Merridale Primary School
E-safety Policy
September 2018
Due for Review: September 2019

School Vision

Technology is now considered to be an essential part of modern life and that it is a duty to provide pupils with quality technology as part of their learning. Merridale Primary School embraces this challenge and this digital safeguarding policy considers the use of both fixed and mobile devices with internet connections, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, gaming devices and other portable media devices. It will be revised to incorporate new and emerging technologies as they appear.

Equality and Diversity

The use of technology is a part of the statutory curriculum and a necessary means of delivering 21st century teaching and learning for staff and pupils. Internet access is an entitlement for all. However, responsible and safe use must be at its core.

Technology in a changing world

Schools are part of a world where technology is integral to the way life is led in the 21st century. Compared to even five years ago the technology available outside school is rapidly increasing. In line with the Gilbert review document 2020 Vision, schools need to increasingly respond to:

- An ethnically and socially diverse society
- Far greater access and reliance on technology as a means of conducting daily interactions and transactions
- A knowledge based economy
- Demanding employers, who are clear about the skills their businesses need and value
- Complex pathways through education and training, requiring young people to make choices and reach decisions.

Why do learners need to be safe working with technology?

As the uses of online technology resources grow, so has the awareness of risks and potential dangers which arise for their use. The school aims to prepare its learners to be able to thrive and survive in this complex digital world. This policy outlines the safeguarding approach to achieve this.

Management of Digital Safeguarding

Clearly stated roles and responsibilities-

- **Headteacher**

  The headteacher will ensure that the digital safeguarding policy is implemented and will monitor compliance with the policy, and that appropriate roles and responsibilities of the school's digital safeguarding structure is in place. They will ensure regular reports on the monitoring outcomes for digital safeguarding are reported to the governing body.

- **Nominated e-safety coordinator**

  There is an identified e-safety co-ordinator who is responsible for e-safety developments in school and sharing of practise with staff and the wider community of governors and parents.

This person will be in receipt of current training of the latest guidance and procedures and is the main contact for local authority e-safety networks.

All digital safeguarding incidents within the school need to be reported to this person. They will use the SIMs behaviour tracker to keep a log of e-safety incidents. Alongside the headteacher, they will make decisions about how to deal with reported incidents and adapt policies where necessary. They will also ensure that appropriate education is put in place as a response.

- **E-safety governor**

There is an identified safeguarding governor who monitors and liaises with the e-safety co-ordinator and who will report to the full governing board.

- **E-safety responsibility within subject and management roles**

All staff with subject and management roles have a duty to incorporate e-safety principles in their area of responsibility, deputising to any of the above roles where necessary.

- **Teacher**

All staff understand the need for care and caution when using technology both for academic and social purposes and apply it to teaching and learning situations. They need to work to the agreed guidelines. They have a “front line” monitoring and reporting role for incidents.

- **Learning Mentor**

The learning mentor will work alongside the e-safety co-ordinator to monitor e-safety incidents within school and help to deliver appropriate education to children and parents who are involved.

- **Support Staff**

  As for teaching staff, however, given the nature of their role, learners may find it easier to disclose incidents to them. Support staff should be clear about the reporting procedures and use these when incidents occur.

- **School Council Representatives and Digital Leaders**

  As a responsible member of their class, the school council need to have e-safety as an item on their agenda. These representatives could help to monitor the appropriate use of technology at a learner level within the school.

Procedures

- All staff and members of the school workforce and children will sign an AUP (acceptable use policy) on an annual basis to ensure that all changes have been agreed.
- Children will be taught about the CEOP report abuse button during e-safety lessons. E-safety issues should be reported to class teacher or e-safety co-ordinator.
- A log of e-safety incidents will be kept on the SIMs behaviour tracker and these will be reviewed termly by the e-safety co-ordinator to ensure that next steps have been implemented.
- If child safeguarding issues arise they will be reported to the safeguarding co-ordinator and procedures as defined in the school’s safeguarding policy will be followed.
- If necessary the headteacher and safeguarding co-ordinator will follow appropriate procedures for reporting incidents beyond the school to the LA.

    - All staff are entitled to training and support regarding e-safety. This will be delivered on a regular basis and a record of its delivery will be kept.
- E-safety education is built into our PHSE and computing curriculum with e-safety education being delivered at an appropriate level on a regular basis. Our e-safety curriculum map outlines objectives taught each year.
- We will endeavour to provide appropriate training for parents and keep a log of training provided.
- If e-safety incidents occur, the e-safety co-ordinator will ensure that appropriate teaching is put in place to respond directly to the incident.
- E-safety teaching will be monitored as part of our teaching and learning policy.
- The incident log will be reviewed to effectively assess the impact of e-safety practise and this will be used to inform future planning.

