Online Safety

Adopted On:	September 2016
Review Date:	September 2017
Review Frequency:	Annually
Committee Responsible:	Exec

Online Safety Policy

Online Safety at Moss Lane

At Moss Lane we take online safety seriously. To ensure we keep children and adults safe, we apply a triad of strategies using **policies, educational training** and **technology** (infrastructure).

It is universally recognised that the appropriate use of technology brings great benefits to learning and achievement in schools. We use online technologies to communicate, work more efficiently, share resources and manage information and data.

This widespread usage has increased the risk of potential safeguarding issues relating to online activities. Recognising the online safety issues and planning accordingly ensures our children are kept safe so they are protected from potential harm, both within and outside school. At Moss Lane, we believe there must be a balance between protecting children with safety nets and teaching 'digital online resilience'. We develop children as critical thinkers so they have the skills to deal with risks and make informed decisions.

The schools commitment to online safety is part of its safeguarding responsibilities. Therefore, this policy relates to other policies including **Safeguarding, PHSE, Behaviour, Acceptable use and Anti-bullying**. The DSL (Designated Safeguarding Lead / Head teacher) works closely with the Online Safety Leader, staff, and the Online Safety Governor to make sure policies are consistent and complement each other to keep children safe.

Currently the internet technologies children are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst we are aware that we work with young children in Foundation and Key Stage One, we are also aware that they witness the use of these technologies by others.

Our main safety net for the children's use is **Hector Protector.** This is a dolphin on screen the children can click on if they feel unsafe. The staff uses the website https://www.thinkuknow.co.uk/5_7/hectorsworld/ to introduce Hector to the children and how they can use it. From year 1 the children are also shown how to click on the home screen tab to go back to a safe page.

Online Safety Team

This online-safety policy has been developed by a working group including the:

- *Head teacher (DSL)*
- *Online-Safety leader (**CEOP trained)***
- *Impero online safety adviser*
- *Parent governor responsible for safeguarding*
- *Children (pupil voice included in termly discussions and through acceptable use messages relayed to other pupils when they log on.)*

Every child in the school has read or listened to the 'Acceptable Use Policy' and have agreed to follow the rules. Each class links an area of policy to the value of the month (on rotation) so children are contributing to the online safety rules in school. Their links are put on screen for children to read every time they go online in the computer suite. This ensures the children remain up to date and it keeps the message fresh.

Consultation with the whole school community takes place through a range of formal and informal meetings. We will also ask for parents and children to alert us of any concerns with online safety so we can review our policy as situations arise.

The online safety group has responsibility for monitoring the online-safety policy including the impact of initiatives. They will discuss:

- The monitoring and review of the school online-safety policy
- The monitoring and review of the school filtering system
- The review of the online safety curriculum and its impact
- Monitoring the incident logs
- Consulting stakeholders – including parents / children /staff
- Monitoring improvement actions

Schedule for Monitoring and Review

This online safety policy was approved by *Governing Body*	*September 2016*
The implementation of this online-safety policy will be monitored by the:	*Online Safety Team*
Monitoring will take place at regular intervals and as and when incidents occur:	-Using Impero software during teaching sessions as concerns arise -Reporting key words put into Impero as we become aware of new developments -Feedback and discussion meetings twice a year with CPO and responsible person- named governor.
The *Governing Body* receive a report on the implementation of the policy including details of online-safety incidents at regular intervals	
The Online safety Policy is reviewed annually, and regularly in the light of new developments or reported incidents. The next anticipated review date will be:	*September 2017*
Should serious online-safety incidents take place, the following external persons / agencies should be informed:	*Online safety leader/ CPO/ Police*

Risks

The Byron Review "*Safer Children in a Digital World*" published in 2008 illustrates the potential online risks to children and young people in the following grid:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content (child as recipient)	adverts, spam, sponsorship, personal info	violent/hateful content	pornographic or unwelcome sexual content	bias, racist, misleading info
Contact (child as participant)	tracking, harvesting, personal info	being bullied, harassed or talked about	meeting strangers, being groomed	self-harm, unwelcome persuasions
Conduct (child as actor)	Illegal downloading, hacking, gambling, terrorism	bullying or harassing another	creating and uploading inappropriate material	providing misleading info/advice

