Potters Gate CE Primary School and St. Andrew's Infant School

Review Period:	Annual
Next Review Due:	November 2024
Local Committee Lead	Safeguarding
Staff Lead	E-Safety Lead

E- Safety Policy

This policy is created to ensure that all pupils are taught to be aware of safety online. This takes into account increased use of online use through Teams, when necessary.

Teaching and learning

- The Internet is an essential element in life for education, business and social interaction. We have a duty to provide students with quality Internet and digital access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- 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 shown how to publish and present information appropriately to a wider audience.
- Pupils will be taught how to evaluate Internet content
- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content
- Pupils will be taught how to store information securely and safely

Managing Internet Access

- School computer systems security will be reviewed regularly.
- Staff will alert the DSL team if inappropriate material or content has not been filtered.
- Virus protection will be updated regularly.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- 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.
- Staff to pupil email communication must only take place via a school email address and will be monitored.
- Class teachers will be provided with a class email address for communication with parents and carers.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will monitor e-mails from a school account to another school account for safeguarding reasons. All e-mails from a child's e-mail account to an external account will be blocked and a notification to the IT manager will be sent.
- Notifications will be sent to the IT manager when a child e-mails another internal e-mail account.

- Notifications will be sent to the IT manager when an adult e-mails a pupil e-mail address. This is a safeguarding measure
- The forwarding of chain letters is not permitted.
- All Pupils will be provided with a personal school email address for the purpose of accessing remote learning on Teams only.

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 and designated office staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names and personal information will not be published on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or any other publication.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- Staff will be given a copy of children whose parents have asked for photographs to not be published.
- Image file names will not refer to children by name
- Parents will be informed of the procedures regarding image taking and must follow school policy as outlined above.

Social networking and media

- The school will control all access to school social media and website accounts
- Publishing of children's work and images will follow the same guidelines as stated above
- Pupils will be advised to never give out personal information of any kind on social media which could lead to risks
- Pupils and parents will be advised of the risks the use of social media can have and the potential dangers it poses to children.
- All rules and guidelines will be followed by all that access social networking and media sites as outlined by the relevant body

Managing filtering

- The school will work in partnership with The Good Shepherd Trust to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the coordinator.
- Senior staff will ensure that regular checks are made to ensure that the monitoring and filtering methods are reviewed and reported to the Local Committee.

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 and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Staff will use a school phone where contact with pupils is required.
- Each class has their own class iPad for the purpose of taking pictures of learning during lessons and external visits.
- All staff to be aware that many forms of technology can operate without wi-fi (use of hubs) and are therefore not filtered by the school system.
- All technology used in school for the purpose of teaching and learning should be used via the schools wi-fi internet
- Parents and teachers to be aware that many new gaming services and consoles are able to operate remotely of Internet access and therefore relevant privacy and safety settings should be in place
- The use of individual mobile phones and other technology shall not be used for teaching and learning
- All content should be stored in accordance with school guidelines
- Content should not be sent or received via Bluetooth, Airdrop (Apple or android devices), Quickshare (Samsung devices)
- Communication with parents and carers and accessing children's work should be done so via a school computer or laptop and not by personal devices.

Remote teaching and learning: setting and accessing work (COVID-19)

- All Children will be given individual school email addresses for the purpose of accessing the content on Teams
- Teachers will upload relevant work and content using the class Teams account
- Individual communication will be through the class email address
- All work will be sent to children via Teams, and children will be able to upload their responses and relevant tasks for teachers to see
- Individual feedback will be provided against the work uploaded
- Work and resources set via Teams is for the use of school learning for the individual classes or pupils
- Communication via the chat area of Teams is visible to all that have access to that group and therefore should not refer to individual children or their work by staff or parents
- Children in Reception will continue to use Tapestry with the use of Teams for live sessions only

Remote teaching and learning: live teaching (If applicable)

- Live sessions will take place via Teams during the event of remote learning
- Teachers will ensure that the background of where they are videoing and content is appropriate at all times.
- Teachers to be dressed appropriately for remote teaching, with the same expectations as there are in school
- Children will be dressed appropriately for the 'school' day at home

- Children will be in a suitable and appropriate location when attending live sessions. They are not to be in bedrooms etc.
- Parents/Carers will be expected to be in the same room as children when they are attending a virtual lesson.

Remote teaching and learning: risks and storage of information (COVID-19)

- All content will be stored in accordance with the e-safety policy as it would be in school.
- The login details for all those that can access the class Teams page will not be shared and stored safely.
- All teachers have been given training on the use of Teams and the expectations should the need for remote learning take place.
- A remote learning plan has been shared with all parents, outlining expectations and how to use Teams safely.
- Children will be reminded of the schools e-safety procedures that are followed in class
- Children will be reminded of how to access and share work via Teams
- The first live session via Teams will focus on e-safety, setting rules and guidelines to follow as a class as they would be in school at the start of each half term

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) 2018.

Policy Decisions

- The school will maintain a current record of all staff and pupils who are granted access to school computer systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials using computers, laptops or iPads.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'Acceptable Use Policy' before being allowed to access the internet from the school site.
- All members of staff will be asked to sign an 'acceptable use' policy, annually in September following Safeguarding training.

Assessing risks

- 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 SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

- Staff will report any material of concern to the relevant e-safety lead to ensure that it can be monitored and filtered in future.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff, who will also be a DSL trained staff member.
- Any complaint about staff misuse must be referred to the head teacher, in line with KCSIE (September 2022)
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet, in line with the school behaviour policy.
- Any concerns relating to e-safety, computing or technology will be reported using Cpoms, by the class teacher or relevant member of staff. Parents will be informed of any e-safety concerns, through an e-safety concern note home. In more serious cases the school will meet with parents to discuss e-safety concerns with their child.
- Class teachers to be aware of new and relevant technology and the concerns it causes, this is to be addressed, where relevant, in class.
- Any concerns raised by a parent to a member of staff will be reported in the same manner as above.
- Class teachers will regularly address the concerns through a purpose taught e-safety lesson to raise children's awareness

Community use of the Internet

All use of the school Internet connection by community and other organisations shall be in accordance with the school e-safety policy.

Communications Policy

- Appropriate elements of the e-safety policy will be shared with pupils.
- E-safety rules will be posted in all networked rooms and referred to regularly.
- Pupils will be informed that network and Internet use will be monitored and all misuse and concern will be reported.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils.
- All children will participate in the annual Safer Internet Day to raise awareness of correct and safe use of technology and the Internet.
- Key elements of the e-safety policy will be referred to specifically, such as the use of logins, communication and storing of work and images when using Teams
- In Key Stage 2, children will be given an introduction to using their school emails, before the event of remote learning, highlighting the importance of keeping login details safe and the acceptable use of email
- All email communication will be monitored

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 will be monitored and traced to the individual user. Discretion and professional conduct is essential, in line with Keeping Children Safe in Education September 2023
- The e-safety policy will be shared on the class files page for Teams to allow parents and children to remind themselves of the procedures to follow and how to keep themselves and others safe whilst online.

Enlisting parents' support

- Parents and carers will be invited to attend an e-safety information meeting, which could be remotely through Zoom.
- Parents and carers will from time to time be provided with additional information on e-safety, through a termly newsletter created by the E-safety leader.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents will be sent notifications if a child reports inappropriate online activity in line with our Behaviour and relationships policy
- Parents will be able to communicate with class teachers via the individual class email addresses or more appropriately the class e-mail address.

Linked Policies

Behaviour Policy

Anti-Bullying Policy

Staff Code of Conduct Policy

Acceptable Use Policy