Studley Community Infants' School

E-Safety Policy

November 2015

NAMED PERSONS RESPONSIBLE AT STUDLEY INFANTS SCHOOL		
POSITION	**NAME**	**SIGNATURE**
HEAD TEACHER	D Bateman	
COMPUTING & E-SAFETY LEADER	J Cockette	
CHAIR OF GOVERNORS	G Marshall	
E-SAFETY GOVERNOR	D Edwards	

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

The E-Safety Policy is part of the Learning Improvement Plan (LIP) and relates to other policies including those for Computing and for child protection.

Introduction

Studley Community Infants' School views the matter of E-Safety collaboratively with child protection and not independently as computing or ICT. All staff and pupils have a duty of care to be aware and vigilant of their own and others E-Safety at all times. This policy should be read alongside the child protection policy, acceptable use policy and social network policy.

Roles and responsibilities

Governors will view and agree to all policies before they are published.

The Head Teacher will have overall responsibility for all e-safety matters and will be informed of all incidents in line with the yellow reporting sheet used for recording and reporting e-safety incidents.

The E-Safety Co-ordinator will ensure the E-Safety policy is updated annually and current practice falls in line with the stated guidelines.

All staff have a responsibility to support E-Safety practices in schools. Pupils and staff at all levels need to understand their responsibilities and liabilities in the event of deliberate attempts to breach E-Safety protocols or those laid out in the Acceptable Use Policy.

Aims

1.1 General Aims of Studley Infant School

At Studley Community Infants' School we strive to create an atmosphere that is happy, caring and challenging. We want every child to feel they belong here and to feel safe and secure. We believe in the importance of developing the whole child through offering a broad, balanced and creative curriculum where both individuality and team-work are valued. We will help our children to begin to develop learning skills that will last a lifetime, so that they can make their best contribution to the community and society.

With regard to computing, we will ensure:

- pupils know how to communicate safety and respectfully online, keeping personal information private, and can recognise common uses of information technology beyond school;
- a continued development of self-assessment of e-safety using the 360° tool.

1.2 Aims of E-safety

The requirement to raise awareness in children and young people of the risks associated with inappropriate contact via the internet and content on the internet is addressed as part of the wider duty of care to which all teachers are bound. It is essential that all pupils are taught the relevant skills and strategies to remain safe when using the internet and related technologies. This may be as discrete internet safety lessons, as part of the Computing curriculum, delivered via whole school assemblies or embedded within all curriculum work wherever it is relevant. Recognising the issues and planning accordingly will help to ensure appropriate, effective and safe pupil use.

In-line with Every Child Matters 2 'Staying safe' we will raise awareness of children and adults to the risks associated with use of the Internet and other electronic communications and how they can protect themselves. This protective behaviour will be integrated into the curriculum.

§ The Internet is an essential element in 21st century life for education, business and social interaction. The school will provide students with quality Internet access as part of their learning experience.

§ Internet use will be a part of the statutory curriculum and will be used as a necessary tool for staff and pupils.

§ The e-safety policy will work alongside and will cross reference with the behaviour and safe guarding policy.

Teaching and Learning

2.1 Overview of E-Safety Curriculum

In line with National Computing Curriculum, pupils will be taught to –

- Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In line with the Studley Community Infants' School E-Safety curriculum, pupils will -

- Build on existing skills and knowledge
- Access age appropriate use of the internet
- Be taught appropriate and acceptable internet use through modelling and discussions
- Use the internet to enhance cross curricular experiences
- Learn how to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Embed Studley Infant School's 'SAFE Rules of Acceptable Internet Use'

To ensure the school remains at the forefront of E-Safety there is an active E-Safety Committee including a committed Governor representative which supported the school in gaining the 360º Safe Accreditation.

Managing Internet Access

3.1 System Security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Services.

3.2. Accessing the Internet

- The school strives to keep in line with emerging technologies with access to the internet is on all of school devices is managed and monitored closely by all members of staff. The LA also monitors the websites visited and the user's activity.

3.3 Reporting concerns

3.3.1 Reporting system for staff

- Reporting forms are available in all rooms around the school and will be completed by any member of staff if they have a concern about the safety of any child using the internet, at school or home.
- Reporting forms will be completed immediately and contain as much fact and detail as possible.
- On completion they will be passed to a member of the Child Protection team or the E-Safety Officer.
- The SLT will review all reports and decide on the best course of action.
- The governors will be made aware of all reports made.
- The E-Safety Policy and E-Safety Curriculum will be changed and adapted to suit the needs highlighted by reports made.

