E-SAFETY POLICY

LEIGHTERTON PRIMARY SCHOOL

Review date: Annual

Date	Signed (Chair of Governors)	Signed (Headteacher)

Leighterton Primary School
E-safety Policy

Why is Internet Access Important?

The development and expansion of Computing, and particularly of the internet, has transformed learning in recent years. Children and young people need to develop a high level of computing skills, not only to maximise their potential learning tool, but also to prepare themselves as lifelong learners and for future employment. The internet and other digital and information technologies are powerful tools, which open up new technologies to everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion and promote creativity and increase awareness of context to promote effective learning. The school has a duty to provide pupils with quality safe internet access as part of their learning experience.

Current and emerging technologies are used in school and outside school by children and include:

- The internet
- Email
- Instant messaging often using web cams
- Blogs
- Podcasting
- Social networking sites
- Video broadcasting sites
- Chat rooms

Development, Monitoring and Review of this Policy

This e-safety policy has been developed by the Computing subject leader, the Headteacher and governors.

This e-safety policy was approved by a Governors Sub Committee on:	
The implementation of this e-safety policy will be monitored by the:	Headteacher Computing Subject Leader
Monitoring will take place at regular intervals:	At least once a year.
Due to the ever changing nature of Information and Communication Technologies, the school will review this E- Safety policy annually and, if necessary, more frequently, in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	
Should serious e-safety incidents take place, the following external person will be informed:	Gloucestershire Designated Safeguarding Officer.

The school will monitor the impact of the policy using:

- A log of reported incidents

- Monitoring logs of internet activity (sites visited and filtered sites)

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/guardians) who have access to and are users of Leighterton Computing systems.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of our school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/guardians of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The Safeguarding Governor will:

- Regularly monitor e-safety incident logs
- Regularly monitor filtering logs

Headteacher

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility will be delegated to the E-Safety Coordinators (Class Teachers).

The Headteacher will ensure that the E-Safety Coordinators receive suitable CPD to enable them to carry out their role and train other colleagues as necessary.

The Headteacher will receive regular monitoring reports from the E-Safety Coordinators as appropriate.

The Headteacher is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E Safety Coordinators

The Computing Subject Leader is Meryl Hatfield. She must:

- Take day to day responsibility for E-safety issues and have a leading role in establishing and reviewing the school e-safety policy and related documents.
- Ensure all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice to staff.
- Liaise with Gloucestershire Computing team.
- Liaise with school technical staff.
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.
- Discuss current issues, review incident logs and filtering log with Safeguarding Link Governor as necessary.
- Report to Headteacher as necessary.

Technical Staff

- Our Computing technicians and Network Manager are responsible for ensuring: That the school's Computing infrastructure is secure and is not open to misuse or attack.
- That Leighterton meets the e-safety technical requirements outlined in the SWGFL Security Policy and Acceptable Usage Policy.
- That users may only access the school's network through a properly enforced password and passwords are regularly changed.

Teaching Staff and Support Staff

Teaching staff and support staff are responsible for ensuring that:

- They understand the e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the E-Safety Coordinators, Computing Subject Leader and Headteacher.
- Digital communication with pupils should be carried out on a professional level and only carried out using official school systems.
- Pupils understand and follow school e-safety policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and copyright restrictions.
- They teach to pupils the importance of reporting abuse, misuse or access to inappropriate materials. Teaching time is dedicated to this within the two yearly Computing topic cycle across the whole school. A yearly 'Safer Internet Day' is held each year to promote safer and more responsible use of online technology and mobile phones.
- In lessons where the use of internet is pre-planned, pupils are guided to sites that are checked as suitable for their use and should any unsuitable material is found in internet searches information is given to one of the E-Safety coordinators immediately.

Pupils

Pupils should:

- Be responsible for using the school Computing systems in accordance with Pupil Acceptable Use Policy, which their parents/guardians have signed.
- Have a good understanding of research skills and the need to avoid plagiarism and copyright restrictions; they gain this knowledge through direct teaching in KS2.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials. Teaching time is dedicated to this within the two yearly Computing topic cycle across the whole school and through the celebration of the annual Safer Internet Day.
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy also applies to their actions out of school.

Parents

Parents and guardians play a crucial role in ensuring that their children understand the need to use the internet and digital technology in an appropriate way. E-safety advice for parents and guardians is that photographs taken at school events should not be used on social media. Parents and guardians will be responsible for endorsing (by signature) the Pupil Acceptable Use Policy.

