Arden Primary School

eSafety Policy

The school has appointed the ICT Subject Leader as the eSafety coordinator. The implementation of this policy is the responsibility of the Headteacher, Subject Leader and all teaching staff. The eSafety Policy will be reviewed and updated annually in the light of new initiatives. This will be done by the coordinator in consultation with the Headteacher, staff and governors. This policy will next be reviewed in March 2016.

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 administration systems.

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

Pupils 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 including museums and art galleries;

•   Educational and cultural exchanges between students 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;

•   Exchange of curriculum and administration data with the Local Authority and The Department for Education

How Can Internet Use Enhance Learning?

- The school Internet access is designed expressly for pupil use and includes 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 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, retrieval and evaluation

Authorised Internet Access

- The school will maintain a current, electronic record of all staff and pupils who are granted Internet access
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource (Appendix A)
- Parents/carers will be informed that pupils will be provided with supervised Internet access
- Parents/carers will be asked to sign and return a consent form for student access (Appendix B)
- Pupils must apply for Internet access individually by reading the ARDEN PRIMARY SCHOOL E-SAFETY RULES FOR RESPONSIBLE INTERNET USE document (Appendix G) and then agreeing to comply and sign the Responsible Internet Use statement (Appendix C).

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to E-safety co-ordinator and recorded in the eSafety log (Appendix D)
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law
- Pupils are taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

Email

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher/teaching assistant 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
- 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
- The forwarding of chain letters is not permitted

Password Protection
- The school issues passwords to all staff
- Staff are encouraged to change their passwords on a regular basis
- Generic passwords are not used

Social Networking
- The school blocks/filters access to social networking sites and newsgroups
- Pupils are not allowed on social network sites in school or using school equipment
- Pupils are advised never to give out personal details of any kind which may identify them or their location
- Pupils are advised not to place personal photos on any social network space
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others

Filtering

- Internet access is controlled, maintained and filtered by our Internet Service Provider (ISP) which is Stockport MBC

Video Conferencing
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call
- Videoconferencing will be appropriately supervised for the pupils' age

USB memory sticks & other Portable Data Storage Devices
- Staff to consider what data should be stored on USB sticks/other data storage devices
- Sensitive data should be encrypted

Digital Cameras
- Staff must only use school cameras to photograph pupils
- Staff must not use personal equipment to photograph pupils
- Storage cards must be cleared when camera returned

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 to be downloaded only to school network
- Photographs to be deleted when no longer required
- Current LA policy is adhered to regarding photographing & publishing images of children

Mobile Phones & Other Hand Held/Communication devices

- Mobile phones & other hand held communication devices are not be used for personal use in the lesson or formal school time (pupils & staff)
- For the purpose of security, we recognise that parents/carers of KS2 children may want their child to bring a mobile phone to school. If this is required, at the beginning of the school day, all phones will be turned off and handed to the class teacher who will keep them in a safe place until the end of the day when they will be handed back to the child. Children are only allowed to turn on their mobile phone when outside the school grounds. Parents/carers will be asked to sign a consent form to authorise their child to bring a phone to school. (Appendix D) **Full responsibility for the phone will rest wholly with the parents/carers.**KS1 children are not allowed to bring phones to school
- Mobile Phone Bluetooth should be turned off
- Sending of abusive or inappropriate messages is forbidden
- Outside school hours, children are discouraged from taking mobile phone photographs and videos on the grounds of an infringement of personal privacy, image and child protection

Managing Emerging Technologies

- Emerging technologies are 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 are not used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff members' or pupils' personal information will not be published
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will be appropriate for the context
- Pupils' 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 pupils are published on the school Website
- Work will only be published with the permission of the pupil and parents

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

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 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.
- 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

Adopted :March 2015
Review: March 2017

Communication of Policy

Pupils

- Rules for Internet access will be posted in the ICT classroom and in all classrooms (Appendix G)
- Pupils will be informed that Internet use will be monitored
- Each class will display a copy of the rules for internet use and display a copy of the pupil agreement form.

Staff

- All staff will be given the School eSafety 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 who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues

Governors

- Responsible Use Policy (governors to ratify)

Parents

- Parents'/carers' attention will be drawn to the School eSafety Policy in newsletters, the school brochure and on the school website

Visitors

- Visitors to school will be informed about the eSafety policy at the reception desk, where appropriate
- Rules for visitors clearly displayed (i.e. use of mobile phone/camera/film equipment etc)

Training

Pupils

- PSHCE/Outside agencies/embedded across the curriculum
- Age appropriate

Staff

- All staff (teaching & non teaching)
- Outside agencies/LA
- Yearly review of training
- INSET

Governors

- Outside agencies/LA
- Yearly review of training

Parents/Carers

- Sessions/workshops for parents

Parents/Carers

- Sessions/workshops for parents

Appendix A

Staff Information Systems Code of Conduct

To ensure that staff members are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff members 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 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 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.

- 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 or the Designated Child Protection Coordinator to be recorded in the school's eSafety log

- I will ensure that any electronic communications with pupils are compatible with my professional role.

- I will promote eSafety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

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 being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

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

Signed: …………………………………………. Printed: ………………………………………………… Date: ……………

---

eSafety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the eSafety Rules have been understood and agreed.

Parent's/Carer's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names

Parent's/Carer's Consent for Internet Access

I have read and understood the school eSafety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. My child & I know who to talk to if we have any concerns about e-safety.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	Date:
Please print name:	
Please complete, sign and return to the school	

Pupil/Parent RUP

E-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the E-Safety Rules have been understood and agreed.

Class:_____

Pupils' Agreement

• I have read and I understand the school e-Safety Rules.

• I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.

• I know that network and Internet access may be monitored.

• I know who to talk to if I see something online or receive a message I'm not happy with.

Signed…   Date_____

eSafety Incident Log

Date	Staff	Incident	Action

eSafety Incident Log

Appendix E: Mobile phone consent form

Arden Primary School

Parent/carer, please sign below and return to school – thank you

I consider it necessary for my child to bring a mobile phone into school. Therefore, I give my permission. I accept full responsibility for the phone.

Child's name …………………………………………………………………………. Class …………

Parent/carer signed ………………………………………………………………………….

Date …………………………………………….

✂……

Arden Primary School

Parent/carer, please sign below and return to school – thank you

I consider it necessary for my child to bring a mobile phone into school. Therefore, I give my permission. I accept full responsibility for the phone.

Child's name …………………………………………………………………………. Class …………

Parent/carer signed ………………………………………………………………………….

Date …………………………………………….

✂……

Arden Primary School

Parent/carer, please sign below and return to school – thank you

I consider it necessary for my child to bring a mobile phone into school. Therefore, I give my permission. I accept full responsibility for the phone.

Child's name …………………………………………………………………………. Class …………

Parent/carer signed ………………………………………………………………………….

Date …………………………………………….

Appendix F: eSafety Audit

This quick self-audit will help the senior leadership team (SLT) assess whether the eSafety basics are in place.

Has the school an eSafety Policy that complies with CYPD guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The eSafety Coordinator is:	
Has eSafety training been provided for both pupils and staff?	Y/N
Is the 'Think U Know' training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the school's eSafety Rules?	Y/N
Have school eSafety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Is Internet access provided by an approved educational Internet service provider and complies with Department for Education requirements for safe and secure access?	Y/N
Has the school filtering policy been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Are staff members with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	Y/N

Appendix F: Are you an eSafe school?

Do all your staff...	Does your school...
☐ Understand e-safety issues and risks? ☐ Receive regular training and updates? ☐ Know how to escalate an issue of concern? ☐ Know how to keep data safe and secure? ☐ Know how to protect themselves online? ☐ Know how to conduct themselves professionally online? ☐ Know about the updated e-safety guidance for QTS standard Q21: Health and well-being?	☐ Have a nominated e-safety co-ordinator? ☐ Audit its e-safety measures? ☐ Have a robust AUP? ☐ Use a Becta accredited supplier for internet services? ☐ Include e-safety measures in Section 4b of your SEF? ☐ Keep an incident log and monitor your measures? ☐ Handle cyberbullying issues well? ☐ Raise awareness of the issues, e.g. through holding an assembly?
Do your learners...	**Do your parents/carers and governors...**
☐ Understand what safe and responsible online behaviour means? ☐ Receive e-safety education at appropriate places across the curriculum? ☐ Get the opportunity to improve their digital literacy skills? ☐ Know the SMART rules? ☐ Know how to report any concerns they may have?	☐ Understand e-safety issues and risks? ☐ Understand their roles and responsibilities? ☐ Receive regular training and updates? ☐ Understand how to protect their children in the home?

Appendix G

ARDEN PRIMARY SCHOOL E-SAFETY

RULES FOR RESPONSIBLE INTERNET USE

At Arden Primary school we have computers, laptops and Ipads with Internet access to help us with our learning. These rules will keep everyone safe online and help us to be fair to others.

- I will not access other people's files;

- I will use the computers only for school work;

- I will not bring memory sticks, tablets or smartphones with internet access into school without permission;

- I will ask permission from a member of staff before using the Internet;

- I will not use my personal email or social media in school.

- I will not give addresses or phone numbers, or arrange to meet someone, unless my parent, carer or teacher has given permission;

- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or receive a message I do not like;

- I understand that the school can check my computer files and the Internet sites I visit.