Paget Primary School
Information and Communications Technology Policy:
Acceptable Use of Computing Equipment
2023

Introduction

The school has provided computers, iPads and email accounts for use by staff and students as an important tool for teaching, learning and administration of the school. The use of school computers and iPads by students and members of staff is governed at all times by the following policy.

All students and members of staff have a responsibility to use the school's computers, iPads and network in a professional, lawful and ethical manner. Deliberate abuse may result in disciplinary action and/or the police being contacted.

Please note that the use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which pupils and members of staff can use the system, but to ensure compliance with the legal responsibilities of the school and to safeguard the reputation and safety of all users. Please respect these guidelines, many of which are in place for staff protection.

Lastly, the school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the school neither wishes nor intends to dictate how home computers are used, staff should consider that the spirit of this policy applies whenever undertaking an activity that stems from employment with the school.

Acceptable Use of the School Network and Loaned Equipment

Core Principles

⇒ In no circumstances should members of staff or students access or share information that is clearly inappropriate; for example, pornographic, racist, sexist or otherwise offensive material.

⇒ If sites containing offensive material are visited by accident, these incidents should be reported to a senior member of staff. Evidence of repeated visits to such sites will result in action being taken by the school.

⇒ Students and staff must respect and not attempt to bypass the security or access restrictions that are in place on the computer system.

⇒ Students and staff must not intentionally damage, disable, or otherwise harm the school's computer hardware or software.

Use of Email

All members of staff with a computer account are provided with an email address for communication, both internally and with other email users outside the school. This includes are members of the Governing Body. Staff must be cautious when sending both internal and external mails, remembering that the professional standards that apply to internal memos and external letters must also be observed when writing e-mails. Staff must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Social Networking Sites

Staff must take care when using social networking websites such as Facebook or Twitter, even when such use occurs in their own time. In particular staff:

- Must not add any current pupils under the age of 18 to their 'friends list'.
- Must ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- Should avoid contacting any pupil privately via a social networking website, even for school-related purposes.
- Staff should also take care when posting to any public website, including online discussion forums or blogs and ensure that comments do not harm their professional standing or the reputation of the school.

Privacy and Data Protection

The school takes the issues of privacy and data protection very seriously and as such it employs a variety of measures to ensure it meets the legal obligations it has to both staff and students:

- There is software in place to monitor all usage of the school network by students, governors and staff. Please be aware that computers usually leave a 'trail' of documents worked on, websites visited, emails sent/received and so on.

- If a personal computer is used at home for work purposes, users must ensure that any school-related sensitive or personal information is secured to prohibit access by any non-member of staff.
- Staff should avoid storing information on the school computer system that is unrelated to school activities.
- Users must not store any sensitive or personal information about staff or students on any portable storage system, such as a USB memory stick, portable hard disk or personal computer, unless that storage system is encrypted.

School Website and Twitter Account

The school website and Twitter account is intended to celebrate good work, promote the school and update parents. Staff are required to provide regular updates for both the website and the school Twitter account, and are encouraged to promote them to both pupils and parents. As always, certain safeguards have been put in place to protect all concerned.

- Permission is obtained from parents before any photos are posted; a list of those parents who have given permission is kept on the J drive.
- To ensure that individual children cannot be identified, no personal information such as names or addresses should be included.
- Group photos may have a caption that includes first names but there must be no correlation between their order and the position of the children in the photo.
- The work that is posted must be of a high quality and reflect positively on the school.
- Staff must not use the school's Twitter account for anything unrelated to their work, engage in discussions with parents or 'followers', or post anything that is likely to damage the reputation of themselves or the school.

Reporting Problems with the Computer System

It is the job of the ICT Network Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. In order to sustain this:

- Staff should report any problems that need attention to the ICT Network Manager as soon as possible. If they are not in school, the most manageable method of doing this is to add a ticket into the online system.
- If a computer has been affected by a virus or other malware or even suspected to have been, staff should report this to the Network Manager immediately.
- Lost documents or files should be reported as soon as possible. The longer a data loss problem goes unreported, the more likely that it will not be possible to recover the data.

Student Use of the Computer Network

By its very nature, student use of the Internet will provide access to information that has not been pre-checked by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher. There is a risk therefore that children might access unsuitable material either accidentally or deliberately.

The school believes that the benefits to pupils of accessing Internet resources far exceed the disadvantages. However in order to minimize the risks the following safeguards have been put in place:

- Paget Primary uses the Birmingham 'filtered' Internet Service, which minimises the chances of pupils encountering undesirable material. ENTRUST run weekly reports regarding the school's ICT activity. Any notifications of inappropriate use are flagged to the HT on the day of the incident. Future Digital Reports (ENTRUST) are received weekly and monitored by the HT and DHT.
- All children sign an e-safety contract with rules about Internet use. This contract is discussed as a class and then displayed in the classroom.
- Pupils are supervised at all times when using school computer equipment.
- In order to identify misuse, Smoothwall Monitor is installed on the school network and is regularly monitored.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Computing Policy is followed. Any breach of this policy should be immediately reported to a SLT member. In particular, the following should be reported:

- Any website which is accessible from within the school that is felt to be inappropriate for staff or students.
- Any inappropriate content suspected to be stored on the computer system or loaned equipment.
- Any breaches, or attempted breaches, of computer security.
- Any instance of bullying or harassment suffered from/by any member of staff, or pupil via the school computer system.
- Reports should be made either via email or directly to an appropriate member of staff. All reports will be treated confidentially.

Loaned Equipment

- Equipment loaned to staff remains the property of the school and must be available for inspection at all reasonable times. If equipment is loaned it is expected that it should be brought to school on a regular basis.

- Although equipment is loaned to support the completion of school related tasks, staff are permitted to use loaned equipment outside of school hours for their own personal use. It is important to note that this use remains subject to the school's acceptable use policy.

- Staff must ensure that they maintain their loaned equipment and report any problems, damages or losses to the Network Manager.

Loaned Equipment and Serial Numbers:

I acknowledge that I have read and understood the above policy and understand the terms and conditions under which equipment has been loaned to me. I accept that a breach of the policy may lead to action by the school.

Staff Member's Signature:

_____

Date:_____