Parent/guardians should:

- Ensure that children access the Internet in a communal room where they can be easily supervised.
- Ensure appropriate supervision for the age of their children including supervising all use of the Internet by younger users.
- Ask their children about what sites they are looking at.
- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated.
- Ensure content is appropriately filtered for younger users.

Image Taking by Parents/Legal Guardians or Family Members

- Parents, legal guardians, family members and friends can take images of their child and friends participating in school activities for family and personal use only and agree that any images taken will not be shared on social media.
- Parents will be asked for their permission before photography is allowed.

Education

Pupils

E-safety education will be provided in the following ways:

- In KS2 a planned e-safety programme is taught as part of our two yearly topic cycle. These lessons cover both the use of Computing and new technologies in school and outside of school.
- Key e-safety messages are taught to all pupils through Computing teaching and assemblies (e.g. assemblies during Safer Internet Day and follow up work that week).
- KS2 pupils are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

Education and Training – Staff

- E –safety training will be available for staff.
- All new staff should receive e-safety guidance as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies for pupils and staff.
- The Computing / E-Safety Coordinators will receive regular updates through attendance at e-safety conferences and training sessions and by reviewing documents released by BECTA, SWGfL, Gloucestershire Council and others.

Training – Governors

Governors will have opportunities to attend appropriate e-safety training as necessary.

Technical – Infrastructure/Equipment, Filtering and Monitoring

The school will be responsible for ensuring:

- That the school infrastructure/network is safe and secure as is reasonably possible and that policies and procedure approved within this policy are implemented. It will also need to ensure that the relevant staff roles named in the above sections will be effective in carrying out their e-safety responsibilities.
- School Computing systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in SWGfL Security Policy and Acceptable Use Policy and any relevant Local Authority E-Safety Policy and guidance.

- There will be regular reviews of the safety and security of school Computing systems.
- Servers are securely located and physical access restricted.
- All users will have clearly defined access rights to school Computing systems.
- The administrator passwords used by the Network Manager are known by the school/ LA Computing technical team and can be shared at any time with the Headteacher.
- The school maintains and supports the managed filtering service provided by SWGfL.
- Any filtering issues should be reported immediately to SWGfL.
- Requests from sites to be removed from the filtered list will be considered by technical staff in conjunction with the Headteacher, Computing / E-Safety coordinators and advice from the LA. If the request is granted this needs to be logged and dated with signatures of the Headteacher and a Computing / E-Safety coordinator.

Curriculum

- In lessons where the internet is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff must be vigilant in monitoring the content of websites that pupils visit.
- Pupils should be taught to be critically aware of the content they can access on-line and understand that not all information is accurate.
- Pupils should be taught to acknowledge the source of the information used and respect copyright when using material accessed on the internet.

Use of Digital and Video Images – Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents/guardians will be obtained before photographs of pupils are published on the school website.

Mobile Phones

- The school policy is that pupils are not allowed mobile phones in school. The school phone can be used to contact parents/carers with important messages. Staff are not permitted to use their personal mobile phones to take images of the children.

Social Networking and Personal Publishing

- The school will block/filter access to open social networking sites and give access only to those sites that are monitored and approved by South West Grid recommendations.
- Tools including message boards, blogs, instant messaging and collaboration tools will be used in this safer, closed environment.
- Although pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils, pupils will be taught about the potential risks of social networking sites and what information should not be shared on such sites. The purpose of this is to acknowledge,

(although not condone), the reality that some children may already have access to social networking sites by this age.

Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they use personal data.
- Transfer data using secure password protected devices.

Communications

- The official school email service may be regarded as safe and secure and is monitored. School also uses Egress to send secure communications.
- The school uses a text messaging service for parents, enabling instant correspondence. This service will not be used for any personal use.
- Users need to be aware that email communications may be monitored
- Users must immediately report to an E-Safety coordinator, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying and must not respond to any such email.
- Any digital communication between staff and pupils, or staff and parents/guardians must be professional in tone and content.
- Pupils in KS2 are taught about email safety issues, such as the risks attached to the use of personal details. They should be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

This E-Safety policy has been written with reference and guidance from the South West Grid for Learning 2020 publication 'South West Grid for Learning Trust SCHOOL E-SAFETY POLICY'

This Internet Policy has been agreed by staff and approved by Governors. Due to the ever changing nature of Information and Communication Technologies, the school will review this policy annually and, if necessary, more frequently, in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Pupil Acceptable Use Policy

I have read the E-Safety Policy for Leighterton Primary School and understand its implications.
I have received the Guide for Parents document and have read and understood its guidance and advice and have shared the information and guidance with my child, (see appendix 1 and 2).

