Acceptable Use Policy Staff Supplement

This policy applies to staff, members of the governing board, 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	April 2021	✓
Approved	Board of Governors	23 June 2021	✓

To be published on the following:	
Staff Portal	✓

1. Introduction

1.1 Staff are bound by the terms of the school Acceptable Use Policy (AUP) (previously known as the student AUP) which must be read in conjunction with this staff supplement that identifies additional requirements and exceptions to the school AUP that are applicable to staff working at St Paul's. In this policy "staff" includes teaching and non-teaching staff, governors, and regular volunteers.

1.2 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.

1.3 This policy should be read in conjunction with the following school policies:

- School Acceptable Use Policy (AUP)
- Safeguarding and Child Protection Policy
- Data Protection Policy
- Staff Code of Conduct
- School Privacy Notices
- Data Breach Policy
- Anti-Bullying Policy
- Data Retention Policy
- Online Safety Policy
- Taking, Using and Storing images of Students Policy
- Student Device Policy
- Mobile Phone Policy

Staff are also expected to read the minutes of Friday staff briefings to keep abreast of important announcements and developments regarding online safety and to implement them appropriately and in a timely manner.

1.4 The school seeks to embrace the use of IT by staff to enhance teaching & learning and the school's administrative processes. The aim of this policy is to ensure that:

- Information and resources appropriate for the operation of the school are readily available to the relevant users throughout the school.
- Confidentiality of personal data is maintained in line with our Data Protection Policy.
- The integrity of our systems and the information held within them is maintained.
- Undesirable consequences associated with breaches of information security are avoided.
- Staff understand their responsibilities online to ensure the welfare and safeguarding of students.

- Staff are aware of and trained in the core digital skills required to support the online safety of the school in addition to specialist skills relating to their role.
- 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.
- Staff understand that it is their responsibility to reinforce online safety amongst its community, to report concerns and not to ignore breaches of school policy.

1.5 All staff and adults offering services at the school who access school IT systems are required to read and comply with the School AUP and Staff Supplement. Failure to comply with the policy may lead to disciplinary action (refer to school Disciplinary policy).

1.6 This policy is also written in conjunction with *Keeping Children Safe in Education 2020 (Annex C).*

2. Responsible use of IT systems and equipment

2.1 Staff are expected to use school IT systems responsibly and primarily for the purposes of their job (see section 8 – Use of school IT facilities for personal use).

2.2 Staff should be familiar with the school AUP and enforce this where appropriate, reporting unacceptable use to the Director of IT, Bursar, or Director of Pastoral Care, and staff should lead by example.

2.3 Staff should be aware that access to the network and use of systems is logged, not actively monitored, but may be reviewed in accordance with this policy and staff access of blocked sites will be logged automatically by the system.

3. Data protection and data protection legislation

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

3.2 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.

3.3 You are obliged to comply with the school data protection policy when processing personal data on behalf of the school. If you do not comply this may result in disciplinary action. - see disciplinary action policy.

3.3.1 Compliance with the school data protection policy will help the school to meet its obligations under data protection legislation. In some circumstances strict compliance with the act will be subsidiary to other considerations, for example situations involving safeguarding concerns.

3.3.2 Members of staff should err on the side of caution when dealing with data protection issues and, in particular, whether to report a data breach. It is the responsibility of staff to report a potential breach or a possible subject access request. It is preferable to discover in retrospect that it was not necessary than vice versa. Similarly, the consequences of covering up a data breach can be as significant as the data breach itself. No matter how uncomfortable we

might feel about the initial breach, it is essential that we overcome our personal anxiety by sharing the responsibility with the appropriate school officers.

3.3.3 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. This can be done via the *data breach* tab on the staff portal homepage. For online or breaches involving IT, the Director of IT should also be contacted without delay.**

- 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.

3.4 Where school laptops or equipment have been issued to a member of staff, that member of staff will have elevated access to school databases and should therefore not use personal equipment for school business.

- This applies when onsite or remote working.
- An exception to this, is the use of school email on personal devices, which must be accessed only on devices as follows:
  - with up-to-date system software;
  - through core school systems that access the information directly from the school network (i.e. Microsoft Outlook, not Apple Mail nor other third party services);
  - with encryption enabled (facial recognition and/or a minimum six-digit password must be enabled within settings (highly sensitive information is regularly communicated within school email);
  - with advice from the Director of IT if in any doubt.

3.5 Exceptions for the use of personal devices for school purposes, and the storage or removal of personal data or confidential information from school systems related to the school for school business (by any means, including email, printing, file transfer, cloud or (encrypted) memory stick) must be registered with the Director of IT, with approved encryption, and with the written approval of the member of school staff responsible for the data in question.

3.6 Staff must 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, visitors, or general public and particularly if the computer is connected to a secondary screen, monitor or projector. (Examples of data breach include public transport where members of the public can read content from devices; or devices left logged in at home or at work, but unattended).