3.3.2 Reporting system for pupils

- .
- Posters showing Child Protection and E-Safety Officers are displayed in all classrooms.
- PHSE Protective Behaviours unit works with children in developing a communication hand, highlighting people each child would feel comfortable talking to if they felt their Early Warning Signs.

Talking tins also available for children who are unable to write down their thoughts.

3.4 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. These will be dealt with by the class teacher and Head Teacher and will include child protections officers if necessary.
- Pupils must not reveal personal details of themselves or others, other than authorised information, in e-mail communication, or arrange to meet anyone without specific permission. This is taught throughout the year via assemblies, room displays and ICT lessons.
- Use of words included in the Policy Central 'banned' list will be detected and logged and the behaviour policy will be followed.
- Whole-class addresses will be used.
- E-mail 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.
- Members are to use their professional conduct when using the schools e-mail account system.

3.5 Photographing and Videoing

- All photographs and videos will be taken on school devices. If such equipment is being taken off the premises e.g. on an external trip, all existing content will be removed before leaving the school site.
- All photographs and videos will not be stored on memory sticks or laptops which are leaving the school site, unless such devices are encrypted.
- Photographs and videos will only be taken of children whose parents have given signed permission. Such signed documents will remain on file for the duration of the child's time at Studley Infants' School.
- Photos and videos of children will include groups and not individuals (with the exception of individual learning journals) and will always show the intended learning context.

3.6 Published content

3.6.1 School web site and Virtual Learning Page

- The contact details on the Web site and Virtual Learning Page should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Head Teacher and ICT leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.6.2 Digital Signage

- No personal information will be published. If names are used it will only show first names and the year group or class number where needed for clarification e.g. in the instance of two children sharing the same name.
- The Head Teacher, administration team and ICT leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.6.3 Publishing pupil's images and work

- Images of children and their work will be published on our School web site, Virtual Learning Page and in school Digital Signage.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified and will show pupils in their intended learning context.
- Pupils' full names will not be used anywhere, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils or images of work are published.
- No details will accompany published photographs or videos e.g. children's names, age, class number.
  Exceptions can be made in the case of competition winners, with parental permission. In such cases only first names will be used.

3.7 Social Networking and personal publishing

- Social networking sites and newsgroups will be blocked in school unless a specific use is approved.
- Throughout the academic year pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- Pupils are taught of the possible risks involved with online gaming e.g. communicating with unknown people, sending or receiving files.
- Parents are asked to not publish any photos or videos taken when on the school site on any social networking sites. In the case of these guidelines not being followed appropriate action from the Head Teacher will be implemented.
- Members of staff wishing to be involved in Social Networking sites outside of school will do so using their professional conduct.
- Any child under the age of 13 known to have a Social Network account will be reported through the appropriate channels.

Please see Social Networking Policy

3.8 Management

3.8.1 Filtering

- The school will work in partnership with the Warwickshire ICT Development Service and Becta to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the class teacher, school E-Safety coordinator and Head teacher.
- The Head teacher and E-Safety coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.8.2 Managing videoconferencing

§ IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

§ Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.

§ External IP addresses should not be made available to other sites.

§ Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

§ Videoconferencing should be supervised appropriately for the pupils' age.

3.8.3 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.

§ Staff and pupil mobile phones will not be used during lessons or formal school time and will not be used to photograph or video children.

3.9 Mobile devices

The school embraces the use of mobile technologies in school by both staff and pupils.

3.9.1 School owned mobile devices at home

§ School owned mobile devices are available to take home to support work done outside of school hours. They will be used for school tasks only.

§ Internet use on these devices will be monitored when in school, sites visited at home will be flagged when on the school site and will be reported if inappropriate.

§ Personal pupil information will be stored on encrypted devices if it is to be taken off the school site.

§ Photographs and videos will regularly be removed from mobile devices and stored on the school secure shared system.

§ School devices will not be used for personal use in school or at home
See Social Networking Policy.

3.9.2 Personal mobile devices in school

§ All personal devices will remain in a secure lockable cabinet during school hours.

§ Staff may use their mobile phones to make calls in areas of the school where no children are present and outside of teaching time unless it is an emergency situation that the Head Teacher has agreed. They can use them in staff designated area. No video or photograph during school hours.

3.10 Cyber Bullying

Cyber bullying is not and will not be accepted by any member of the Studley Community.

- All pupils are taught the expectations and sanctions of cyber bullying via the 'SAFE' rules of acceptable use
- All staff and pupils are aware of the reporting process they should follow if they become aware of cyber bullying (see section 3.3 Reporting Concerns)
- Any pupil found to be involved in sending any form of cyber bullying, to other pupils externally, will have internet privileges removed.

