media guidelines

9.1 The School's policy on staff use of social media is available at Appendix B and forms part of this policy document. The policy outlines guidance on the use of social media and networking sites.

10. Monitoring

10.1 Any monitoring undertaken by the school will be conducted in accordance with the prevailing legislation and for the purpose of ensuring compliance with this policy, the staff code of conduct or where there is the possibility of unlawful activity.

10.2 Attempts to access blocked web content by students are regularly monitored in the school. Staff access of blocked sites is not monitored but is logged automatically by the system. These records may be accessed as part of an investigation where there is a relevant concern about a member of staff. Where sites are blocked that are required for legitimate work reasons the IT Department must be notified.

10.3 It is possible for the school to monitor email usage by staff. Other than where there is a concern that email is being abused, used for unlawful purposes or may provide evidence of other behaviour that would be counter to the staff code of conduct, email content will not be routinely monitored. Should monitoring of email content be considered necessary, the member of staff will be informed unless the police or other authorities advise otherwise.

10.4 If it is discovered that any of the systems are being abused and / or that the terms of this policy are being infringed, action may be taken which could result in dismissal, termination of employment or other legal action.

Email protocol Appendix A

Sending emails

Security and data protection:

- Email should not be used to send highly sensitive and confidential information. Either communicate this information face to face or send via an encrypted method. Information about pupils should be communicated via ISAMS or CPOMS if a pastoral issue.
- Assume that everything that you write in an email could be seen by others or by the subject of an email in the event of a subject access request. Always maintain a professional tone.
- Think carefully before "replying to all" and ensure that you want all the recipients to receive the message.
- Likewise look at an email chain carefully before you forward an email to ensure that there isn't information further down that you shouldn't be sharing more widely.
- If sending an email to a large group of people, it is almost always preferable to use the BCC function so that each recipient does not see who else is on the distribution list. The BCC function **must** be used if recipients wouldn't normally have each other's contact details (eg a group of new or existing parents).

General guidance:

- Before sending an email, consider the use of other school systems (e.g. publishing information on the Portal or sharing a document with colleagues via the group drive)
- Wherever possible, use face to face communication rather than email and avoid prolonged discussions on email that could be better dealt with face to face or on the phone
- Never write an email when you feel angry
- Avoid open questions on email, eg 'does anybody know what the policy is on…'
- Similarly, avoid sending an email to a number of people because there is uncertainty over who should be dealing with the issue. It is more efficient to ascertain who the appropriate contact is before sending the email
- Think carefully before copying emails to others. Line managers are responsible for passing on information to their direct reports as appropriate and therefore the sender does not need to do this for them
- There are no restrictions on when staff choose to work/send email but staff should be mindful of sending email outside of working hours and the expectation should not be for a necessary and immediate response. All urgent communication should be done by phone

Managing your inbox

- Conduct a regular housekeeping exercise to completely clear your inbox and do not keep emails for longer than needed.
- If an email contains sensitive personal information, transfer the information to another secure system (eg CPOMS) as your inbox is not an appropriate storage system for personal data.
- Set up an appropriate filing system to store and retrieve old emails
- Check email regularly but not obsessively
- If a message can be dealt with immediately, address it at once
- Once an email has been dealt with, delete it from your inbox or file it if it needs to be retained.

Fewer emails mean reduced stress, less time tied to your desk and more freedom to engage in personal communication with others which is often more effective.

Appendix B

Social Media policy

1. Purpose and scope of the policy

1.1 This policy applies to the use of social media for school business and sets out expectations for staff personal use, whether during working hours or at other times. Its purpose is to help staff avoid the potential pitfalls of sharing information on such social media sites and should be read in conjunction with the Staff Acceptable Use of IT policy. The policy applies at all times whether using school computers or your own device and both when in school or at home.

2. Introduction

2.1 The School recognises that the internet provides unique opportunities for sharing and communicating in both a personal and professional context. Staff are free to use social media such as Facebook, LinkedIn, Twitter, as well as collaborative tools such as blogs and wikis for personal use. However, staff should remain mindful of their professional responsibilities and use sound judgement and common sense.

2.2 When communicating with pupils, staff should use a school system (such as the Portal or email). If school systems do not meet your needs consult with the Director of IT and eLearning who can suggest an alternative and provide advice on using any social media platforms appropriately.

3. Guiding principles

3.1 In accordance with the Staff Code of Conduct, staff are expected to demonstrate a sense of responsibility and in doing so, adhere to the following principles:

3.2 Staff should ensure that their personal social media accounts are set as private and must not 'connect' with pupils or parents or join the same social media groups.

3.3 Staff should exercise caution when making links with ex-pupils of the school on a personal social media account. The Staff Code of Conduct advises staff not to 'connect' with recent Old Paulinas on personal social medial accounts within two years of them leaving the school and in any event not until they are over 18. Keep in mind that an OP may also be linked or 'friends' with current pupils which (depending on your privacy settings) may expose your personal information or content.

3.4 Staff should ensure that the privacy settings for any personal social media profiles are configured appropriately and limit the amount of information that is publicly available.

3.5 Staff must be mindful of how they present themselves and the school on such media. The private life of an employee at the School may have professional consequences and this must be considered at all times when sharing personal information in this format.

3.6 Staff must not represent personal views as those of the School, nor disclose the views of colleagues or others working with the school (eg management consultants).

3.7 When writing an internet post, staff should remember that this is not a secure form of communication and consider whether the contents would be more appropriate in a private message. While there may be strict privacy controls in place on personal accounts, information could still be copied and shared by others and can easily enter the

public domain. For this reason it is always sensible to consider that all information posted online has entered the public domain.

3.8 Staff should protect the privacy of others by omitting personal information from internet posts such as names, email addresses, home or work addresses, phone numbers or other personal information, and it is recommended that the same principles are followed for the user's own personal information.

3.9 Staff must not post anything that may offend, insult or humiliate others, particularly on the basis of their age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity. Nor must staff post anything that could be interpreted as threatening, intimidating or abusive. Offensive posts or messages may be construed as cyberbullying.

3.10 Staff must not post disparaging or derogatory remarks about colleagues or the School, or its Governors, volunteers, pupils or parents.

3.11 Staff must not use social media in a way which could constitute a breach of any of the School's employment or other policies.

4. Official use of school social media accounts

4.1 As far as possible school IT systems should be used for all official school business, however social media may be used where school systems do not meet specific requirements, for example communications and marketing, alumnae relations or for specific curriculum needs. The Head of Communications can advise on appropriate use of social media for school purposes.

4.2 School social media accounts must be kept separate from personal accounts and registered using a school email address.

4.3 School social media account usernames and passwords must be logged with the Director of IT and eLearning.

4.4 A designated member of staff must be responsible for managing and approving content posted on the social media account, including content or comments that external parties may post.

4.5 Accounts that are no longer used should be deactivated or deleted.

4.6 The School will monitor the use of school social media accounts to check that their use is compliant with school policies.

5. Removing postings

5.1 Staff may be required to remove internet postings which are deemed to constitute a breach of this policy.

6. Breach of Social Media policy

6.1 Failure to comply with this policy may result in an investigation and hearing under the School's disciplinary policy or other appropriate action.