Pownall Green Primary School

Love learning, love life!

Acceptable use and eSafety Policy

Subject Leader(s):	**Sarah Seymour Smith**
Aligned governor:	
Policy reviewed:	**September 2021**
Next Review:	**September 2022**

This policy should be read alongside other policies of the school, particularly:

Teaching and Learning Policy
ICT policy
Anti-Bullying Policy
Remote Learning Policy
Safeguarding Policy

The school has appointed the computing coordinator as the eSafety coordinator. Our eSafety Policy has been written by the school. It has been agreed by the senior leadership team and School Governing Body

The eSafety Policy will be reviewed annually. This policy will next be reviewed in **September 2022.**

Why is Internet use important?

The purpose of Internet use in school is to enhance teaching and learning, raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning for staff and pupils. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access as part of their learning experience and is part of our vision to create a safe, e-confident school.

Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient
- Access to world-wide educational resources
- Educational and cultural exchanges between students world-wide
- Access to experts in many fields for students 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;
- Exchange of curriculum and administration data with the Local Authority and DES

How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for student use and includes filtering by Stockport (Local Authority) appropriate to the age of students.
- Students 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 students in on-line activities that will support learning outcomes planned for the students' age and maturity
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Authorised Internet Access

- The school is forensically monitored.
- The school will maintain a list of all staff held and students who are granted Internet access
- All staff must read and sign the 'Staff Information Systems code of conduct' before using school ICT resources, including the internet. (appendix 1)
- Parents will be informed that students will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form for student access
- KS2 students must agree to comply with the 'Safety on the Internet and Responsible Use of Computers' document (Appendix 2). This will be visited every September with the students in class and displayed in the computing suite.

Evaluation of Internet content

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to ICT subject leader for appropriate action then reported to Stockport LA.
- School will ensure that the use of Internet derived materials by students and staff complies with copyright law
- Pupils will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

Email

- Students may only use approved e-mail accounts on the school system. Students do not have personal email accounts in school.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- Pupils will be taught how to safely send and receive appropriate emails as part of their curriculum

Password Protection

Passwords may be issued by school to staff and students. For example, email, Blog and school network.

- Staff are encouraged to change their passwords on a regular basis.
- Students must not disclose passwords to other students.

Social Networking

- The School will not allow pupil access to social networking sites and newsgroups unless a specific use is approved (for example, forums posted on the blog)
- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students should be advised not to place personal photos on any social network space and place all privacy settings on high
- Staff are to be aware of guidance related to their own personal use of social networking sites (Please see staff handbook)

Live online lessons (see remote learning policy)

Live online lesson protocols will be shared with staff, students and parents. Parents and staff will be required to read and acknowledge these protocols.

Communication with parents

Communication with parents will be through SIMS, the year group email address and phone calls *(using the school line).* It will not be through personal, work email addresses or personal phone numbers. Staff may also communicate through Google Classroom if a question is raised about an assignment.

Filtering

The school will work in partnership with the Local Authority to ensure filtering systems are robust and as effective as possible. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the LA via the computing lead.

USB memory sticks & other Portable Data Storage Devices

- Staff must consider what data should be stored on USB sticks/other data storage devices
- Sensitive data should be encrypted.

Remote access to the school system.

- Staff will have to sign the Remote Access Agreement before they are allowed to access the school systems from a remote site (appendix 3)
- They will have to adhere to the agreement in full.

Use of Digital Cameras/computing equipment to take photographs

- Staff to use only school cameras/iPads to photograph students.
- Staff must not use personal equipment to photograph students.
- Storage cards to be cleared when pictures have been uploaded to the school network.
- Staff must check consent for use of photographs within school and other school run platforms e.g. website.

Storage of Photographs

- Photographs to be stored in secure area within school network.
- Photographs to remain on school premises (when practicable –i.e. off-site school trips – images only to be downloaded to school network.)

- Photographs to be deleted when no longer required.
- Current LA policy is adhered to regarding photographing & publishing images of children.
- Publishing of photographs will only be done with parental permission

Mobile Phones & Other Hand Held/Communication devices

- Mobile phones & other hand held communication devices must not be used for personal use in the lesson or formal school time (students & staff).
- Students must hand in their mobile phones at the start of the day and these will be returned at the end of the school day.
- Mobile Phone – Bluetooth should be turned off and mobile switch off in lesson time.
- Sending of abusive or inappropriate messages is forbidden.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the safeguarding officer and agreed by the governing body, before use in school is allowed.
- Mobile phones/ handheld communications devices/ gaming consoles will not be used for personal use during lessons or formal school time.