Risks and Acceptable Behaviours

- General use of the internet

The internet is a vital tool to be used inside and outside of school. However there have to be procedures put into place to ensure appropriate use. At the beginning of each year, children are required to sign an AUP appropriate to their Key Stage, which refers to appropriate internet use.

- Passwords/personal details

Both children and staff are given passwords and logon details to access the learning platform. Staff are encouraged to personalise their password and change it regularly. Children are encouraged to report any occasions when there password may have been compromised so that it can re-set accordingly. In foundation stage and key stage 1 children will log on to the school system with a generic username and password which will typically be entered by a member of staff. From key stage 2 all pupils will use an individual username and password to access ICT facilities within school.

- Data Security

We discourage the use of memory sticks especially if they contain sensitive information about children e.g. photographs or personal details. Rather than memory sticks staff are encouraged to use the Learning Platform or the staff shared area for data storage and security. In case of theft, we encourage all staff to not store images of children on their laptops.

- E-mail

Staff are encouraged to use their Cloud W email account rather than a Hotmail or Yahoo account as they are easily ‘hackable’. We also encourage staff not to email files that contain any details of pupils, using the cloud w platform as an alternative.

- Cloud W

The cloud w Learning Platform is widely used by staff, children and governors. To ensure digital safety, all users have a personal logon and password that is unique. All users are

encouraged not to share their details with anyone particularly when out of school setting. Each class site has a set of class site rules outlining how children should conduct themselves. If a password breach occurs the e-safety co-ordinator is responsible for altering the password accordingly. Staff and pupils who leave the school will be removed from the learning platform through the regular running of the SIMs connect tool and this will be monitored by the e-safety co-ordinator.

- Appropriate use of hardware

Staff are given appropriate training when they receive a new piece of hardware. They are asked to sign a laptop agreement when they begin employment at the school.

- Photographs, video and sound recording

At the beginning of their time at Merridale, parents will complete our internet and photography permission form which allows children to be photographed and recorded during their time at school. A central list of permissions is held on the staff shared area and all school staff should be aware its contents. If children are not allowed then relevant staff will need to be aware and ensure that this is adhered to.

- Copyright

Staff are made aware of copyright issues through appropriate staff training and a digital copyright statement. If they wish to use images or videos then there are 'copyright' free sites such as www.freeplaymusic.com which are accessible. Children will routinely explore copyright issues where appropriate.

- Social networking/cyber bullying

Social networking plays a huge part in today's society. Staff are made aware of the Local Authority view regarding acceptable behaviour - staff should not to make any reference to their job, school or other colleagues on the site and are strongly discouraged from accepting friend requests from current or former pupils under 18 years of age. Any disclosures made regarding cyber bullying that occur either within or outside school should be reported and dealt with the school's anti-bullying policy. Cyber bullying will be covered during e-safety education across year groups.

- Mobile phones/technology

Children are discouraged from bringing mobile phones into school unless a parent specifically requests this. If this is the case then they should be handed in at the main office at the beginning of the day and collect them again at the end of the day. Staff are not permitted to use a mobile phone within the hours 8.30am – 4.30pm except in the PPA room, staff room or school office. Videos and photographs are not to be taken or stored on staff mobile phone under any circumstances.

Physical and technical security

- Firewall, filtering, antivirus provision

We have firewall protection on a local level and we connect to the internet via a proxy server which has network filtering, anti virus protection and spam protection. This is all carried out through the LA technical support and in line with LA guidelines.

- Passwords

We have separate security and permissions to files and folders on the school server to allow and deny access. All users have an individual password and username, with the exception of children in Foundation and Key Stage 1 (see earlier in the policy)

- Network monitoring

Network traffic is monitored by ITCS and the civic centre on a corporate level. This is in line with LA guidelines and support.

- Personal safety

Laptops are stored in a locked laptop trolley within the school strong room. The keys for this are kept in a secure office. Staff laptops need to be kept secure at all times, in line with the staff laptop agreement.

- Security marking and inventory

An inventory of the school ICT equipment will be undertaken annually and updated as necessary. The inventory will make it clear where staff responsibility lies for ICT equipment.

Impact of the Digital Safeguarding Policy

The effectiveness and impact of this policy may be measured in the following ways:

- Termly report of incident log.
  E-safety incidents will be recorded through SIMs behaviour tracker. All incidents of a digital safeguarding nature will be reported in the same manner as other safeguarding incidents. Termly statistics will be reported to the headteacher by the e-safety co-ordinator.