

Acceptable Use of Computing Policy

(This policy forms part of the overall Computing policy)



Lead	Joshua Parker
Head	Sandie Edward
Chair of Governors	Jeremy Hooper
Policy amended	September 2026
To be reviewed	September 2027

Introduction

Our Vision for St Philip's
Happiness, Love and Security abound
Everyone is special
Every achievement is celebrated
Relationships and Teamwork matter
A beacon of light in the community
Christ in everything we do.

This policy is written with our Vision Statement at its heart.

Boundaries between localised and global networks in computing are increasingly less clear, as the vast majority of both home and school computers, together with a large percentage of mobile phones, effectively have a permanent open connection to the Internet. This policy hence doesn't attempt to distinguish internet use from other computing use and is intended to apply to all uses of ICT equipment within school and use of school ICT systems at home. Connection to global networks via the internet opens access to a vast network of resources. It enables sharing of information and multimedia resources, access to software not held locally, communication in a wide variety of forms and more continuous working between home and school. As is widely recognised, however, the largely unregulated nature of this network also makes it an environment in which technology and education need to work in partnership to ensure its safe use by pupils.

The purpose of this policy is to:

- Establish the expectations we have in school for the use of the ICT by pupils and staff.
- Outline the ways that these expectations are communicated to all concerned.
- Establish the sanctions that will need to be applied where these expectations are not met.
- Establish the expectations we have for the use of ICT by pupils and staff while remote learning and working.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians. At St Philip's Primary School, we feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents. Staff, parents and children will be sent an explanatory letter and the rules, which form our Computing Access Agreement and acceptable use.

This policy has been updated in line with the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education 2026](#), and its advice for schools on:

[Teaching online safety in schools](#)
[Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)

Safeguarding and online safety is key and the keeping children safe in education document is as important for online safety as it is for overall safeguarding.

All staff receive safeguarding and online safety training as part of induction and regular safeguarding updates.

EXPECTATIONS

- It is expected that all users of the ICT, teachers, pupils, students, parents and visitors be required to follow the conditions in this policy, and the rules for acceptable use, whether it be in school on the PCs, teacher laptops or laptops that have been made available for remote learning/working.
- A responsible approach to resources should be shown.
- All Computing activity should be appropriate to staff professional activity or the pupil's education.
- Use of the internet and facilities such as the electronic mail service are intended primarily for educational purposes.
- Any communication should be honest, legal, decent and true. Any expression of a personal view about the school, an individual or another business in an Internet communication must be endorsed to that effect.
- All users should show consideration and respect for other users both locally and with whom they may come into contact on the Internet.
- Any online safety, safeguarding or child protection concern identified through the use of technology must be reported immediately in accordance with the school's Child Protection and Safeguarding Policy and referred to the Designated Safeguarding Lead (DSL) or Deputy DSL where appropriate.

DETAILED CONDITIONS OF USE

All Internet activity should be appropriate to staff professional activities or the children's education;

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;

- The school's Internet may be accessed by staff and children throughout their hours in school; teaching staff have access to the school's shared drive at home.
- For staff occasional and reasonable personal use is permitted (for example during lunch breaks), as long as this does not interfere with the performance of your duties or the work of other staff.
- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media;
- Use of the school's Internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded;
- Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the school's network is the property of the school and making unauthorised copies of materials contained thereon maybe in breach of the Data Protection Act, Individual Copyright or Intellectual Property Rights;
- Use of materials stored on the school's network for personal financial gain is excluded;
- Posting anonymous messages and forwarding chain letters is excluded;
- The use of the Internet, e-mail, or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden;
- Individuals must not create, possess, share, request or distribute inappropriate, harmful or abusive content. Any incident involving online abuse, image-based abuse, harassment or exploitation will be treated as a safeguarding concern and managed in accordance with safeguarding procedures.
- All web activity is monitored, including the content of e-mail, therefore it is the responsibility of the user to ensure that they have logged off the system when they have completed their task;
- Children must not be given unsupervised access to the Internet. For the purposes of this policy, "supervised" means that the user is within direct sight of a responsible adult;
- The teaching of online safety is increasingly included in the school's Computing and PSHE teaching, but teachers within all year groups should be including Internet

safety issues as part of their discussions on the responsible use of the school's computer systems;

