

Laughton Community Primary School

E-Safety Policy



Created: November 2015
Review date: November 2016

Core Principles of E-Safety

The internet is becoming as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help to ensure responsible use and the safety of pupils.

A recommended e-safety policy is built on the following three core principles:

Educating young people to be responsible users of ICT

21st Century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must also learn how to recognise and avoid these risks for themselves as they grow older – to become “internet wise”. The precise nature of the risks faced by young people will change over time as new technologies, fads and fashions take hold, but there are general principles of safe online behaviour that apply to all sorts of situations, eg. pupils need to know how to react if they come across inappropriate material and that they should not give out personal information such as their address and telephone number to strangers or publish this on the internet. They should evaluate critically the quality of the material they find on the internet. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Guided educational use

Significant educational benefits should result from curriculum IT use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum IT use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful IT use will also reduce the opportunities for activities of dubious worth.

Regulation and control

Internet safety depends on staff, schools, governors, advisers, parents and the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones.

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions.

This document describes strategies to help to ensure responsible and safe use. They are based on developing responsibility, guiding pupils towards educational activities and limiting access. Strategies must be selected to suit the school situation and their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Laughton Community Primary School E-Safety Policy

1 Who will write and review the policy?

- Our e-safety policy has been written by a Primary Teaching school in East Sussex, building on the SEGFL (South Eastern Grid for Learning) policy and government guidance. It has been adapted to suit the needs of Laughton Community Primary School and been agreed by the senior management and approved by governors. It will be reviewed annually.

2 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 business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

3 How does the internet benefit education?

Benefits of using the internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives in Schools
- 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 materials 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 LA and DFE.
- Mentoring of pupils and providing peer support for pupils and teachers

4 How will internet use enhance learning?

- The school internet access will be designed expressly for pupil use and will include 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. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

- Staff should guide pupils in on-line activities that will support the 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, evaluation and retrieval.

5 How will pupils learn to evaluate internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT co-ordinator (Rachel West).
- Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. All pupils will need close supervision when researching topics over the internet.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

6 How will e-mail be managed ensuring safety for pupils?

- 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 details of themselves or others in e-mail communication or via a personal web space, such as address or telephone number, or arrange to meet anyone.
- Personal email or messaging between staff and pupils should not take place.
- Whole-class or group e-mail addresses should be used at Key Stage 1 and below, rather than individual messaging.
- 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.

7 How should website/learning platform content be managed?

- The point of contact on the website/learning platform should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website/learning platform photographs that include pupils will be selected carefully.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/learning platform.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website/learning platform should comply with the school's guidelines for publications.

8 Newsgroups, e-mail lists and forums

- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.
- Access to forums that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted.

9 Chat and instant messaging

- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will not access social networking sites for example 'My Space' or 'Bebo'.
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
- Any form of bullying or harassment is strictly forbidden.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.
- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.

10 Personal websites and blogs

- When publishing material to websites and elsewhere, pupils should consider the thoughts and feelings of those who might view the material. Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable.

11 Photographic, video and audio technology

- It is not appropriate to use photographic or video devices in changing rooms or toilets.
- Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.
- Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities.
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.
- Pupils should always seek the permission of their teacher before making audio or video recordings within school.

12 How can emerging ICT applications be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time, except by staff when they are on a break.
- Mobile phone cameras should not be used inappropriately by staff and photographs should not be forwarded to unknown sources.
- The use of blog messaging on social network sites is strictly forbidden.

13 How will internet access be authorised?

- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At EYFS and Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form. Please see the sample form later in this document.
- Primary pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.

14 How will the risks be assessed?

- 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, or the Local Authority, 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 under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored.
- Access is strictly forbidden to any websites that involve gambling or financial scams.

15 How will filtering be managed?

- The school will work in partnership with parents, the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.org.uk).
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.
- YouTube cannot be accessed until after 4p.m when staff can download appropriate support materials for lessons.

16 How will the policy be introduced to pupils?

- Rules for internet access will be posted in all rooms where computers are used and drawn to the children's attention.
- Pupils will be informed that internet use will be monitored.

- Instruction in responsible and safe use should precede internet access.
- E- safety lessons will be included in the PSHCE (physical, social, health, citizenship, emotional) programme covering both school and home use.

