Staff Acceptable Use 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	Director of Strategic Development	June 2020	✓
Approved	Board of Governors	25 June 2020	✓

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

Introduction

This policy covers the acceptable use of IT and data and applies to all members of St Paul's staff. In this policy "staff" includes teaching and non-teaching staff, governors, and regular volunteers.

This policy applies when accessing:

- school data and information, in any format, relating to its community and operations;
- the school network and/or information systems, by any means or device, whether directly or remotely, wired or wireless, on school or personal devices;
- the internet, social media, or emerging communications platforms, whether through the school network, equipment and/or information systems, or through personal devices, including through personal networks and the user's own mobile service provider while on duty, conducting school business and/or representing, or perceived to be representing the school.

This Policy should be read in conjunction with the following School Policies:

- Safeguarding and Child Protection Policy
- Data Protection Policy
- School Privacy Notices
- Data Breach Policy
- Anti-Bullying Policy
- Data Retention Policy
- Online Safety Policy
- Taking, Using and Storing images of Children and Young People Policy

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 students.
- Staff understand the boundaries of acceptable behavior, to mitigate the risk of inappropriate communication taking place between staff and students and of having misplaced allegations being made against staff.

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.

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 disciplinary policy, or other appropriate action may be taken.

This policy is also written in conjunction with *Keeping Children Safe in Education 2019 (Annex C).*

Responsible use of IT systems and equipment

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).

Staff should be familiar with the student acceptable use policy and enforce this where appropriate, reporting unacceptable use to the Director of IT, Bursar, or Pastoral Deputy, and staff should lead by example.

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 this policy and staff access of blocked sites will be logged automatically by the system.

Staff must not deliberately browse internet sites or view content that is illegal, violent or considered offensive or indecent (for example material that is pornographic, racist, sexist or that promotes violence, 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).

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.

Data protection and the GDPR

Staff should understand their responsibilities when accessing, using and sharing school data and only do so according to the school staff data protection policy and data protection legislation as well as their contracts of employment.)

Unless otherwise stated all data and information relating to your work at the school (for example personal information relating to staff or students, work submitted by students, internal examinations, financial data or confidential minutes) is subject to the school data protection policy.

Personal email should not be used for school work.

All official school business must be conducted on school systems

Use of personal devices for school purposes, and the storage or removal of personal data or confidential information from school systems (by any means, including email, printing, file transfer, cloud or (encrypted) memory stick) must be registered with and approved by a

member of school staff responsible for the data in question and encryption should be approved by the Director of IT.

When working from home staff should use school equipment and only access school data on school-approved systems. School data should not be downloaded to personal or home equipment, nor to USB drives or storage devices.

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 secondary screen, monitor or projector.

If a member of staff is aware that school data, particularly staff or students' 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 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, including during the school holidays.

Data stored on the school network is backed up regularly. Removable media and storage devices must not be used without explicit approval by the Director of IT.

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').

IT security

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 the IT Department portal page on security).

Staff must only login to school systems and equipment, with their own username and password.

Staff must not share their username and password with anyone else.

Staff should be aware that the school will never request their password by email or other means.

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.

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

Staff must not attempt to circumvent the school's IT security controls (including through the use of VPNs), nor seek to gain unauthorised access to data.

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

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.

Use of email (see also Appendix A)

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.

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.

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, these should be linked or advice should be sought from the IT department.

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 email protocol is attached at Appendix A.

Safeguarding and conduct with students

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

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 immediately. Do not attempt to access the content yourself as this could corrupt any evidence.

Student 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 and following the *Taking, Using and Storing images of Children and Young People Policy*.

Permissions are required from students (and parents) in certain circumstances and therefore staff should always assume that images and videos of students should not be shared publicly without prior permission and guidance from the communications team.

In accordance with the Staff Code of Conduct, staff should not give out their personal mobile, email or home telephone numbers to students. School phones should be used on trips to avoid staff having to give out their personal phone number to students. If staff are required to communicate with students using their own device, communication should be via the school email system or school-approved systems such as Microsoft Teams.

Visiting Music Teachers (VMTs) may give personal email addresses to parents as they are providing private lessons under the terms of the VMT handbook.

