St. Paul’s Primary School

Acceptable Use Policy (Staff) 2024

Introduction

The school has provided ICT equipment (laptops, iPads etc.) for use by staff, providing access to a vast amount of information, and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers.
- Only use the computers for educational purposes. Activities such as buying or selling personal goods are inappropriate.
- Digital cameras (such as those found on iPads) are for school use only. They may be used to provide visual records of school trips & class activities. Do not use personal mobile phones to record images of children.
- When using cameras, please be aware of any children whose parents do not wish them to be recorded in this way. It is your responsibility to check this.
- Avoid using removable media (such as USB drives) to store data. If you do, ensure that you only save planning or resources – do not store any personally identifiable data about the children (assessment data or reports, for example, should only be saved in the school’s password protected, cloud based, Google Drive).
- Avoid using personal ICT equipment in school. If used in school, always check personal equipment with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

Security and Privacy

- Protect your identity by keeping your password to yourself; never use someone else’s username or password.
- In line with policies outlined in the staff handbook, other computer users (in and out of school) should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you, the children or your work at risk.
- School data storage areas (Google Drive for example) may be checked at any time to monitor responsible use.

Internet

- You should access the Internet only for school related activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities (Facebook messenger etc.) should be avoided.
- Video file sharing sites (such as YouTube) can be a valuable teaching resource, but it is vital that you screen any footage completely before showing it to the children. Children should never be allowed to access these sites unsupervised.
- Where children will be using websites for research purposes, please check the site thoroughly (including external links or advertisements) before allowing the children access.

Email, Social Media & Mobile Phones

- The use of mobile phones during lessons is prohibited. Phones should be kept on 'silent' or ideally, off during time with children.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or sexually inappropriate content, DO NOT DELETE - always report such messages to a member of senior management. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- Remember, once you forward an email, it will have your email address embedded permanently as a previous sender – it is your responsibility to ensure the email is of an appropriate nature.
- Ensure that any privacy settings on any social media (Facebook, Twitter etc.) are kept up to date and secure – be particularly aware of following or befriending parents of children potentially, currently or previously at the school.
- **Images, photographs, links shared and comments on social media which are defamatory, illegal or that contravene School, Local Authority or National guidelines on professional standards will not be tolerated and will be dealt with in line with the school's disciplinary procedures.**

Please read this document carefully. If you violate these provisions, access to the Internet and school equipment may be denied and you could be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school ICT facilities within these guidelines.

Name: Signature: Date: