Pensby Primary School

Acceptable use of the Internet & ICT & eSafety policy

Mrs K Brown September 2009 / July 2012 / July 2013/July 2014

Acceptable Use / eSafety Policy

Mrs K Brown is the member of staff responsible for eSafety in the school. Mr J Klausen supports Mrs Brown in this role and reports to her. Mr D Spencer is the named governor for eSafety in the school. Our Acceptable Use and eSafety Policy has been written by the school. It has been agreed by the senior leadership team and was approved by the governing body on in 2009. This policy will be reviewed annually and will next be reviewed in September 2014.

WHY IS INTERNET USE IMPORTANT?

The Internet is essential in the 21st Century for education, business and social interaction. It allows for information to be transmitted to many locations throughout the world. Messages can be sent, ideas discussed, and material published and viewed with very little restriction. These features make the internet an invaluable resource used by millions of people each day.

The purpose of internet use in school is to assist pupils to achieve increasingly high standards, to support the professional work of staff and to enhance the school's management. Benefits of using the Internet in education include:

- Access to numerous educational resources.
- Inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC).
- 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 material 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 LEA and DfES'
- The National Curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. As a consequence of this, to effectively deliver the curriculum, teachers need to plan to integrate the use of communications technology such as web based resources and e-mail to enrich and extend learning activities.
- Effective internet use is an essential life-skill for pupils to master.

PRINCIPLES OF INTERNET SAFETY:

In common with most technologies, Internet use presents risks as well as benefits. Pupils could be placed in inappropriate and even dangerous situations without mediated Internet access. To ensure responsible use and the safety of pupils the school's policy is built on the following four core principles:

Guided educational use:

Internet use will be planned, task orientated and educational within a regulated and managed environment.

HOW DOES INTERNET USE BENEFIT THE CURRICULUM AND SCHOOLS?

- 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 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 DCSF

HOW CAN INTERNET USE ENHANCE LEANRING?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of students
- 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

CONDITIONS OF INTERNET AND WWW USE

Personal Responsibility:

Internet safety depends on staff, governors, advisors, parents and where appropriate, pupils themselves taking responsibility for use of the Internet and associated technologies. The school will seek to balance education with responsible use, regulation and technical solutions to ensure pupils' safety. Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to a member of the SLT or Governing Body.

Regulation and Acceptable Use:

The use of the Internet, which brings with it the possibility of misuse, will be regulated. Fair rules, written for pupils to read and understand, will be prominently displayed as a constant reminder of the expectations regarding Internet use.
The school expects that staff will use new technologies as appropriate within the Curriculum and that staff will provide guidance and instruction to pupils in the use of

such resources. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the 'Network Etiquette and Privacy' (page 5) section of this policy provides suitable guidelines.

Authorised Internet Access:

- The school will maintain a current record of all staff and students who are granted Internet access
- All staff must agree and sign the Staff Information Systems Code of Conduct and acknowledge understanding and acceptable of the terms in the AUP and eSafety policy
- Parents/families will be informed that students will be provided with supervised Internet access
- Parents/families and pupils will be asked to sign and return a consent form for pupil access as detailed in the AUP policy before a pupil is given access

World Wide Web:

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to Headteacher and recorded in the schools eSafety Incident Log (see safety audit document) .
- Pensby Primary School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law
- pupils should be 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 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

Social Networking:

The School will should block/filter access to social networking sites and newsgroups unless a specific use is approved

- 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

- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others

NETWORK ETIQUETTE AND PRIVACY:

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other user's files or folders.
5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact a member of the SLT.
6. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
7. Disruptions – do not use the network in any way that would disrupt use of the network by others.
8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
9. Staff or pupils finding unsuitable websites through the school network should report the web address to a member of the SLT or Governing Body.
10. **Do not attempt to visit websites that might be considered inappropriate.**
11. Files held on the school's network will be regularly checked by a member of the SLT.
12. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

UNACCEPTABLE USE:

Examples of unacceptable use include but are not limited to the following:

1. Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
2. Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
3. Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless

anxiety. (The Local Authority have filters in place to block e-mails containing language that is or may be deemed to be offensive.)

4. Accessing or creating, transmitting or publishing any defamatory material.
5. Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
6. Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
7. Transmitting unsolicited material to other users (including those on other networks).
8. Unauthorised access to data and resources on the school network system or other systems.
9. User action that would cause corruption or destruction of other users' data, or violate the
10. Privacy of other users, or intentionally waste time or resources on the network or elsewhere.
11. Cyber-bullying

These rules are presented to the children in a child friendly format as in appendix A.

FURTHER PROTECTION OF STAFF AND PUPILS

Staff (and pupils) are users of technology and internet throughout the school. To protect them they are expected to adhere to the following:

Mobile phones:

Staff mobile phones should never be used within lesson times and should be switched off. Staff mobile phones must be kept in a secure area where pupils cannot see them. Staff mobile phone use should only take place at break times and pupils must not see staff using their mobiles phones.