4. IT security

4.1 The security of the school's IT systems is only as strong as its weakest link. It is therefore the responsibility of all staff who should follow the advice and guidance specified by the IT department (please see the IT Department portal page on security).

4.2 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 data protection legislation. 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, these should be linked, or advice should be sought 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 email protocol is attached at Appendix A.

6. Safeguarding and conduct with students

6.1 Staff should understand their responsibilities regarding safeguarding (see the Safeguarding (Child Protection) policy and Online Safety policy) and understand that these also apply when using IT systems and equipment.

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, you may confiscate the device, but should consult a member of SMT and contact the Director of IT immediately before taking any further action. Do not attempt to access the content yourself as this could corrupt any evidence.

6.3 **Remote working**. Lessons on remote platforms (such as Teams or Zoom) should have the following settings applied:

- 'Authenticated participants only' (logins ending with @spgs.org)
- Authorised visitors only.
    - (Visitors will be expected to meet normal safeguarding criteria)
- Staff are instructed to use the 'Waiting Room' feature of Zoom for lessons and students must be admitted by the host teacher with the host teacher present at all times.

6.4 **Online resource approval process**. The use of online resources should be in accordance with the online resource approval process.

- Approval for new online resources for teaching & learning, co-curricular and pastoral purposes should only be sought in consultation with HoD/HoYs. Online resources that require payment or enrolment need special attention and should not be used without agreement of the Bursar.
- Staff should be aware of the Online Resource Approval listings and should ensure that they do not use online resources that have not been approved for the year groups that they are referring them to.
- Staff should be aware that online resources that are not approved may be blocked on student 1:1 devices, preventing access, for example, for homework and research.
- Staff and student judgment prevails. While staff should never endorse or recommend resources that they have not fully checked, nor submitted for approval, in all cases staff should be aware that the online resource approval process may be fallible if third party resources change without warning or notification. In view of this, staff are expected to

check resources regularly at the point of recommendation and should instruct students to apply the best of their judgment on accessing resources, reporting any concerns using the online reporting form.

7. Capture, storage and publication of images/recordings

7.1 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*. Staff may use their own personal device, but only by taking the photo through the OneDrive app as this will automatically store the image to the school's system and not to the staff member's personal storage. These should then be moved by the Head of Department to the departmental folder for which they are responsible. **Images must never be saved or stored to a member of staff's own personal storage** (e.g., mobile phone photo roll). Please seek guidance from IT if required.

7.2 In addition to the main school AUP and *Taking, Using and Storing images of Children and Young People Policy*, staff should be sure that the capture of images/recordings:

- is transparent, obvious, and approved;
- of staff or students for promotional or marketing material is lodged and approved with the Communications Office;
- of academic work is lodged and approved by the relevant academic Head of Department or Director of Studies;
- of pastoral activity is lodged and approved by the relevant pastoral Head of Year or Director of Pastoral Care;
- of co-curricular activity is lodged and approved with the Deputy Head – Co-curricular;
- of any other activity is approved by the Director of Communications.

7.3 Permissions are required from students (and parents/guardians) in certain circumstances and therefore staff should always assume that images and recordings of students should not be captured or shared publicly without prior permission and guidance from the Director of Communications or the Bursar.

7.4 In accordance with the Staff Code of Conduct, staff should not give out their personal mobile, email or home telephone numbers to students.

- If staff are required to communicate with students using their own device, communication should be via the school email system, using school accounts only, or school-approved systems such as Microsoft Teams.
- Where school channels, including Teams, is not sufficient, school phones may be issued, for example on trips.

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

7.6 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.

8. Personal online presence and personal use of school IT network and systems

8.1 It is understood that staff may occasionally need to use the school's IT facilities for personal, non-school related use and staff should seek permission from their line manager However use should not interfere with schoolwork and staff responsibilities and should be limited to break times. 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.

8.2 To be mindful that personal conduct online can have professional consequences and activity affecting a member of staff's reputation and/or the reputation of the school, including posts or comments that refer to specific matters related to the school and/or members of its community on public or private social media sites must be avoided. School channels and procedures are available for this.

8.3 Online activity for personal gain that impacts, or capitalises on roles, responsibilities or professional conduct, or knowledge gained in the course of working at St Paul's must be agreed in advance through your line manager and further advice can be sought from HR.

8.4 School reprographics equipment, including printers, scanners, and photocopiers are for school operations and business, and should not be used for personal gain.

- These may be used for personal items on an exceptional and limited basis and disciplinary action may be taken if it is established that school IT facilities have been used to excess for personal use.
- Staff should not save personal files on the school network such as personal photos, music files etc.

8.5 Use of personal devices in school

8.5.1 Staff may use their own personal devices (laptops, tablets or smartphones) in school for their own personal use, 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. Personal devices should not, however, be used for school business if the member of staff has been issued a school device; see here.

