Pallister Park Primary School E-Safety Policy

Policy Update Summary

POLICY	
E-Safety	Date of review: February 2023
School: Pallister Park Primary	Date of Meeting: February 2023

CHANGES FROM PREVIOUS APPROVED POLICY	
Feb 2023 - Updates have been made on the following; 1. New policy from previous one shared with Trustees April 2024 - Updates have been made on the following; 2. No changes	
Report provided by: C Round	

Contents

1. Who does the policy apply to?

1.1. This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

1.2. Head teachers are empowered (The Education and Inspections Act 2006), within reason, to regulate the behaviour of pupils when they are off the school site and permits members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

1.3. Pallister Park Primary School will deal with such incidents within this policy (and associated behaviour policies) and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

1.4. Children's mental health, which will be a concern in all bullying incidents is something we will be ensuring that staff consider and when this might become a safeguarding concern.

Introduction:

2. What is E-Safety?

2.1. E-Safety focuses on the education of children and young people on the benefits and risks of using new technology (including Internet technologies and electronic communications such as mobile phones and wireless technology); providing safeguards and awareness for users to enable them to control their online experiences. Pallister Park Primary School's E- Safety policy will operate in conjunction with other policies including those for Safeguarding, Behaviour, Anti-Bullying Strategy and Data Protection. We aim to ensure that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies, without risk to themselves or others.

2.2. E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Thorough implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.

2.3. The E-Safety policy will be reviewed annually.

3. Benefits of digital technology:

3.1. The internet and other digital information technologies are compelling devices and have become an essential part to the lives of children and young people in today's society. Electronic communication opens up new opportunities for everyone; helping teachers and pupils share and learn from each other. These technologies can stimulate discussion and creativity, whilst increasing awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

3.2. The benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils world-wide;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;

3.3. Exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

3.4. The effective and safe use of these innovative and progressive technologies has proven to raise self-esteem and impact directly on pupil progress.

4. Why is Internet Use Important?

4.1. Internet use is an integral part of everyday life at Pallister Park Primary School; for both pupils and teachers. It raises educational standards, promotes pupil achievement, supports the professional work of staff and enhances the school's management and administration systems.

4.2. As part of the statutory curriculum, it is a necessity for effective learning. Access to the Internet is therefore an entitlement for pupils, who need guidance and development in a responsible and mature approach to its use. Our school has a duty of care in providing pupils with quality and safe Internet access.

4.3. The internet is a powerful tool and we actively encourage its usage outside of school. However, children will need to learn how to evaluate and judge Internet information; taking care of their own safety and security.

5. World Wide Web

5.1. If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Headteacher/ OneIT, who will be able to add the site to the school filter list.

5.2. School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

5.3. Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

6. Social Networking

6.1. We will block/filter access to social networking sites and newsgroups unless a specific use is approved.

6.2. Pupils are advised never to give out personal details of any kind which may identify them or their location.

6.3. Pupils are advised not to place personal photos on any social network space.

6.4. Pupils are advised on security and encouraged to set effective passwords, deny access to unknown individuals and instructed how to block unwanted communications.

7. Managing Emerging Technologies

7.1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

7.2. Mobile phones will not be used for personal use during lessons or formal school time by staff.

7.3. Pupils who require a mobile phone MUST take it to the office for the duration of the school day.

7.4. The sending of abusive or inappropriate text messages is forbidden.

8. Published Content and the School Website

8.1. The contact details on the website will be the school address, e-mail and telephone number.

8.2. Staff or pupils' personal information will not be published.

8.3. The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

9. Publishing Pupils' Images and Work

9.1. Photographs that include pupils will be selected carefully, in accordance with Child Protection regulations.

9.2. Pupils' full names will not be used anywhere on the school website or social media.

9.3. Permission from parents or carers will be obtained before photographs of pupils are published online.

9.4. Permission as agreed as part of our acceptable use and social media agreement.

10. Assessing Risks

10.1. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.

10.2. The school will audit ICT use to establish if the E-Safety policy is adequate and that the implementation is appropriate.

11. Technical – infrastructure / equipment, filtering and monitoring

11.1. Pallister Park Primary School will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible. We will ensure that the policies and procedures approved within this policy are implemented.

11.2. School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the Local Authority E-Safety Policy and guidance.

11.3. There will be regular reviews and audits of the safety and security of school ICT systems

11.4. Servers, wireless systems and cabling must be securely located and physical access restricted

11.5. All users will have clearly defined access rights to school ICT systems.

11.6. All users (at KS2 and above) will be provided with a username and password by the ICT lead who will keep an up to date record of users and their usernames.

11.7. Usernames and passwords will be made accessible to teachers.

11.8. Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

11.9. Requests from staff for sites to be removed from the filtered list will be considered by the SLT and ICT leads.

11.10. School ICT technical staff regularly monitor and record the activity of users on the school ICT systems.

11.11. An appropriate system is in place for users to report any actual/potential E-Safety incident to the Headteacher.

11.12. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system.

12. Curriculum

12.1. E-Safety is a focus in all areas of the curriculum and staff reinforce E-Safety messages in the use of ICT across the curriculum.

12.2. In lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

12.3. Where pupils are allowed to freely search the internet, e.g., using search engines, staff are be vigilant in monitoring the content of the websites the young people visit.

12.4. It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT lead and Headteacher can, if agreed, temporarily remove those sites from the filtered list for the period of study. Any request to do so, is auditable, with clear reasons for the need.

12.5. Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

12.6. Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

13. Communication of Policy

13.1. Pupils

13.1.1. Pupils are informed that Internet use is monitored.

13.1.2. A planned E-Safety programme is provided as part of ICT/PHSE /other lessons and is regularly revisited – this covers both the use of ICT and new technologies in school and outside school.

13.1.3. Key E-Safety messages are reinforced as part of a planned programme of assemblies.

13.1.4. Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

13.1.5. Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

13.1.6. Pupils are made aware that there will be consequences to any E-Safety breach.

13.2. Staff

13.2.1. All staff are given the School E-Safety Policy and its importance explained.

13.2.2. Staff are aware that Internet traffic is monitored and traced to the individual user.

13.2.3. Staff act as good role models in their use of ICT, the internet, and mobile devices.

13.2.4. An audit of the E-Safety training needs will be included as part of the general ICT training needs review process. It is expected that some staff will identify E-Safety as a training need within the performance management process.

13.2.5. All new staff receive E-Safety information as part of their induction programme, ensuring that they fully understand the school E-Safety policy.

13.2.6. The Head teacher/ICT lead will provide advice/guidance /training as required to individuals as required.

13.2.7. Discretion and professional conduct is essential always.

13.2.8. Staff are permitted to use their own computing equipment (not including mobile phones) to work with however NO data pertaining to pupils or personal information of other persons/staff may be stored locally upon that system. Storage drives are provided for such storage both on and off the site (Office 365 One Drive). Similarly, data stored upon external storage or removable drives is not permitted unless encrypted/password protected.

13.2.9. Staff are aware that personal computing items if used for school purposes are done so at their own risk in terms of damage or loss.

13.2.10. Staff are aware of the procedures and consequences of any E-Safety breach.

13.3. Parents

13.3.1. Parents' attention will be drawn to the School E-Safety Policy during the admission process, on the school website, in newsletters and parents evening.

14. Linked Policies

14.1. Data Protection Policy – GDPR

14.2. GDPR Parental Consent