"Longwoodese – A Language We All Speak"

Promoting

- Enthusiasm
- Experience
- Expertise
- Emotional Intelligence and Wellbeing
- Environment

E-Safety Policy

Agreed: November 2016

Last Reviewed: August 2020 by CM

Next review date: August 2022

Introduction

The purpose of this policy is to protect and educate parents, pupils and staff in their use of technology. It also ensures that appropriate mechanisms are in place to intervene and support any incident.

The Policy relates to the Safeguarding Policy, Anti-Bullying Policy, Health and Safety Policy as well as the ICT curriculum and Internet access.

Most recent E-Safety staff training took place with Hertfordshire County Council in October 2018. Training has been discussed at School staff meetings.

Mr Malcolm Livesey is the E-Safety Lead.

What are the Risks?

Stranger Danger, Grooming, Inappropriate Websites, Cyberbullying, Peer on Peer Abuse, Sexting, Images, Identity Theft, Personal Information, Future Prospects, Blackmail, Threats, Contact with Birth Family and Location.

Inappropriate Websites

Pornography, Race Hate, Pro-Eating Disorders, Pro Self-Harm, Gambling, Violence and Extremism.

This policy addresses three areas of risk:

1. being exposed to illegal, inappropriate or harmful material;
2. being subjected to harmful online interaction with other users;
3. personal online behaviour that increases the likelihood of, or causes, harm.

OFSTED – OUTSTANDING SCHOOLS

All children feel safe – are highly aware of how to keep themselves and others safe, including in relation to E-Safety.

Writing and Reviewing the E-Safety Policy

- All staff members share responsibility for e-safety.
- Assemblies, lessons (ICT, PSHE and all subjects), plays / concerts / outings include e-safety to help pupils become safe users of new technologies. Pupils are encouraged to use the internet to aid their learning, with managed systems to protect them.
- Staff and families are encouraged to work together to develop clear strategies for e-safety, which must be reviewed and developed. The views of pupils and parents is used to develop e-safety provision.
- Staff are included in e-safety training as well as monitoring and reviewing technology and the risk it poses.

- Regular training is given by Hertfordshire County Council.
- Hertfordshire County Council emails their quarterly E-Safety newsletter which is distributed around Longwood. This is used to update this policy.

Education

The internet is an essential element in 21st century life for education, business and social interaction. Longwood School has a duty to provide pupils with high-quality internet access to enrich and extend the learning experience. It is also used to support the work of staff and enhance the School's management information and business administration systems.

Longwood School has a progressive curriculum that is flexible, relevant and engages pupils' interest. We promote E-Safety as well as inform pupils how to protect themselves and others.

Internet will enhance and extend learning

Staff are aware of and pupils will be educated in the safe use of the Internet.

Clear boundaries are set and discussed with staff and pupils, for the appropriate use of the Internet.

Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Managing Internet Access

- There is a Pupil Acceptable Use Agreement / E-Safety Rules document which is given to all parents of children in School each year. Parents are to read and discuss the e-safety rules with their child.
- There is a Professional Responsibilities for All Staff document. This is for when staff are using any form of ICT, including the Internet, at Longwood and outside Longwood. Staff have signed a register to acknowledge being given a copy of this document.
- Longwood has filtering software which allows only appropriate web sites to be visited at School.
- Staff are to ensure that the use of Internet derived materials complies with copyright law.
- Longwood uses TSO Hosting, which is a Recognised Internet Service Provider.
- Pupils are taught what internet use is acceptable and what is not. They are given clear objectives for internet use. Staff are to guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.
- Pupils are taught what to do if they experience material which they find distasteful, uncomfortable or threatening.
- Pupils are taught to be critically aware of what they read and are shown as well as how to validate information before accepting its accuracy.
- Where the internet may be used for homework research, suitable web sites, such as the BBC, will be recommended.

- No Nursery or Pre-School children under the age of 5 years have access to the internet at Longwood without direct supervision.
- E-Safety is promoted by the School Council.

E-Mail, Facebook, Twitter and other Social Network Sites

Access in School to external personal email accounts is not allowed.

Facebook and Twitter accounts are not appropriate for children under the age of 13 years, and therefore are not allowed at School and discouraged at home. Filters prevent access to social network sites at Longwood.

Any data sent via email relating to the personal details of children, families or staff is password protected.

Longwood School will educate pupils about social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils are taught how to report abuse and to talk to their class teacher if they are concerned about what they experience on their computer.

Pupils are taught the reasons why personal photographs should not be posted on any social network space without considering how the photograph could be used now or in the future. Parents are allowed to take photographs at school concerts etc, but are warned not to post these on any social media if the photo includes any child other than their own.

Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communication. Pupils should only invite or communicate with known friends and deny access to others.

Security of Data

All data relating to the personal details of staff and children is kept in files at the main office or Mr Livesey's office, which is manned or locked at all the time that Longwood is open. The information is locked away when Longwood is closed. Data stored in classrooms is kept in cupboards which are locked when the teacher is not present.

Personal data relating to the children is stored on the main office computer which is protected by a password.

Teachers and Nursery Staff hold other assessment and records of children on their own or Group computers. These are protected by passwords.

Email accounts, Microsoft Accounts package and any School Management Packages are protected by passwords.

Relevant staff know passwords and therefore have access only to what is relevant to them. The office staff and SMT have access to all data. The teachers and Nursery staff only have access to the assessment records of the children they teach or care for.

Mobile Telephones

These are not to used anywhere in the building except in the staff room. This applies to visitors, parents, teachers and staff.

Digital Photographs

These are taken on cameras supplied to each Nursery group room and School class for evidence of children's achievements. These are downloaded onto the main office computer for printing. The digital copy is then deleted from the camera and computer immediately after printing. Some photographs are used for assessment/archives, which may be uploaded to cloud storage.

E-Safety Advice for Parents and Staff

Hertfordshire County Council has a document with advice for parents (January 2014). This can be downloaded from our web site.

Parents should read and take note of the Facing up to Facebook – the magic 13! (Hertfordshire County Council) document, which can be downloaded from our web site. Parents should use this advice as well as the E-Safety and Acceptable Use of ICT Agreement.

Parents are to ensure that their children play age-appropriate games. Parents are to take note of the **PEGI age rating** for each game.

Many **Apps** have an age requirement in their Terms and Conditions.

Parents are to watch out for **ask.fm**, **chat roulette** and **snapchat** web sites and many others. Children should not be using these sites.

Cyberbullying – One in three 11 to 16 year olds have been deliberately targeted, threatened or humiliated by an individual or group through the use of mobile phones or the internet.

Parents are to look at website **www.thinkuknow.co.uk** run by CEOP.

Parents of 4-7 year old children - search for CEOP Lee and Kim for Lee and Kim's Adventures.

Parents of 8-10 year old children – search for CEOP Jigsaw.

Grooming – this is not always aimed at meeting the child, and is becoming more 'clever' and is not always sexual. Talk to your children:

- About how easy it is to lie online
- About their online friends
- About never meeting an online friend   **REPORT INAPPORPRATE CONTACT TO**:
- About how to report inappropriate contact   **ceop.police.uk**
- About how you are there to support them

Worried, Frightened or Scared – children can ask for help – www.cybermentors.org.uk