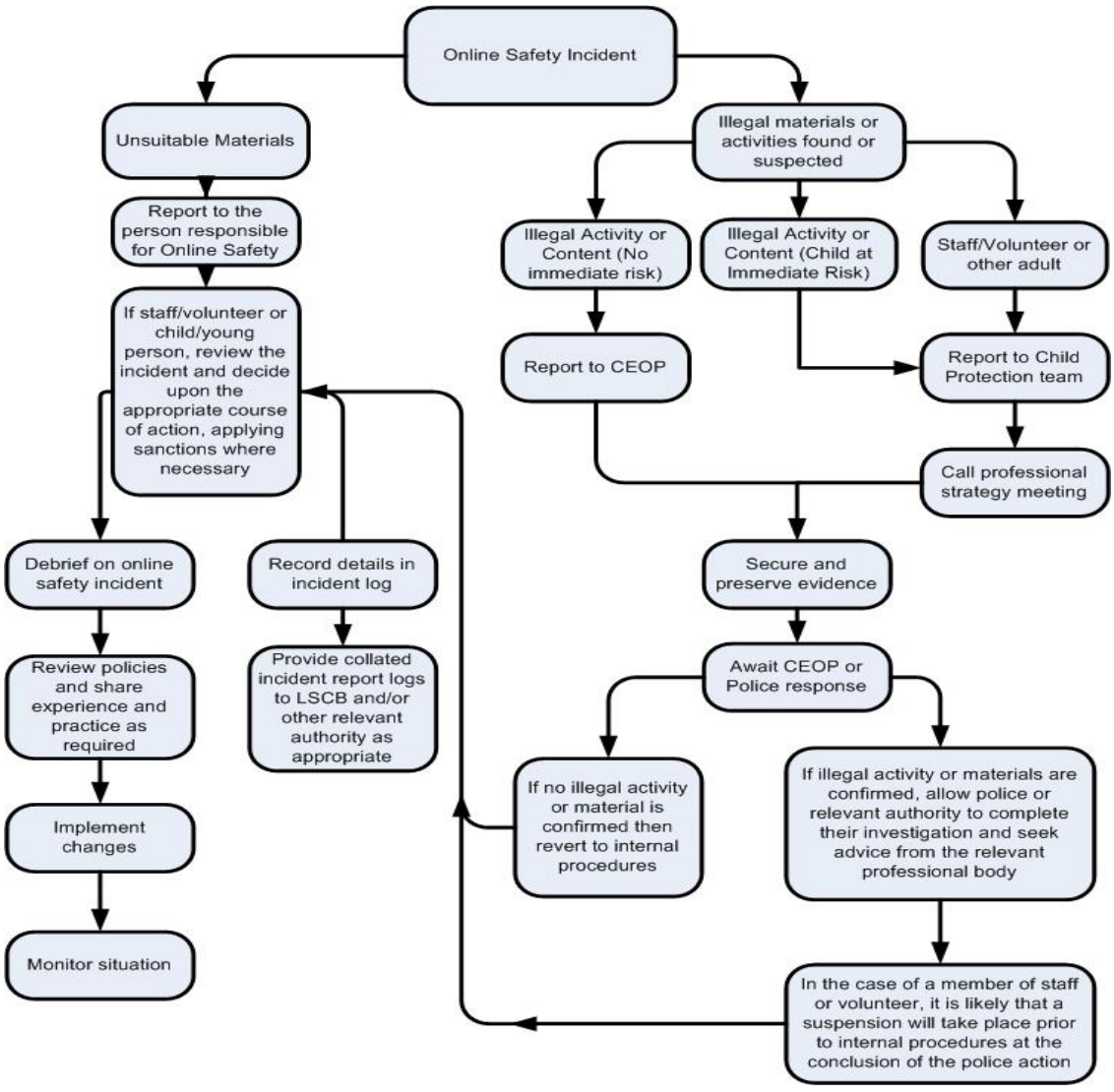
Managing Risks

Reporting and Recording incidents

Complaints of Internet misuse will be dealt with by the head teacher VA. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. This includes incidents of when devices are reported as unsafe e.g. illegal images are found.

If a child reports a concern (e.g. clicks on **hector** or the **home screen**) to indicate they do not feel safe, the adult responsible at the time will check the content and if they are concerned they will record the URL (address), time, date and content to the CEOP (head teacher) and the online safety leader. The two responsible adults will act on the report and decide what action should or should not be taken. Depending on the severity of the incident, other parties may need to become involved such as the police. All reported incidents will be recorded on an online safety incident form. The child will be praised for alerting an adult.

Online safety flow chart-procedures



Record of online safety incidents

To ensure this form is covered under the schools Data protection policy, all completed forms will be given to the DSL (Head teacher) who will store these in her office.

Group/Names	
Date	
Reason for investigation	

First reviewing person

Name		
Position		**Signature**

Second reviewing person

Name		
Position		**Signature**

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

Online Security at Moss Lane

Virus protection

This is installed and updated regularly. Our school currently uses RM for Broadband (Sophos for virus protection) with its firewall and filters.

Impero software

The online safety leader (CEOP) has been trained in using Impero and has trained the teachers. They can monitor the use of computers in the computing sweet, blank screens, lock screens, remote in and control screens, power on or off individual, or all screens. Teachers will use this software to monitor activity during lessons. They will be trained on how to report incidents as they arise through teaching. Any violations that appear through Impero monitoring will be assessed by the online safety leader and CPO and a decision will be made regarding appropriate action. We can also add key words to block access when deemed appropriate or necessary.