Website content and management

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published
- The computing coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include students will be selected carefully and will be appropriate for the context
- Students' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site or blog.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with the Local Authority
- Also see the use of 'USB memory sticks and other portable storage devices' section.
- Data will be backed up daily remotely and securely through the school's annual purchase of an SLA from Stockport Council's ICT team.

Protecting Personal Data

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

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 Stockport Council can accept liability for the material accessed, or any consequences of Internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence. The school will audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate every 12 months.

Handling eSafety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff, Safeguarding officer or Headteacher
- Any complaint about staff misuse must be referred to the Headteacher, or to the Chair of the Governing Body of the complaint is regarding the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding policy and a DSL informed immediately.
- Pupils and parents will be informed of the complaints procedure

ICT and Internet use across the school community

Students

- PSHE/Outside agencies/embedded across the curriculum
- Age appropriate sessions during the school's annual e-safety lesson and the curriculum.
- Safe and responsible use is reinforced throughout the curriculum, emphasized on the website and at all times during the school year. When using ICT resources and the internet, staff should take the opportunity to reiterate safe and appropriate usage with students.

Staff

- All staff (teaching & non teaching)
- Outside agencies/LA
- INSET

Governors

- Outside agencies/LA
- INSET

Parents

- Parents' attention will be drawn to the school e-safety guidance in newsletters, curriculum documentation, curriculum meetings and the school website.
- A partnership approach with families will be encouraged. This may include: demonstrations, practical sessions and suggestions for safe internet use at home.

Communication of Policy

Students

- Rules for Internet access are visible in school and are discussed at the beginning of each year with the students. They then sign a poster that is displayed in the computing suite.
- Students will be informed that Internet use will be monitored

Staff

- All staff will be emailed a copy and asked to read through it at the beginning of each academic year with its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Professional integrity and conduct is essential
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues

Governors

- Policy will be discussed and ratified by the Governing Body.

Parents

- Parents’ attention will be drawn to the School eSafety guidelines in newsletters, the school brochure and on the school website.

Visitors

- Rules for visitors are clearly displayed (i.e. use of mobile phone/camera/film equipment etc) at the school reception desk.

Pownall Green

Primary School

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's eSafety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer/laptop for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission from the ICT coordinator or Headteacher.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school eSafety Coordinator and the Designated Child Protection Coordinator (Headteacher).
- I will ensure that any electronic communications with students are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I understand that I must ***NEVER*** use my personal email account or email address to communicate with students or their families.
- All images will be stored on the central server in school in the designated folder and managed effectively.
- I am aware of the rules for computer and internet usage for pupils; I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will only use age-related, designated search engines with pupils and will supervise children using the internet at all times.
- I will not use personal equipment (such as cameras/mobile phones etc) to take or store images of pupils.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ………………………………………… ………… Print Name: ………………………………………………

Date: ………………………………

Pownall Green Primary School

Remote Access Agreement
Pownall Green Primary School

This remote access policy defines standards for connecting to the school's network and security standards for computers that are allowed to connect to the school's network. This policy is designed to prevent damage to the school network or computer systems and to prevent compromise or loss of data.
Only upon approval will the account settings be changed to allow remote access.

Remote Computer Requirements

- You must have a recognised and up-to-date anti-virus product operating on the computer at all times.
- The computer must be protected by a firewall at all times when it is connected to the internet.
- You must have a robust password.

Individuals must not:

- Allow anyone else to use their user ID / password.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access the school's network.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to the systems or information.
- Attempt to access data that they are not authorised to use or access.
- Give or transfer data or software to any person or organisation.

I agree to the above terms. I understand that failure to adhere to the above terms may lead to disciplinary action.

Name: ______________________
Signed: _____________________
Date: ________________________

Pownall Green Primary

ICT Safe Rules

S - I will only use the internet when my teacher or an adult is in the room.

A - I will only click on buttons and links when I know it is safe.

F - I will ask a teacher or an adult before I print anything.

E - If I see something I don't like on the screen, I will always tell an adult.

I am going to use the computer sensibly and safely in school.

Pownall Green Primary

ICT Safe Rules

S **Safe** Do not give out personal information.

M **Meeting** someone can be dangerous. Remember online 'friends' are still strangers.

A **Accepting** emails, files, messages may contain viruses or nasty messages!

R **Reliable** Someone online might lie and information on the internet might not be true, Check it!.

T **Tell** someone if you feel uncomfortable or worried about something.

- I will ask before I print.
- I will look after the equipment in school.
- I will only use my own log in account.
- I will use the VLE for the correct purpose.