I agree to my child _____ having access to the Internet and to Computing systems at school within the framework detailed in the school E-Safety Policy.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that pupils will be safe when they use the internet and Computing systems. I also understand that the school cannot ultimately be held responsible for their nature and content of materials accessed on the internet and using mobile technologies.

Signed _____

Date _____

Use of Digital/ Video Images

I agree to the school taking and using digital/video images of my child. I understand that the images can only be used to support learning activities or publicity that reasonably celebrates success and promotes the work of the school.

Signed _____

Date _____

Leighterton Primary School

Appendix 1 – Pupil Acceptable Use and E-Safety Policy Agreement

Rationale

The purpose of this policy is to ensure that young learners know how to use the Internet and other technologies responsibly and know what to do if they discover harmful content on the Internet.

Finding Information on the Internet

I know:

- That I will get to use the Internet if I use it responsibly, and that being responsible means trying not to visit unsafe sites or registering for things I am not old enough for.
- What to do if I open something I do not like.
- How to search the Internet safely.
- That any information I put on the web can be read by anyone.
- That I should not copy others work and use it as my own.

Using Technology to Contact People

I know:

- How to protect my identity and keep my personal information private.
- How to use the safety features of websites.
- That I should be careful who I add as friends online.
- That I need to be polite and friendly online.
- Not to open e-mails if the subject is offensive or if I do not know who it is from.
- What to do if I receive an offensive e-mail/message
- That people online may not be who they say they are.

Signed _____

Leighterton Primary School

Appendix 2 – Guide for Parents

Monitoring Home Use of the Internet

Parents / carers should:

- Ensure that young people access the internet in a communal room
- Ask their children about what sites they are looking at
- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated
- Ensure content is appropriately filtered for younger users

Content – finding and publishing information on the internet

Parents / carers should:

- Ensure that their children know that they will only get to use the internet if they use it responsibly and that being responsible means they should not try to visit unsafe sites or register for things they are not old enough for.
- Ensure that their children know that any protection system does not stop all unsafe content and that children need to tell them if they access something inappropriate.
- Encourage children to search safely to find the information they want and search safely themselves using very specific search terms to reduce the likelihood of accessing unsafe material.
- Supervise younger children when they are using the internet
- Talk to children about the fact that any information published on the web can be read be anyone
- Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves in danger

Contact - Using technology to contact people

Parents / carers should:

- Discuss user names with children and talk about how to choose them carefully to avoid putting themselves at risk and protect their identity
- Identify the information that young people should keep private in order to prevent them being contacted or traced including
- Talk to children about the need to use safety features of web sites
- Talk to their children about limiting access to their personal information
- That e-mails / messages can be intercepted and forwarded on to anyone
- should talk to their children about being careful who they add as friends
- Talk about the need to be polite online and friendly online and think about the language they use (it could be forwarded to my parents or head teacher!)
- Discuss how to use the subject field in e-mails
- Not to open messages if the subject field contains anything offensive or if I do not recognise who it is from (delete it without opening it)
- Discuss what to do if I receive an offensive message / e-mail including how to keep evidence
- Explain that people online may not be who they seem

Staff (and Volunteer) Acceptable Use Policy

I have read the E-Safety Policy for Leighterton Primary School and understand its implications.

For my professional and personal safety:

- I understand that the school will monitor my use of Computing systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to the use of school Computing systems out of school.
- I understand that the school Computing systems are for educational use and I will only use the systems for personal or recreational use within the policies and rules set out by school.
- I will not use other usernames and passwords without their express permission.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the Headteacher.
- I will be professional in my communications and actions when using school Computing systems.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take or publish images of others I do so with their permission (using the most current Pupil Acceptable Use Policy forms signed by parents/ guardians).
- I will only communicate with pupils and parents/guardians using only official school systems.
- I understand that I am responsible for my actions in and out of school. I understand that the Acceptable Use Policy applies not only to my work and use of Computing equipment in school, but also applies to my use of Computing systems and equipment out of school and my use of personal equipment in school.
- I understand that if I fail to comply with the Acceptable Use Policy Agreement I could be subject to disciplinary action.

I have read and understand the above and agree to use the school Computing systems (both in and out of school) and my own devices (in school when carrying out communications related to school) within these guidelines.

Staff/ Volunteer Name: _____

Signed _____ Date_____