LONG MEADOW SCHOOL

E SAFETY POLICY

Policy adopted:	September 2014
Date of last review:	June 2017
Date of next review:	June 2018
Type of policy:	Non- Statutory / LMS
Frequency of review:	3 years
Governor committee:	Curriculum Committee

Long Meadow School
E-Safety Policy

The aims of our E-Safety Policy

The school has a responsibility to protect and educate pupils and staff in their use of technology and their on-line presence by helping them to develop the skills to stay safe online. The school will provide all stakeholders with the means and appropriate mechanisms to intervene and report incidents and concerns.

Definition of E-Safety

Risk can be categorised into three areas:

- Content: being exposed to illegal, inappropriate or harmful material which may include pornography, ignoring age ratings on games, substance abuse, racist language and pro-anorexia, self harm and suicide sites
- Contact: being subjected to harmful online interaction with other users – grooming, cyber-bullying, identity theft
- Conduct: personal online behaviour that increases the likelihood of, or cause, harm, privacy issues, including disclosure of personal information, digital footprint and online reputation, health and well-being (amount of time spent online), sexting (sending and receiving of personally intimate images, copyright infringements

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the school

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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Protection on the school's network

The school computing network has a firewall and web-filtering system in place, known as Protex. Should any material of an inappropriate nature appear on a device in school, details of the web address must be maintained and the school's broadband provider, E2BN, can be informed so that it blocked in future.

Protex is used by many Local Authorities to provide a compliant web filtering service for hundreds of schools in the UK. E2BN applies Internet Watch

Foundation Child Sexual Abuse block lists and Home Office "Prevent" lists. It is compliant with DFE guidelines . Further details can be found here: http://blog.e2bn.org/wp-content/uploads/2016/09/Appropriate-filtering-response-E2BN.pdf

How is E-Safety taught?

E-safety is taught as part of the Computing curriculum and 'Being Safe On-Line' needs to be referred to in every computing lesson. E-Safety is also taught in PSHE lessons with reference to staying safe and cyber-bullying. It is an essential part of 'circle time' discussions. All classrooms have the 'SMART' poster on display giving advice on E-Safety behaviour. School assemblies are also used to provide information to the children.

Pupil E-Safety curriculum

The curriculum covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music/video files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the 'CLICK CEOP' button.

Responsibility for E-Safety
Responsibility for E-Safety lies with the Headteacher. All adults working with children using any IT device is responsible for not only keeping them safe, but also educating them to the challenges faced in the on-line world. All adults working in the school are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements (Currently Protex, backed by Eqiinet, approved by DfE) • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles • To be aware of procedures to be followed in the event of a serious e-Safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures • Ensures staff will model safe and responsible behaviour in their own use of technology during lessons. • Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights; • Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling • Monitor reports of E-Safety issues on CPOMS
E-Safety Coordinator Deputy Headteacher	• To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy • To promote an awareness and commitment to e-safeguarding throughout the school community • To ensure that e-safety education is embedded across the curriculum • To liaises with school ICT technical staff • To communicate regularly with SLT and the governing body to discuss current issues and incidents • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident • To ensure that the CPOMS e-Safety incident log is kept up to date • To facilitate training and advice for all staff • To liaise with the Local Authority and relevant agencies • To remain regularly updated in e-safety issues and legislation
E-safety Governor	• To ensure that the school follows all current e-Safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider

Role	Key Responsibilities
	community to become engaged in e-safety activities
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly
IT support contractor	• To report any e-Safety related issues that arises, to the e-Safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy. • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls exist to protect personal and sensitive information held on school-owned devices • To ensure web filtering is applied and updated on a regular basis • To keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To check that the use of the *remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
School Administrator	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Policy • To report any suspected misuse or problem to the using an e-safety incident form – available in the staff area on the network • To maintain an awareness of current e-Safety issues and guidance • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones and private messaging • Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

Role	Key Responsibilities
Pupils	• To read, understand, sign and adhere to the Pupil Internet Agreement • To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To 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 covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies
Parents/carers	• To support the school in promoting e-safety and endorse the Pupil Internet Agreement' • To consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

How do pupils raise concerns?

Pupils will be taught to raise concerns when they feel uncomfortable on line at anytime, either at home or in school. They will be shown how to turn the screen off so that the information is retained but cannot be seen by other children. They will then be taught how to tell their parent, carer or teacher immediately. In situations where a child has been made uncomfortable by the actions of another online user, they need to be taught how to report this via CEOP or the NSPCC. The 'CEOP Report' button is on the front page of the school website.

How do Staff raise concerns?

Staff should raise their concerns by reporting them via CPOMS once the incident has been investigate and resolved. If staff feel unable to resolve an issue they will refer it to the E-Safety Coordinator.

How do Parents raise concerns?

In the first instance, parents and carers should report their concerns to the class teacher. If the information is of a particularly sensitive nature, parents and carers may wish to speak directly to the headteacher.

Keeping Parents Informed

The school will hold regular face to face briefings for parents, provide resources, send updated alerts as well as providing information to parents on the content of the annual ‘Internet Safety Day’

Monitoring Current Trends

The school will annually undertake a survey of the children’s on-line behaviour and report its findings to parents, staff and the governing body. Depending on the outcome of the survey, the school may decide to adapt its E-Safety teaching in order to react to current trends.

Staff Professional Development

E-Safety training is provided annually to all staff at the start of the school year. A briefing is also held midway through the year to discuss the content and focus for the annual ‘E-safety Day’. Staff are kept informed of urgent updates through the school email system.

Consequences for Breaches of the E-Safety Policy by Pupils

The school behaviour policy should be implemented should a child breach the E-safety policy, with staff deciding what consequences should be put in place. Issues of cyber-bullying should be treated as bullying if the actions of the child too place in the school or if outside school, had its roots in membership of the school.

Policy Review

The E-Safety policy should be reviewed every three years, although it may be updated in line with current advice.

DM June 2017