Holland Junior School
The Pioneer Academy

E Safety Policy

Date of reviewed: September 2023
Date of next review: September 2025

School Vision

At Holland Junior School we are a happy, friendly and caring school at the heart of our community. Hand in hand with our families, we have high expectations which nurture the successes, growth and happiness of every child. Children will leave our school with lasting memories and the skills to blossom in their future.

Writing and reviewing the E-safety policy

The E-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- *The school's Head Teacher, Deniece Graham will also act as E-Safety Officer.*
- Our E-Safety Policy has been written by the school, in accordance with Government guidelines. It has been agreed by senior management and approved by governors.

Teaching and Learning
Why Internet use is important

- 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school internet access is designed expressly for pupil use and includes filtering systems to support safe use.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access
Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is updated regularly.
- Advice on security strategies will be monitored and clarification or advice will be sought as necessary.

E-mail

- Pupils may only use approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- No content should be added to the site without the head teacher's approval

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified – consent will be obtained.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- Inappropriate sites shall be blocked.
- Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school should be carefully monitored and is inappropriate for primary-aged pupils.

Managing filtering

- The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Officer.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions
Authorising Internet access

- Access to the Internet will be through directly supervised access to specific, approved online materials.
- Parents will be asked to sign and return a consent form.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the E-Safety policy to pupils

- E-safety rules will be posted around the school and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be asked to sign an acceptable use agreement.

Staff and the e-Safety policy

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be asked to sign an acceptable use agreement.

Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school Web site.
- Parents will receive a copy of their child's acceptable use agreement and will be asked to go through it with their child.
- Parents will sign an agreement to confirm they understand the school's procedures on acceptable use of the Internet and will support the school's E-Safety policy.

Failure to Comply

- Failure to comply in any way with the policy will be considered as a serious risk to children's wellbeing and safety and all incidents of non-compliance will be investigated by a senior member of staff.

Monitoring/review of ICT and E-Safety policy

This policy will be regularly evaluated and updated in accordance with the School Development Plan to ensure that:

- All new staff are aware of the current practice in ICT.
- New developments and initiatives are taken into account.

- Ideas of new staff are incorporated.
- Policy and practice are matched.

Staff ICT Acceptable Use Agreement

ICT is a part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Child Protection Officer.

- I accept full responsibility for the security of all ICT hardware allocated to me. I understand that this responsibility extends to all data on the hardware.

- If remote access to the school network is available, I understand that I am fully responsible for the secure use of that facility.

- Under no circumstances will I allow anyone, including members of my family, to use or have access to ICT equipment allocated to me.

- I understand that the ICT equipment allocated to me is not for personal use; otherwise it will become a taxable benefit.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

- I will not browse, download or send materials that are illegal or could be considered offensive.

- I will ensure that all electronic communication with pupils and staff is compatible with my professional role.

- I will report any accidental access or receipt of inappropriate materials, or filtering breach, to the Child Protection Officer and the ICT coordinator.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that personal data (such as data held on SIMS) is kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely.

- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent / carer. Only devices provided by the school can be used to record digital pictures.

- I will not use any other form of mobile storage for transferring images of pupils or staff to outside sources without permission.

- I will respect copyright and intellectual property rights.

- I will not engage in any online activity that may compromise my professional responsibilities, i.e. due care and consideration should be taken when using websites such as 'Facebook'.

- I understand that all my use of the Internet (including email) and the network can be monitored by my Line Manager or Head teacher.

- I will support and promote the school's safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature……………………………………………………………… Date………………………………………

Full name………………………………………………………………………………………………………

Key Stage 2
Pupil Acceptable Use Agreement

Dear Parent / Carer,

ICT has become an important part of learning at our school. We expect all children to be safe and responsible when using ICT.

- I will only use ICT in school for school purposes.

- I will make sure that any ICT contact I have with adults and children is polite and friendly.

- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my monitor and tell my teacher immediately.

- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher or a responsible adult.

- I will not open an attachment or download a file unless I have permission and I know and trust the person who has sent it.

- I will not give out my own details such as my phone number or home address.

- I will never arrange to meet someone I have only ever previously met on the Internet or by email unless this is part of a school project approved by my parent / carer and my teacher, and a responsible adult comes with me.

- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

- I know that my use of ICT can be checked and that my parent / carer will be contacted if a member of school staff is concerned about my E-Safety.

Signature _____

Date_____

Parent/Carer E-Safety Agreement Form

Parent/guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the internet, Learning Platform and other ICT facilities at school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent them from accessing inappropriate materials. These steps include an educationally filtered service, restricted access e-mail, employing appropriate teaching practise and teaching E-Safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their E-Safety they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's E-Safety.

Parent / Carer Signature: _____

Date: _____