Photographs or audio/video recordings of students should only be taken using school-approved systems and should not be stored on personal devices.

Staff must not use their personal device storage for photographs or audio/video recordings. School cameras are available to borrow from the IT department, or images/video can be recorded using OneDrive on their devices, ensuring that the files are stored on their school accounts.

School images and video should only be captured according to the Taking, Using and Storing images of Children and Young People Policy

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.

Guidelines on the use of social media are outlined in the online safety policy.

Use of school IT facilities for personal use

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.

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.

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.

Use of personal devices in school

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.

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.

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).

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

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.

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.

Social media guidelines

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.

Monitoring

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.

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.

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.

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 students 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 students, staff must use a school system (such as the Portal or email). If school systems do not meet your needs consult with the Director of IT Systems 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 students or parents or join the same social media groups.

3.3 Staff should exercise caution when making links with ex-students 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 students 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, students 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 School IT systems must 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 Director 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 Communications.

4.4 A designated member of staff must be responsible for managing and approving content posted on the departmental social media account, including content or comments that external parties may post. Where images of students are posted on social media accounts staff must refer to the Quick Guide to Posting Images on Social Media attached at Appendix C and then obtain authority to post from the Director of Communications.

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.

Quick Guide to Posting Images on Social Media Appendix C

This document is intended to be a quick reference guide to posting images on social media. It is not intended to be a comprehensive guide and it is not a substitute for reading the full SPGS policies.

BEFORE ANY PHOTOGRAPH MAY BE POSTED ON SOCIAL MEDIA THE CONSENT OF THE DIRECTOR OF COMMUNICATIONS MUST BE OBTAINED.

In particular, the following should be read carefully:

- Taking, Using and Storage of Images of Students Policy
- Staff Code of Conduct
- Social Media Policy
- Staff Acceptable Use of IT Policy

Step 1

Has the parent (and/or student if the student is of sufficient maturity) told the school that they do not want their child's image to appear in any published photographs? If so, no photograph should be shared if it includes their image

Our Parent Terms and Conditions inform parents that we may use photographs of students in our promotional material (e.g. admissions publications, on websites or on social media, for use in the school's news and events publications, or for educational purposes.)

It also informs them of their right to tell us that they do not want their child's image to be used in any way. If we receive this instruction it will be recorded by the admissions team.

You should check at regular intervals (e.g. every six months) whether this applies to any of the children in your year group, sports team etc.

Step 2

Decide whether you need to obtain specific consent from the parent (and/or student if the student is of sufficient maturity) to include the photograph in the post. The permission granted by our Parent Terms and Conditions do not entitle us to publish all photographs – it will depend on the exact photograph and what it is intended to be used for.

