E- Safety Policy

To be read in conjunction with:

- *Computing policy*
- *Child protection policy*
- *Guide to safer working practice*
- *Photography policy*
- *Use of mobile phones policy*
- *Cyberbullying policy*

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Lambton Primary School we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Lambton Primary School.

Our e-Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The school's e-Safety Lead is Mrs. Claire Spencer.
- The e-Safety Governor is Mrs. Linda Williams.
- The e-Safety Policy and its implementation shall be reviewed annually.

Roles and Responsibilities
Governors:
Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the e-Safety Governor will include:

- Regular meetings with the e-Safety Lead.
- Regular monitoring of e-Safety incident logs. Appendix 1
- Reporting to the Governors. (Termly HT report)

Head teacher and Senior Leaders:

- The Head teacher are responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety lead.

- The Head teacher/Senior Leaders are responsible for ensuring that the e-safety lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head teacher and Deputy Head teacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Lead:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not. (Responsible use of the internet)appendix 2
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new computing (ICT) curriculum, all year groups have digital literacy units and PHSE that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Inclusion

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through

meetings our SEN coordinator and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read and sign the 'Acceptable ICT Use Agreement' (appendix 3) before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Head teacher, by recording the incident in an e-Safety Log, which will be stored in the Head teacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the e-Safety lead
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

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

E-mail

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- 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.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a using outlook.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Social Networking

- Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites.(All staff are given guidelines in the Guide to Safer Working Practice document, which they sign annually) The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting

All breaches of the e-Safety Policy need to be recorded in the E-Safety reporting file that is kept in the head teacher's office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the Designated Person immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require lead teacher intervention (e.g. cyberbullying) should be reported to lead teacher in the same day.

Allegations involving staff should be reported to the Head teacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline)

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Head teacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phone to contact parents.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the staffroom/one of the school offices.
- Parents cannot use mobile phones on school trips to take pictures of the children

On trips staff mobiles are used for emergency only

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents and carers are not permitted to take photos/videos of their own children in school events. Parents and carers are able to purchase a copy of the class learning journey after the assembly/ performance. This can only be released if the school receive 100% permission from all parents in that class.
- The Head teacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be not be taken during performances but may be taken during refreshment time after the performance on the basis that they are for private retention and not for publication in any manner and do not include other children.
- The Photograph policy should be referred to for more information.

Staff should always use a school camera/ equipment to capture images and should not use their personal devices.
Photos taken by the school are subject to the Data Protection act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.

- The Head teacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. This is taken from permissions sent at the start of the year.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Website.
- Work will only be published with the permission of the pupil.
- Only parents should only upload pictures of their own child/children onto social networking sites.
- The Governors/ headteacher may ban the use of photographic equipment by any parent who does not follow the school policy.

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.
- E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

Assessing Risk

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. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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 one of the Head teacher.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy
Pupils:

- Rules for Internet access will be posted in all networked rooms. (responsible use of the internet appendix 2)

- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites such as msn, Instagram. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.
- Pupils will attend an annual e-Safety assembly held each year by the e-Safety lead.
- Leaflets are around school to help pupils and Safety Street is a source of displays which inform pupils of how to keep safe.

Staff:

- All staff will be given the School e-safety Policy and its importance explained.

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.
- Esafety assembly will be held annually by the e-Safety lead for parents.

Further Resources
We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".

Appendices to this policy;

Appendix 1; Incident logs- kept in school
Appendix 2; Responsible use of the internet -(pupil)
Appendix 3; Acceptable ICT Use Agreement (staff)
Appendix 4;Agreement for learners in KS1
Appendix 5 – Agreement KS2
Appendix 6- Parent letter; email and internet use

Ratified by Governors: 13.6.19

Next review: Summer 2020

Appendix 4 – Agreement

Agreement for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

I am aware of the CEOP report button and know when to use it.

Signed .....

Date _____

TAMBTON
PRIMARY SCHOOL
Believe to Achieve

Appendix 5 – Agreement KS2

Agreement for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

I am aware of the CEOP report button and know when to use it.
I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Signed……

Date _____

Appendix 6 – Parent letter
Internet/e-mail use

Parent /Carer name:……..
Pupil name: ……
Pupil's class: ……

As the parent/carer or legal guardian of the above pupil(s);

- ✓ I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school.

- ✓ I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP) attached. I also understand that my son/daughter may be informed, if the rules have to be changed during the year. E-safety policy available on the school website.

- ✓ 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 a filtered internet service; secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

- ✓ I understand that the school can check my child's school computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour.

- ✓ 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.

Lambton Primary School does not allow photos or videos of pupils to be taken at school by parents/carers, however photo opportunities sometimes occur after school events. In this instance any photos taken should only be of your own child. Video learning journeys are available after school assemblies and are only released when 100% permission is given by all parents/carers of that class.
Lambton Primary School requests that photos/videos obtained from school are not shared on any social networking site such as Facebook.

- ✓ I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent's/ Carer's signature:…… **Date:**…….

Acceptable Use appendix 3

At Lambton Primary School we have an Acceptable Use Agreement which is reviewed annually to safeguard and promote the welfare of staff and pupils.

Internet

Whilst ICT is exciting and beneficial in and out of education, web based resources are not well policed. All users need to be aware of the range of risks associated with the use of these internet technologies and their individual responsibilities relating to the safeguarding of children and themselves, in school and at home.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-safety curriculum. Pupils are aware of the impact of Cyber bullying and know how to seek help if they are affected by any form of online bullying.

Managing the Internet

- The school maintains that pupils will have supervised access to Internet resources through the school's fixed and mobile internet technology. All staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users must observe copyright of materials from electronic resources.

Internet Use

- Pupils at Lambton Primary are too young to use social networking sites, such as Facebook (the legal age limit is 13 year old). However, we recognise children are accessing the sites at home and provide information annually or as necessary to ensure privacy levels are high and children are aware of the risks.
- Annual E safety reminders are taught- specifically in safety week.

Security

Software security

- A security breach, lost stolen equipment, virus notifications, unsolicited emails and all other policy noncompliance must be reported to senior management.
- To minimise risk, pupils should not bring homework to school using portable memory sticks. **Work should be saved to memory stick.**

Password security

- Password security is essential for pupils
- Pupils are expected to keep their passwords secret and not to share with others, particularly their friends.
- Staff and pupils are regularly reminded of the need for password security.

E-mail

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the ICT Curriculum.