ST PETER'S

PREPARATORY SCHOOL

IT Acceptable Use Policy

Updated on 18 March 2026
by Mr Dan Morris
(Director of Operations & Compliance)

Approved by Head: Charlotte P Johnston.

Date: 12th May 2026

Scope of this Policy

This policy applies to all members of the School community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, peripatetic staff and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

A pupil friendly version is also included at the end of this policy.

This policy should be read in conjunction with the School's Child Protection & Safeguarding Policy, Data Protection Policy, Online Safety Policy, and Privacy Notice.

Purpose

This policy seeks to outline acceptable use of School IT systems (and personal devices) at St Peter's Preparatory School, and should be read and accepted in conjunction with the e-safety policy.

Online behaviour

The School recognises the vast learning possibilities associated with accessing the world wide web. However, as a member of the School community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create, post, download, upload, or share any material, comments, or content that is illegal, misleading, or likely to cause offence within the School community. This includes, but is not limited to, content that is obscene; promotes violence, discrimination, or extremism; contains pornography or indecent images of children or young people; incites racial or religious hatred; encourages or involves illegal activity; or is otherwise inappropriate or offensive to others.
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the School community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

The School acknowledges that in certain planned curricular activities, access to some sites, which otherwise might be deemed inappropriate, may be beneficial for educational use (for example investigating racial issues). Any such access should be pre-planned and recorded so that it can be justified if required.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK

Using the School's IT systems

Whenever you use the School's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access School IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, School IT systems.
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's IT systems, and that the School can view content accessed or sent via its systems.
- Any personal devices (e.g., phones, tablets, laptops) connected to the School network must comply with this policy. Staff and pupils must not use personal devices to bypass filters, store inappropriate content, or create personal hotspots.

Monitoring of the School's IT systems is conducted under the School's legitimate interests as outlined in Article 6(1)(f) of the UK GDPR, and in accordance with the School's Privacy Notice. Access and usage logs are retained in accordance with the School's Data Protection Policy and are accessible only to authorised staff.

Use of Personal Devices

- Phones must be switched off or on silent during teaching time and when supervising pupils.
- Use is restricted to designated staff areas (e.g. staff room, offices).
- Personal calls/messages should be limited to breaks or emergencies.
  Phones must not be used while driving on school business (refer to Driving at Work Policy).
- The School recognises that there are times when peripatetic staff may need to use a personal device to access various apps used to assist with teaching. Please refer to Appendix 1 for further details.

Online Safety

You will ensure that you comply with the School's policy on Online Safety.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the School restricting your access to school IT systems.

If you become aware of a breach of this policy or you are concerned that a member of the School community is being harassed or harmed online you should report it to the Head of Pastoral Care. Reports will be treated in confidence.

Appendix 1

IT Acceptable Use for Visiting Peripatetic Teaching Staff

This appendix, which is specifically for visiting peripatetic teachers, works alongside and in conjunction with the St Peter's IT Acceptable Use Policy, Online Safety Policy and Digital Imagery Policy.

Please read and sign to confirm that you understand and will comply with the points below:

- Mobile phones must not be used during 1:1 lessons
- Personal devices, such as tablets and/or laptops, may be used during 1:1 lessons but for work purposes only
- Pupils must be registered as present/absent for their 1:1 lesson via SOCS using a school tablet
- Videoing of pupils for examination purposes is permitted, but peripatetic staff must gain written consent from parents prior to taking video footage
- Video images should only be taken on school equipment and teachers must follow the Digital Imagery Policy with regards to the sharing, distribution and publication of those images

Name:

Signed by: Date:

Acceptance of this policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the Director of Operations & Compliance.

I understand and accept this acceptable use policy:

Name: ……

Signature: ……

Date: ……

Revision History		
Date Revised	**Changes**	**Reviewed By**
04 Apr 2025	Added monitoring of access and usage section.	Dan Morris (Dir. of Operations)
18 March 2026	Reworded bullet point two in Online Behaviour	Dan Morris (Dir. of Operations)
18 March 2026	Added section on Use of Personal Devices	Dan Morris (Dir. of Operations)
18 March 2026	Added Appendix 1 - IT Acceptable Use for peripatetic staff	Dan Morris (Dir. of Operations)

ST PETER'S
PREPARATORY SCHOOL

ICT Acceptable Use Policy - Pupils

When I am using the computer or other technologies, I want to feel safe, all the time. I agree that I will:

- always keep my password a secret.
- only visit sites which are appropriate to my work at the time
- only work online with people from our school and I will deny access to others.
- tell a responsible adult straight away if anything makes me feel scared or uncomfortable, online.
- make sure all messages I send, and Blog posts and comments I submit are respectful of others.
- not send silly, annoying or harmful messages.
- show a responsible adult if I get a nasty message or receive anything that makes me feel uncomfortable or afraid.
- not reply to any nasty message or anything that makes me feel uncomfortable or scared.
- not give my mobile phone number to anyone who is not a real friend.
- only message people I know or those approved by a responsible adult, such as my parents or my teachers.
- talk to a responsible adult before joining any chat room.
- always keep my personal details private. (My name, family information, my journey to school and home from school, my birthday or year of birth).
- always check a responsible adult or my parents before I show any photographs of myself.
- always check with my parents or teachers if I can upload photographs.
- never meet an online friend without taking a responsible adult, such as my parent or grandparent with me.

I know that once I post a message or an item on the Internet then it is completely out of my control and even if I delete it, it may still be available to others.

I know that everything I search for, access, write or say on our school system is logged. It can be viewed, read and moderated (has to be approved) by my teachers. I understand and agree.

Signed ……

Name……..

Date ……