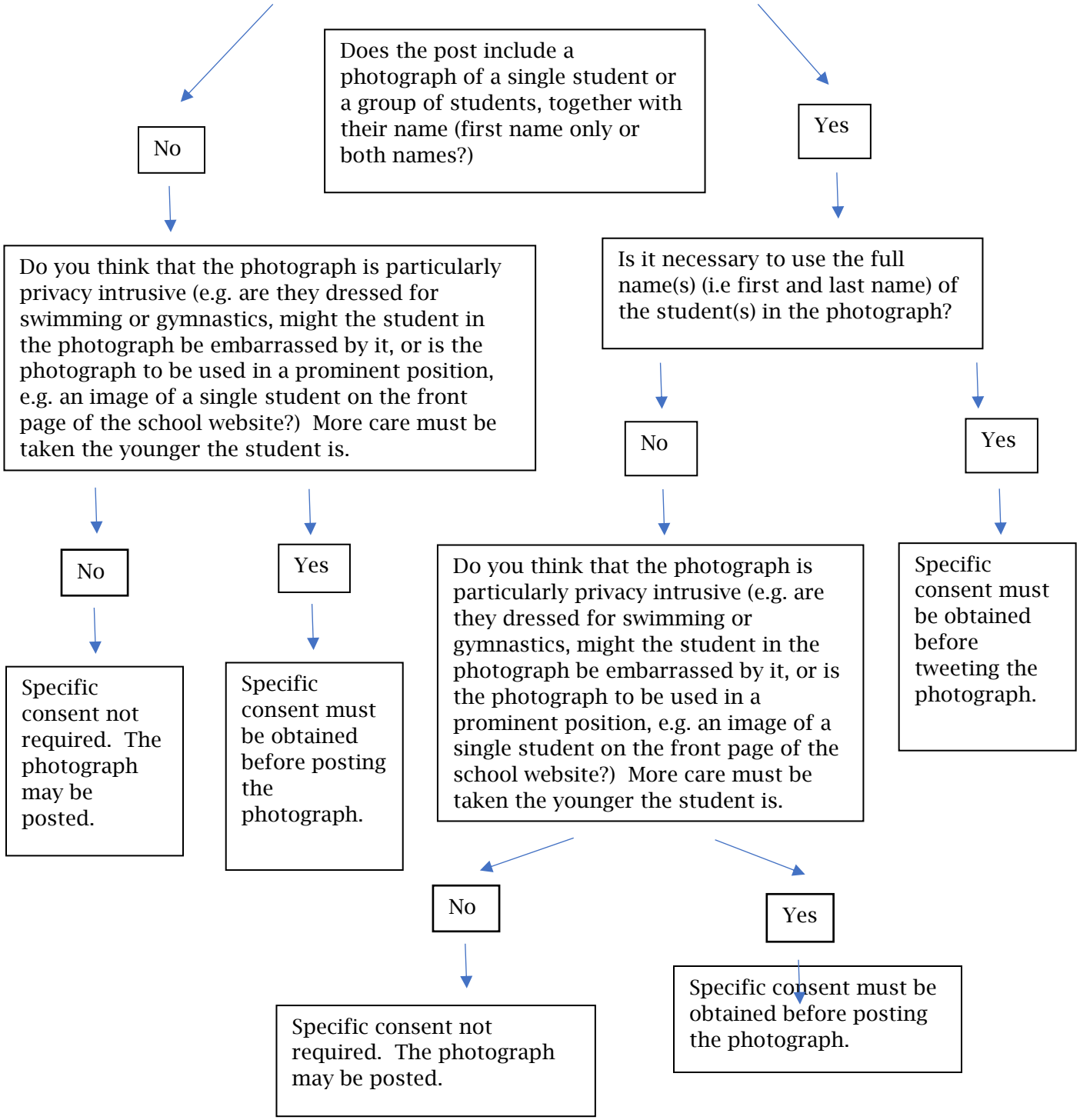
Attached is a flow diagram that gives guidance on whether specific consent if needed.

Step 3

If necessary, obtain specific consent from the parent (and/or the student if the student is of sufficient maturity).

If you need to obtain specific consent you must tell the parent and/or the student what the photograph will be used for and you must record the fact that consent has been given [where would this be recorded?]. You must record the following information: who consented, when they consented, what they had been told and how they consented (e.g. by email or verbally).

The consent is only valid for that photograph. If you want to post another photograph in future where specific consent is required, or that photograph in another publication, you will need to obtain additional separate consent. Blanket consent to all photographs cannot be given.


Does the post include a photograph of a single student or a group of students, together with their name (first name only or both names?)
No
Yes
Do you think that the photograph is particularly privacy intrusive (e.g. are they dressed for swimming or gymnastics, might the student in the photograph be embarrassed by it, or is the photograph to be used in a prominent position, e.g. an image of a single student on the front page of the school website?) More care must be taken the younger the student is.
Is it necessary to use the full name(s) (i.e first and last name) of the student(s) in the photograph?
No
Yes
No
Yes
Specific consent not required. The photograph may be posted.
Specific consent must be obtained before posting the photograph.
Do you think that the photograph is particularly privacy intrusive (e.g. are they dressed for swimming or gymnastics, might the student in the photograph be embarrassed by it, or is the photograph to be used in a prominent position, e.g. an image of a single student on the front page of the school website?) More care must be taken the younger the student is.
Specific consent must be obtained before tweeting the photograph.
No
Yes
Specific consent not required. The photograph may be posted.
Specific consent must be obtained before posting the photograph.