8.5.2 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.

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

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 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 (e.g., 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, e.g., '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 (e.g., 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 policy. The policy applies at all times whether using school computers or your own device and both when in school and 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 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 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.

3.3 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.

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

3.5 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.

3.6 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.

3.7 Staff must not post disparaging or derogatory remarks about colleagues or the school, or its governors, volunteers, students or parents.

3.8 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 All use of social media must be approved by the Director of Communications. 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.

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 lodged and updated 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.

Appendix C. Quick Guide to Posting Images on Public Facing internet channels, including social media (with or without private settings), websites and Apps.

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 compliance with St Paul's policies and those listed to be read in conjunction with this AUP in particular.

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
- Online Safety Policy
- School Acceptable Use 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 and lodged with the Communications Office.

Prior to publication of images or recordings, the list of exceptions should be checked with the Communications Office.

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 & 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.

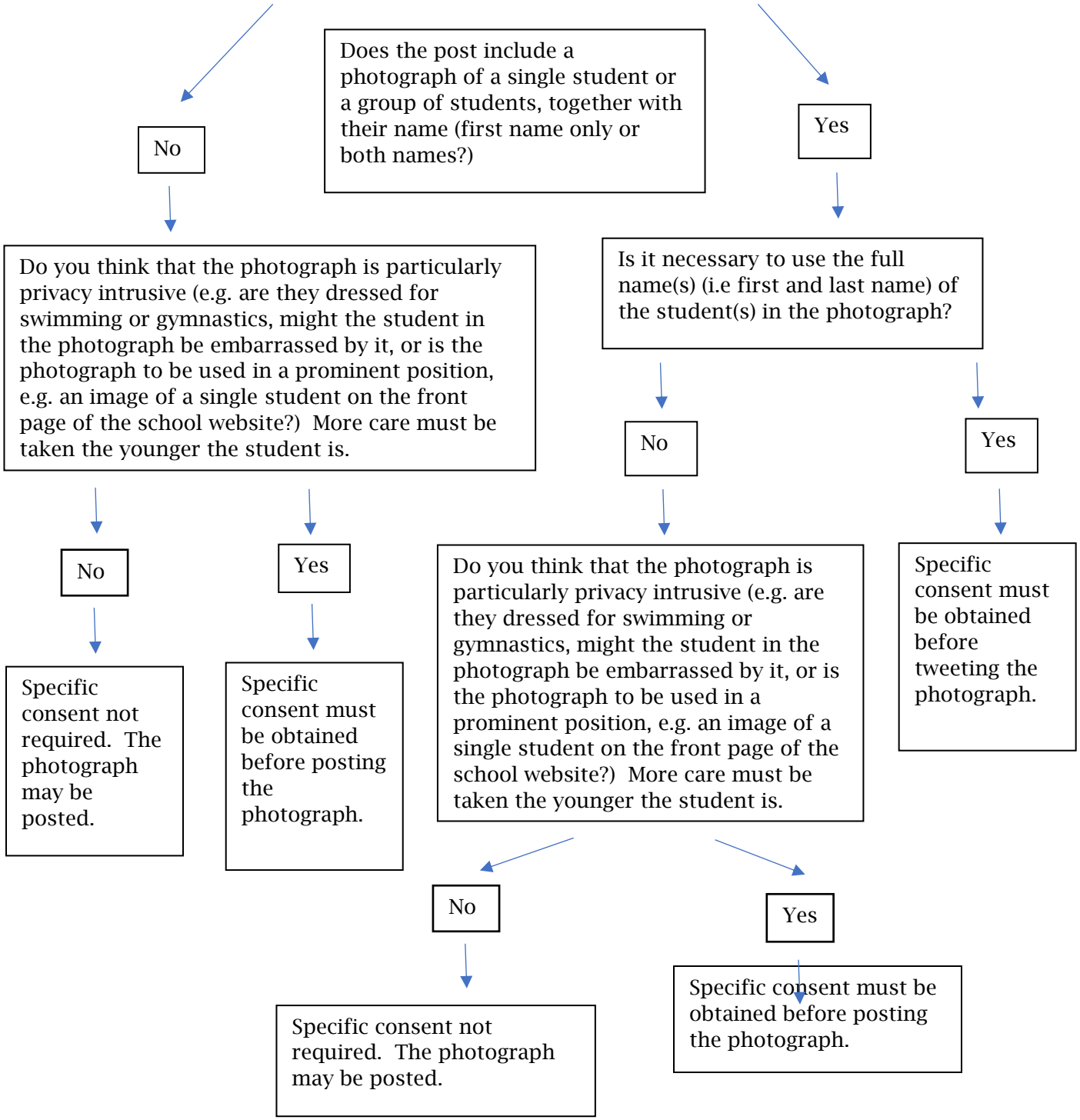
Attached is a flow diagram that gives guidance on whether specific consent if needed.

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. 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.