3.11 Data Protection & Filtering

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- All internet content will be continuously monitored and filtered by the LA with any issues flagged to the Head Teacher.
- All members of staff will continuously monitor and filter the use of internet during lessons in the ICT suite and when mobile devices are used in the classroom, following the suitable reporting of inappropriate websites process if needed.

3.12 Passwords

- All Governors, Teachers, TA's, Support staff and Pupils are provided with a secure password, gaining them access to the school system and the Learning Platform.
- Adults in school are responsible for the security of their own passwords and area. They will keep them private and ensure devices are re-locked when not in use to ensure positive security of personal details.
- Teachers are able to change the passwords of the pupils in their class, either at their discretion or at the request of parents.
- Pupils log in details may be printed in order to support their use during lessons, but will be stored securely when not in use.

Policy Decisions

4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the acceptable ICT use agreement, 'E-Safety Agreement Form for School Staff', before using any school ICT resource.
- All pupils must read and sign an E-safety Agreement Form before accessing the internet. This will be re-signed at the beginning of each academic year alongside the reintroduction of the 'SAFE' rules of acceptable use.
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a e-safety and internet use consent form.

4.2 Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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. Neither the school nor WCC can accept liability for the material accessed, or any consequences of Internet access.
- The Head Teacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

4.3 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.
- E-safety complaints are reviewed and the e-safety policy and curriculum planning is adapted accordingly.

Communications Policy

5.1 Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Pupils are encouraged to play an active role in the development of the e-safety policy and 360° tool

5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained alongside associated documents e.g. the bullying policy.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff will sign the Warwickshire Acceptable Use Policy, including regular before, during and after school club teachers.
- All staff will ensure their personal telephones or other devices capable of taking photographs or videos will not remain in the classroom during teaching hours but will be stored in secure areas of the classroom.
- All staff will be given an induction pack that includes;
- - The E-safety policy
- - The Warwickshire acceptable use policy
- - The Password Safety policy
- - Notification of the safeguarding officers
- - Procedures to follow for reporting

5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy on the school website, in newsletters and the school brochure.
- Parents will have opportunities to attend e-safety sessions on school led by either an internally trained safeguarding officer or a member of the Local Authority.
- Parents are regularly asked for their opinion regarding the E-Safety provision and are given the opportunity to offer suggestions which could develop it further.

5.4 Visitors and the E-Safety Policy

- All visitors will be provided with an E-Safety leaflet outlining the basic guidelines of this policy.

SMSC (Spiritual, Moral, Social & Cultural)

E-Safety plays a key role in the spiritual, moral, social and cultural development of children. Section 8, cross curricular links, of the SMSC Policy should be consulted.

SEN

The school strives to enable all pupils to reach their full potential. Staff will plan for those needing extra support where needed. Planning is linked to the appropriate IEP and cross referenced to weekly plans. The pupils are supported by teachers, ancillary helpers and outside agencies.

E-safety is differentiated and supported by teachers or TA's e.g. widgets accompanying e-safety reminders.

Equal Opportunities

The Policy reflects the school policy on equal opportunities and inclusion, where all children, irrespective of religion, age, gender, ethnicity, language or disability have an equal entitlement to receive a quality of education, covering the full extent of the curriculum.

Health and Safety

In-line with ECM 1 and 2, school systems will comply with this policy, Health and Safety Policy and associated risk assessments.

2 Bibliography

Warwickshire Schools E-Safety Core Policy 2007

Appendix 1

Logging a concern about a child's safety and welfare regarding the internet.

PART 1:

Pupils name:	**Date of birth:**
Date:	**Time (of writing this report):**
Name: **Print** **Signature** **Job title :**	
Note the reason(s) for recording the incident:	
Record the following: Who? What? Where? When? Any evidence?	
Professional opinion where relevant (how and why this may have happened):	
Note actions, including the names of anyone to whom you information was passed:	
Any other factual relevant information:	

Check to make sure this report is clear – will it be clear to someone else who is reading it?