Using approved websites

A technician from JSCP is employed by the school. He works with the school on any online safety issues. This includes liaising with the online safety leader and CEPO.
He also ensures:

- the school's technical infrastructure is secure and not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis in consultation with the Head-teacher and online safety leader
- that monitoring software /systems are implemented and updated as agreed in school policies
- that we use a recognised Internet Service Provider (ISP) or Regional Broadband Consortium.

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online-safety and acceptable use. Filtering systems are in place and flexible to allow for the online safety leader to add more language to be filtered through Impero software. Filtering will show a SURF PROTECT screen. If staff feel this is not necessary for some sites they can inform the online safety leader who will liase with the staff and technician. It is hoped that by having a managed system of filtering, children will have better knowledge and understanding of how to stay safe.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use online devices in an appropriate way. The school will help parents understand these issues through parents' evenings, newsletters, and guidance through appropriate websites e.g.

www.swgfl.org.uk
www.saferinternet.org.uk
www.childnet.com/parents-and-carers
www.internetmatters.org

Parents and carers will be encouraged to support the school in promoting good online-safety practice.

Parents are kept up to date about online safety tips and there are various links to this on the school website. Parents are also invited to informed online safety training sessions.

We also have a CEOP report button on our website where parents and carers accessing the site can report any concerns they have.

Staff Training

We have regular up to date training as the online safety leader acquires new knowledge of safety issues and shares this with the team.

We have a duty to **PREVENT** children from radicalisation. The school has read 'The Prevent Duty' departmental advice for schools and childcare providers June 2015, and knows "*the need to have safeguarding arrangements to promote pupils welfare and prevent radicalisation and extremism*.' Staff and Governors have also completed the online PREVENT training course.

Staff are aware of the 'increased risk of online radicalisation through the use of the internet and have therefore been trained to monitor the use of digital technologies using Impero software. Staff know that when they identify potential risks, they must report these to the CPO and online safety leader.

The online safety leader will receive regular updates through computing network meetings and regular monthly updates through recognised county recommended websites such as internetmatters.co.uk. The online safety leader will lead staff meetings and update staff as new technologies and risks arise.

New staff to the school will be trained in Impero software to monitor internet use when teacher as part of the induction program. Governors responsible for safety will be invited to take part in any online safety training for staff.

Curriculum

We have a 'managed approach' providing a safety net for everyone in school whilst teaching resilience and knowledge of what to do if they feel unsafe.

Online access will be planned to enrich and extend learning activities. It is intended to be flexible, relevant and engaging where we use devices that promote the use of up to date technology.

Staff will guide children in on-line activities that will support the learning planned for their age and maturity. They will also teach them how to search online effectively e.g. put search category in 'to limit results and provide safe research options such as http://swiggle.org.uk/ and 'DK find out' interactive encyclopaedia.

Through a progressive online safety curriculum, children will be educated about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. Children are taught about online safety from their first use of technology at school. Children will be educated to take a responsible approach which is part of the termly lessons children receive at Moss Lane. Children will be taught to recognise and avoid **online**-safety risks and build their **resilience**. Children will be rewarded for positive use through praise and in school reward systems.

Through modelling and specifically planned lessons, children will be shown what to do if they see or hear anything that makes them feel unsafe. They are shown how to click on 'hector protector,' a built in safety dolphin which will immediately blank their screen so the adult can check the content. From year 1, they are also taught that they can click on the home icon to return to the home page (a safe place.)

Children throughout the school are also taught to recognise and discuss the online safety SMART posters. These are displayed at every work station throughout the school and referred to before any online activity. This includes

S – safe, keep it secret
M – meeting strangers means dangers
A – ask before accepting,
R – real, is it true?
T – tell an adult if you feel unsafe.

The online safety leader will also share the safety rules with the whole school in termly assemblies.

More vulnerable children

Some groups of children are potentially more vulnerable and at risk than others when using technology. These can include children with emotional or behavioural difficulties, learning difficulties, and other complex needs, as well as those whose English is an additional language, and looked after children. Children with Special Educational Needs (SEND) can and should use the internet in educational, creative, empowering and fun ways, just like their peers. However, staff need to monitor usage carefully as they may be particularly vulnerable to online-safety risks. For example:

- Children with Autistic Spectrum Disorder may make literal interpretations of content, which will affect how they respond.
- Some children may not understand much of the terminology due to language delays or disorders.
- Some children do not understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgements about what is safe information to share. This leads to confusion about why you should not trust others on the internet.
- There is also growing concern around cyber bullying. We need to remember that some children with SEND may be vulnerable to being bullied through the internet, or may not recognise that they are being bullied.
- Some children may not appreciate how their own online behaviour may be seen by someone else as bullying.

Where appropriate, staff liase with the SEND co to ensure appropriate risk assessments are in place for these children.

Further reading

- http://www.saferinternet.org/ww/en/pub/insafe/index.htm
  http://www.surreyesafety.co.uk/
- http://swgfl.org.uk/
- http://www.bbc.co.uk/cbbc/curations/stay-safe
- www.surwww.esafetyadviser.co.uk