Pupils are not permitted to bring mobile phones into the classroom, playground or other public areas. The may bring mobiles phones on the journey to and from school as agreed between then Headteacher and parents. If an agreement is made the pupil mobile phones is stored securely in the school office. To seek and agreement a family must complete a request for a pupil mobile phone to be allowed on the site.

USB/data sticks:

Staff will use USB to transfer data from home to school. Wherever possible the transfer of electronic files should happen via the schools VLE website which is secured and filtered. If staff use a USB they are responsible for ensuring it is not damaged and does not contain any elements that may compromise the school systems. At all times personal data about staff or pupils should not be transferred using a USB, unless the person is using an encypted USB provided by the school Pupils are not permitted to use data sticks/USB in school and are not allowed to bring these on site.

Social network sites
Staff are strongly advised to use SNS with extreme caution. They should never accept communication between a pupil or the family of the pupil. If a pupil or the family of a pupil attempt to contact them through their SNS they must inform the Headteacher immediately. Staff are advised to use the filters on SNS to ensure their personal details and images are not in the public domain. Pupils receive training about the responsible use of SNS. They are not permitted to access SNS in school or using school equipment.

Use of cameras/ DVD cameras / mobile phone cameras:
Staff should not use their mobile phones to photograph any children in any situation (see mobile phone section). Staff must take great care when photographing or filming pupils to ensure that they are doing so in a public area with other staff and pupils around. They should be clear with the pupils and inform them why the images are being taken and what will happen to the images. Staff must ensure that vulnerable children whose families do not wish them to be photographed are protected. Pupils are not permitted to bring DVD cameras/ mobile phone cameras / or other cameras on site at any time.

Search engines:
Staff should carefully use google as a search engine in school in view of pupils. Pupils should not use google as a search engine in school unless they are supervised by a memebr of staff. Staff should direct children directly to pages required or direct them to a safe search engine such as http://search.bbc.co.uk whenever possible. The school espresso package enables safe surfing and searching and should be used whenever possible. If a search does result in inappropriate content staff must report this to the Headteacher immediately using the ESafety - Incident Report (see safety audit document).

You Tube / site checking:
Sites such as You Tube must not be used within the school. If staff wish to use a videa from you tube they must save it from the site to block out any possible inappropriate content. Staff are advised to check all sites well in advance of a lesson to ensure it does not contain inappropriate content. Pupils are not permitted to access You Tube in school.

ADDITIONAL GUIDELINES

1. Users must comply with the acceptable use policy of any other networks that they access.
2. Users must not download software without approval from a member of the SLT.

services:
There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages

suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

School web site:
The school's web site is to celebrate children's work, promote the school and publish resources for children and parents at home. The point of contact on the web site is the school address, school e-mail and telephone number. Staff or pupils' home information will not be published. Photographs will only be published on the school web site of children who the school holds a photograph permission form for. No photographs will be published with full names. The contact details on the Web site will be the school address, e-mail and telephone number. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Other school publications:
The school publishes bi weekly newsletters, a termly magazine (Pensby Primary Post) and various other letters. Staff produce DVD's of the pupils as part of the curriculum and for competitions. Pupils photographs and images are only used with the permission of the family. Full names are not used alongside images and indeed the school avoids using any names against images wherever it can.

Publishing Students' Images and Work:

- Photographs that include students 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 annually before photographs of pupils are published on the school Web site
- Work can only be published with the permission of the pupils and parents

Network security:
Users are expected to inform a member of the SLT immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

Physical security:
Staff users are expected to ensure that portable ICT equipment such as laptops, digital/video cameras are securely locked away when they are not being used.

Wilful damage:
Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action

and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

Filtering:

The school will work in partnership with the Local Authority, and Becta to ensure filtering systems are as effective as possible.

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/ handheld communications devices/ gaming consoles will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden

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

Protecting Personal Data:

Personal data will be recorded, processed, transferred, stored 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 Wirral Metropolitan Borough Council can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the Internet/ Ict eSafety policy is adequate and that the implementation of the policy is appropriate.

Handling eSafety 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 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

Training

The staff, governors received training in October 2009 and September 2011 and the eSafety leader will revisit training each year. Families have received a 'Know It All' DVD and were shown a CEOP video in September/October 2009. In 2010 a series of child and family e-safety sessions were held. Pupils have received various training in classroom throughout the years of the school being open (drama productions / specific

lesson / PSCHE guidance/ Know It All lessons). Families can ask for advice from any member of staff in the school and are directed via the website to Mrs Brown for specific advice. Training for pupils and parents is ongoing each year.

APPENDIX A: PENSBY PRIMARY SCHOOL ICT RULES

The following rules apply to all pupils:

- I will only enter the school and use a computer when a school adult is present
- I will not put food or drink next to a computer.
- I will not take any paper from the printer unless I have been taught how to do so by my teacher.
- I will treat all equipment with care.
- I will ask permission before entering any web site, unless my teacher has already approved that site.
- I will not look at or delete other people's files
- I will not bring floppy disks or memory stick's into school without permission from my teacher
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- When sending an e-mail, I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit and the e-mail I send or receive.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

Staff must inform the Headteacher of any children who break these rules.