PLEASE PASS THIS FORM TO A DESIGNATED E-SAFETY OFFICER TO COMPLETE OVERLEAF

PART 2:

Time and date information was received and by whom.		
Any evidence to accompany the concern?		
Actions taken (referral to children's services, parent/carer notification, advice provided) Justify reason. Note times, dates and names		
Outcome of action taken (names, information provided or received, outcome)		
Any other information about child in question relevant? (IEP, child protection register ,FSM etc)		
Parent/carer informed?	Yes	No
Reason?		
Parent/carer signature :		
Designated E-Safety officer : Name: Print Signature Date:		

Appendix 2

EYFS/KS1 Pupil Acceptable Use Agreement

Think before you click

S	I will only use the computers or internet when an adult says I can
A	I will only click on icons and links when I know they are safe
F	I will only send friendly and polite messages
E	If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

Appendix 3

E-safety and Internet use Agreement Form For Parents of Studley Community Infants' School

Parent / guardian name: ________________________________

Pupil name: ____

As the parent or legal guardian of the above pupil, I grant permission for my daughter / son to have access to use the Internet and other ICT facilities at school.

I know that my daughter / son has signed an e-safety agreement form and that they have seen and understood the "'SAFE' rules for acceptable internet use".

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 pupils from accessing inappropriate materials. These steps include using an educationally filtered and monitored service, employing appropriate teaching practice 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 or
e-behavior that 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 / guardian signature: _____________________________

Date: ___/___/___

STUDLEY COMMUNITY INFANTS' SCHOOL

Appendix 4

E-safety Agreement Form

For School Staff

To ensure that staff are fully aware of their responsibilities with respect to ICT use, they are asked to sign this acceptable use agreement.

- I understand that the network is the property of the school and agree that my use of this network must be compatible with my professional role.
- I understand that the school ICT systems may not be used for private purposes, without specific permission from the Head Teacher.
- I understand that use for personal financial gain, gambling, political purposes or advertising is not permitted.
- I understand and agree that the school may monitor my network and Internet use to ensure policy compliance.
- I will respect ICT system security and understand that it is a criminal offence to use a computer for a purpose not permitted its owner.
- I will not install any software or hardware without permission.
- I will not disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system.
- I will take all reasonable precautions to secure data or equipment taken off the school premises.
- I will report any incidents of concern to the school's Designated Safeguarding Lead or E-Safety Leader as appropriate.
- I will ensure that my electronic communications with pupils are compatible with my professional role and cannot be misinterpreted.
- I will promote e-safety with the students that I work with and will help them to develop a responsible attitude to ICT use.
- I will respect copyright and intellectual property rights.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed: ……………………………………….…. Capitals: ………………………

Accepted for School: ……………………………. Capitals: ……………………….

Date: …………………………………..

STUDLEY COMMUNITY INFANTS' SCHOOL

Appendix 5

Warwickshire County Council

For Photography Images and Videos of Children

Dear Parent or Carer

During your child's time at Studley Community Infants' School we may wish to take photographs and videos of activities that involve your child. The photographs may be used for displays, publications, the Learning Platform and a web-site by us, by the Local Education Authority or by local newspapers. We may also take part in online web conversations via a webcam with external organisations.

Photography or filming will only take place with the permission of the head teacher / manager, and under appropriate supervision. When filming or photography is carried out by the news media, children will only be named if there is a particular reason to do so (e.g. they have won a prize), and home addresses will never be give out. Images that might cause embarrassment or distress will not be used nor will images be associated with material on issues that are sensitive.

Before taking any photographs of your child, we need your permission. Please **answer the questions below, sign and date the form and return it to the establishment**. You can ask to see images of your child held by the establishment. You may withdraw your consent at any time.

Name of child (Block Capitals) :		
Name of person responsible for the child:		
I understand that: • the local media may take images of activities that show the establishment and children in a positive light e.g. Reception Year pictures of new starters, drama and musical performances, sports and prize giving; • photographers acting on behalf of the school or WCC may take images for use in displays, in publications, on the Learning Platform or on a website; • embarrassing or distressing images will not be used; • the images will not be associated with distressing or sensitive issues; and • the establishment will regularly review and delete unwanted material. • images and videos of your child may be shared on our secure Learning Platform.		
Having read the above statement, do you give your consent for photographs and other images to be taken and used? (please tick the appropriate box)		**YES**, I give my consent for pictures and videos to be taken and used
		NO, I do not give my permission for pictures and videos to be taken and used
Signature of person responsible for the child:		
Relationship to the child:		
Date (Date/Month/Year):		

NB There may be other circumstances, falling outside the normal day to day activities of the school, in which pictures of children are requested. The establishment recognises that in such circumstances specific consent from parent or guardian will be required before photography or filming of children can be permitted.

If you wish to attend establishment functions and take photographs of your and other people's children please take appropriate images, be sensitive to other people and try not to interrupt or disrupt concerts, performances and events. Thank you.

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