Patcham Infant School

E-Safety Policy

June 2017

Patcham Infant School

E-Safety Policy

This Policy should be read in conjunction with our Safeguarding Policy, Behaviour Policy and Staff ICT protocols document

1. Why is internet use important?

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for children who show a responsible and mature approach to its use.
- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience.

11. How will internet access be authorised?

- At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised internet access.

2. How does the internet benefit education?

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;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;

- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfE.
- Mentoring of pupils and provide peer support for them and teachers
- Access to and use of the Learning Platform.

3. How will internet use enhance children's learning?

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, evaluation and retrieval.
- The Learning Platform will provide good home and school links.

4. How will pupils learn to evaluate internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Leader.
- The school will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Staff must view sites before use with children.
- Pupils are taught about internet safety.

5. How will e-mail be managed ensuring safety for pupils?

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail. Any form of bullying or harassment is strictly forbidden
- Pupils must not reveal details of themselves or others in e-mail communication or via a personal web space, such as address or telephone number, or arrange to meet anyone.

- Whole-class or group e-mail addresses should be used at Key Stage 1 and below.
- The forwarding of chain letters is not permitted.

6. How should Website/Learning platform content be managed?

- The point of contact on the website/Learning Platform should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- All photographs of children displayed on the internet (including the website/Learning Platform) will only be shown with parental consent.
- Pupils' full names will not be used anywhere on the website/Learning Platform, particularly in association with photographs.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce it has been obtained.

7. File sharing, e-mail lists and forums

- File sharing sites will not be used or accessed, including programs that use file sharing and bit torrents.
- Access to forums that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted.

8. Pupil Chat and instant messaging

- Pupils will not be allowed access to public or unregulated chat rooms at any time during school hours.
- Pupils will not access social networking sites for example 'Facebook' or 'Twitter'.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.

9. Social Networking Sites

- It is expected that all staff and governors bear in mind their professional obligations whilst using such sites in any capacity and consider whether this communication is appropriate for the public domain. All users should be aware that even with enhanced security settings profile page pictures and information can be readily accessed by anyone.
- Whilst primary aged pupils are not allowed to create their own accounts there have been an increasing number of instances where this has happened. It is clearly inappropriate for staff to communicate with pupils, parents and carers through this very personal medium and the onus is on each user to ensure this doesn't happen.
- In order to protect the interests of all parties we have the following code of conduct:
    - Staff and governors must not accept pupils as friends which could be construed as being part of a "grooming process" in the context of sexual offending.
    - Staff and governors must not post of any communication or images which links the school to any form of illegal or inappropriate conduct which may compromise or damage the reputation of the school. This includes defamatory comments.
    - Staff and governors must not disclose confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
    - Staff and governors must not post images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.
    - Staff and governors must not make reference to children, the school, colleagues or anything relating to the school community whilst on social network sites.
    - Staff and governors are strongly advised not to 'make friends' or communicate with parents and carers via social networking sites as this may lead to compromising situations.
    - We strongly advise that parents and carers refrain from contacting staff members to avoid any compromising situations
    - All users are strongly advised to check their security settings to avoid unwanted access.
    - Deviation from this code of conduct may result in disciplinary procedures.
    - Pupils are taught throughout the school about sensible online practice including such sites particularly the protection of their personal details.

- Parents must not post images of Patcham Infant children, other than their own, whilst engaged in school activities.

10. Personal websites and blogs

- When publishing material to websites and elsewhere, pupil's comments will be monitored. Children should consider the thoughts and feelings of those who might view the material.
- Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable and will not be published.

11. How will the risks of e-safety be assessed?

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils.
- The school will take all reasonable precautions to ensure that users access only appropriate material. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored by the Governors Safeguarding Committee.
- Guidance will be sent out to parents at the beginning of each new academic year about E-safety.

12. How will filtering be managed?

- The school will work in partnership with parents, the LA and the DfE to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Leader/ administrator.
- The ICT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the L.A ICT helpdesk.

13. How will E-safety be introduced to pupils?

- Pupils will be informed that internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.
- A lesson on responsible internet use will be included in the PSHE
- Programme and ICT teaching, covering both school and home use.

14. Working in partnership with parents

- Parents' attention will be drawn to the School E-safety Policy in newsletters and on the school website/Learning Platform.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents on the website/learning platform.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children, through the school newsletters and Learning Platform.
- Parents/carers of children under 16 years of age will generally be required to sign an acceptable use policy on behalf of the child – home school agreement.
- Children under 8 years of age must be supervised by an adult when accessing the internet.

15. How will ICT system security be maintained?

Local Area Network security issues include:

- ✓ The school ICT systems will be reviewed regularly with regard to security.
- ✓ Virus protection will be installed and updated regularly.
- ✓ Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- ✓ Personal data sent over the internet will be encrypted or otherwise secured.
- ✓ Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed.
- ✓ Portable media may not be brought into school without specific permission and a virus check.
- ✓ Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- ✓ Files held on the school's network will be regularly checked.

- ✓ The ICT technician will ensure that the system has the capacity to take increased traffic caused by internet use.

16. How will complaints regarding internet use be handled?

- Responsibility for handling incidents regarding children and staff will be delegated to the headteacher.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.

Sanctions available include:

- interview/counselling by headteacher;
- informing parents or carers;
- removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including the Learning Platform.

E-safety Issues and Staff Responsibilities

The use of photographic, video and audio technology

- Staff may use school photographic or video devices (including digital cameras and camcorders) to support school trips and curriculum activities.
- Staff should not use their own personal camera/phone to take photographs or videos at school or on school trips.
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.
- **It is not appropriate to use photographic or video devices in changing rooms or toilets.**
- Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.

Safeguarding Issues: **(to be read in conjunction with Professional Responsibilities document)**

Important issues to consider:

- E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, **both in and out of school.**
- All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care.

- Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.
- Staff should not take photographs of children home, including those on memory sticks and cameras, in order to protect themselves from any child protection related issues.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- If staff need to email a parent/carer or pupil they should only use official school provided email accounts to communicate with them, which should be approved by the Senior Leadership Team beforehand.
- No document where a child can be identified can be sent by email without notifying the Headteacher first.
- Personal communication through email, messaging or any other social networking site between staff and pupils should not take place. Only communication through a learning platform or the school's website/email service is permitted.
- Access in school to external personal e-mail accounts may be blocked.

Other issues for staff to consider

- The use of user logins and passwords to access the school network must be used and maintained. All passwords must remain private to the individual.
- Any emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

- If any members of staff discover unsuitable sites, the URL will be reported to the ICT technician and head teacher who will then record the incident and escalate the concern as appropriate.

- Only members of the current pupil, parent/carers and staff community will have access to the website/ Learning Platform, from Reception to Year 2.

- The use of mobile phones and other personal devices by staff in school will be decided by the school.

- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

All staff must have read, understand and abide by the statements in this policy.
All new staff will be taken through the key parts of this policy as part of their induction.
All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School e-Safety Policy, and have its importance explained by the ICT Co-ordinator.

Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.

Approved by Governors on: Autumn 2017	Revision date: Autumn 2019