SANCTIONS:

1. Violations of the above rules will result in a temporary or permanent ban on internet use
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When appropriate, police or local authorities may have to be involved.

These rules will be kept under constant review. They will be displayed in the ICT room and in every classroom where there is a computer.

APPENDIX B: ACCEPTABLE USE OF INTERNET PERMISSION FORM

PUPIL'S ACCEPTANCE OF THE SCHOOL'S POLICY REGARDING ACCEPTABLE USE OF THE INTERNET

Please complete and return this form to your child's class teacher.

Name of Pupil: _____ **Class:** _____

Pupil's agreement:
I have read and understood the school rules for responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times. I understand that if I break these rules then I may not be allowed to use the Internet.

Pupil's signature _____ Date ___/___/___

Parent's/Guardian's acknowledgement:
I have read and understood the school rules for responsible Internet use 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. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I understand that the school is not liable for any damages arising from the use of Internet facilities.

Signed: _____ Date ___/___/___

(parent/guardian)

Parent's Consent for Web Publication of Work and Photographs:
I agree that, if selected, my son/daughter's work may be published on the school Web site. I also understand that photographs that include my son/daughter will be published only if they comply with the school rules that photographs will not clearly identify individuals and that full names will not be used.

Signed: _____ Date ___/___/___

(parent/guardian)

SCHOOL:
The school acknowledges the above signatures and therefore grants Internet access.

Signed _____

Mrs K Brown, Headteacher

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 for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional rôle.
- 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.
- 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.
- I will ensure that any electronic communications with students are compatible with my professional rôle.
- I will promote eSafety with students 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 e-mail 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: ……

Accepted for school: …… Capitals: ……

Pensby Primary School
ESafety Audit

Date - September / October 2010

Audit led by – Mrs K Brown/ Mr J Klausen

	YES/NO	ACTION
Does the school have an AUP with esafety staements?	YES	Update at least annually and seek GB approval
When was the policy agreed by governors?	Oct 2009	Update at least annually and seek GB approval
Where do staff see this policy?	YES	In policy pack at beginning of each academic year. First presneted and discussed in staf meeting in Sept 2009
Where do parents see this policy?	YES	Parents informed in Oct 2009. ICT rules sent home. Policy on VLE / parents eve
The designated Child Protection member of staff is	YES	Mrs K Brown / Mrs J Thomas
The esafety coordinator is	YES	Mrs K Brown
Has esafety been provided for staff? When? How?	YES	Briefing in Sept 2009. Further training October 2009
Are Governors aware of the need for esafety When? How?	YES	In GB meeting and in HT reports and committee briefings
Has esafety training been provided for families? When? How?	YES	CD 'know it all' sent to all families – Sept 2009. A parents DVd shown in Oct
Has esafety training been provided for pupils? When? How?	YES	Focus of school in PSCHE, focus of week etc. 2008/09 year 5 & 6 pupils given training through drama workshop
Are staff given/do they sign an ICT code of conduct?	YES	Annually
Do parents and children sign and return an agreement that their child will comply with esafety rules? How? When?	YES	Annually
Have esafety rules been set for pupils?	YES	Review rules in light of any incidents
Are these rules displayed in all rooms with computers?	YES	Ensure rules are always displayed and clear
Is internet access provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?	YES	Provided by LA services / Becta filter as standard with high filter protection
Is personal data collected, stored and used according to the principles of the Data Protection Act?	YES	Maintained by Mrs Yeardsley-Jones
Does the school have a system to block websites/ unblock websites and report esafty incidents?	YES	Yes – see appendices below

APPENDIX 1

Pensby Primary School

ESafety - Request to Block a Website

Person making request _____

Date of request _____

Website address _____

Reason for request _____

_____

_____

Please pass this request to the esafety leader/s Mrs K Brown or Mr J Klausen

---

For use by esafety leaders only

Request approved / denied

Details of action _____

SIGNED _____ **DATE** _____

APPENDIX 2

Pensby Primary School

ESafety - Request to Unblock a Website

Person making request _____

Date of request _____

Website address _____

Reason for request _____

_____

_____

Please pass this request to the esafety leader/s Mrs K Brown or Mr J Klausen

---

For use by esafety leaders only

Request approved / denied

Details of action _____

SIGNED _____ **DATE** _____

APPENDIX 3

Pensby Primary School
ESafety - Incident Report

Person reporting Incident _____

Date of Incident _____

Details of incident _____

_____

_____

_____

Please pass this request to the esafety leader/s Mrs K Brown or Mr J Klausen

---

For use by esafety leaders only

Details of action _____

SIGNED _____ **DATE** _____