- All children should understand that if they see anything that troubles them on a computer screen, they must report it immediately to a member of staff and not attempt to remove what is on the screen. Pupils are also aware of the CEOP button on our school website. Pupils in KS2, where internet access is regular, should be taught to turn off the screen in any such incident. If children are working remotely, they must report any inappropriate incidents to an adult at home but also to the school directly to either:

head@sps.sefton.school
safeguarding@sps.sefton.school

School will then log any incidents in their incident report log kept in school. You can also report none school related incidences to CEOP at

<https://www.thinkuknow.co.uk/parents/get-help/reporting-an-incident/>

- If Staff unintentionally access an offensive, obscene or indecent website they must disconnect from the site immediately and inform the Head Teacher or Responsible Teacher.
- Parents should access content through the school website (Online Safety page) if they have concerns about a particular online platform.
- The school recognises the potential and the risks associated with use of Artificial Intelligence tools. Any use of Artificial Intelligence tools to enhance or support the education of our pupils should be carried out in line with the school's AI policy. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school. Risks associated with AI include the use of tools to bully others or spread misinformation – any instances where AI has been used for these purposes will be dealt with under both this acceptable use policy and our school behaviour and anti-bullying policies where appropriate. Staff and pupils should be aware that AI technologies can be used to create manipulated images, audio or video content. Any use of such technology to cause harm, distress, bullying, exploitation or deception will be treated as a safeguarding matter.
- Information relating to safeguarding concerns will be shared with relevant professionals where necessary to protect children and in accordance with statutory safeguarding guidance and data protection legislation.

FILTERING AND MONITORING

In line with Keeping Children Safe in Education 2026, the school has filtering and monitoring in place to ensure that inappropriate materials cannot be accessed online using school IT equipment. The filtering and monitoring systems are implemented by our IT support

provider, APEX, and are reviewed annually, or if a concern arises or is reported to ensure they are working appropriately. Any major concerns with the filtering and monitoring are reported to governors as and when the need arises and the governing body review filtering and monitoring arrangements annually as part of their policy review cycle.

The filtering and monitoring system sends alerts via email each time there is an attempt to access or type in a website or search term that is blocked. These alerts are monitored by the School Business Manager and then investigated by the Head Teacher where there are concerns. The outcome of any investigations is logged and any concerns dealt with in line with this policy or the school's Child Protection policy as appropriate.

A monthly check of the filtering and monitoring is carried out to ensure that inappropriate websites or key- search terms that would be a cause for concern are blocked by the filtering system. Any issues identified as part of these checks are investigated with APEX so they can be resolved and appropriate restrictions put in place.

SANCTIONS

If any breach of conditions is discovered the following sanctions may be enforced:

- Temporary or permanent ban on ICT use.
- Additional disciplinary action in line with school behaviour policies.
- Parents and other external agencies may be contacted.

INTERNET PUBLISHING STATEMENT

The school wishes the school's web site and any learning platform communities to reflect the diversity of activities, individuals and education that can be found at St Philip's Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles should be borne in mind:

- No video recording may be published without the written consent of the parents/legal guardian of the child concerned, and the child's own verbal consent;
- Surnames of children should not be published, especially in conjunction with photographic or video material;
- No link should be made between an individual and any home address (including simply street names);
- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.

INTERNET AGREEMENT

All pupils and their parents / guardians will be asked to read and sign an agreement covering the expectations we have of pupils using the Internet in school and also the school programmes when remote learning.

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

- Child Protection and Safeguarding Policy
- Online Safety Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Use of AI Policy
- Data Protection Policy