17 How will staff be consulted and made aware of this policy?

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school.
- All new staff will be taken through this policy as part of their induction.
- All new staff will be provided with a copy of this policy.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School e-Safety Policy and have 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.
- The monitoring of internet use is a sensitive matter. The staff that operate monitoring procedures, will be supervised by senior management.
- Staff development in safe and responsible internet use, and on the school internet policy, will be provided as required.
- Breaching this e-safety policy may result in disciplinary action being taken and access to IT being restricted or removed.

18 How will IT system security be maintained?

- The school IT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- Personal data sent over the internet will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

19 How will complaints regarding internet use be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff. Please see appendices.
- Any complaint about staff misuse must be referred to the headteacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions available include:
 - interview/counselling by class teacher/ headteacher;
 - informing parents or carers;
 - removal of internet or computer access for a period
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies. Advice sought should include how best to preserve any possible evidence.

20 How will parents' support be enlisted?

- Parents' attention will be drawn to the E –safety Policy in newsletters, the school brochure and on the school website.

- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home, such as, a strong recommendation to ensure children of primary age do not access facebook and similar social networking sites
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
- Interested parents will be referred to organisations such as PIN (Parents Information Network), Parents Online and NCH Action for Children (see websites in appendices)

21 How is internet used across the community?

- Adult users will need to sign, and comply with, the e-safety policy or alternatively an acceptable use policy.
- Parents/carers of children will be required to sign an acceptable use policy on behalf of the child.

Appendices

- Rules for responsible IT use
- Letter to parents regarding responsible IT use
- Incident report sheet
- Consent form for image use

Parents'/Legal Guardians' Consent to Take and Use Images of Pupils

Key Policy Points:

- Laughton Community Primary School recognises that a balance between the low risk of misuse and the numerous positive results of colourful, well produced school material is necessary.
- The school will only take and use images (photographs, videos and DVDs) that are appropriate and are considered to be safe from misuse.
- Children will be made aware of why their pictures are being taken and how they will be used.
- The school will take extra precautions to ensure that only appropriate images are used for the website.
- If it is found that a camera phone has been misused the school will follow its usual disciplinary procedures.
- If an image of a child is used, the child's name **will not** be published. If a name is published, **no image will be used** without specific consent.
- Parents and legal guardians will be asked to sign an agreement that any images they take during school activities will not be used inappropriately.

.....✂

PARENTS

Please read our Policy for the Use of Images of Children and indicate whether you agree to your child's images being taken. You have the option to indicate whether or not you consent to your child's images being taken and used for different purposes. **You can withdraw your consent at any time by writing to the school.**

Name of child (block capitals)	
Child's date of birth	
Name of parent or legal guardian (block capitals)	
I have read the school's policy on the use of images of children and I agree to its provisions. <i>Please give your consent by putting your initials next to each statement. Your child's images will not be taken/used as specified, if you do not give your consent.</i>	
I give my consent to images of my child being taken and used for official school purposes of promoting or publicising school events in accordance with the guidelines of the policy for the duration of their time at the school.	<i>Please initial here</i>
I give my consent to images of my child being used on the school website and I understand that these images will be available on the World Wide Web.	
I give my consent for images taken by the school in accordance with the guidelines of the policy to be used for official East Sussex County Council publication	
Signature of parent or legal guardian of 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, when images of children are needed. The school recognises that in such circumstances specific consent from the parent or legal guardian will be sought before any photography or filming of children starts. If you have concerns or queries about any of this information, please contact the school. Please return to the school office

Incident report sheet

Date of incident	
------------------	--

Name of member of staff discovering the incident				
Names of adults/ children involved				
Nature of incident	Access to inappropriate material	Cyberbullying	Grooming	Other inappropriate use
Details				
The event occurred...	...during a lesson	...in unsupervised time	...outside of teaching hours	...offsite
Location				
Does the event warrant police involvement? YES if...	<div style="border: 1px solid black; padding: 2px; margin-bottom: 2px;">...grooming.</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px;">...deliberately accessing/ uploading violent or pornographic images</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px;">... inappropriate sharing of images of children or their personal details</div> <div style="border: 1px solid black; padding: 2px;">... other illegal activity</div>			

Informed...	✓ & date/ time
Parents	
SMT	
ICT coordinator	
ICT Technician	

Action taken	date/ time/ name of contact
ICT helpdesk informed/ website blocked	
Advice sought from Personnel Contact	
Police contacted	
Disciplinary sanction applied	

Notes