Merrydale Infant School
E-safety policy

Chair's signature … Mrs Elizabeth Surtees

Head's signature… Mark Tipple-Johnson

Date agreed by the Governing Body 7th April 2022

Review date…April 2023

This policy runs in co-ordination with the schools existing GDPR policies and procedures

Statement of intent

We fully recognise the contribution we can make to protect children and support them in school. This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies. These new technologies include internet access, cameras, mobile phones, and MP3 players which children could use in school or at home. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

Aim

The aim of this policy is to safeguard and promote pupils' safe use of internet and electronic communication technology such as mobile phones and use of email.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from the East Midlands Broadband Consortium;
- A school network that is compliant with National Education Network standards and specifications.
- Staff have received whole school safeguarding training including CSE and on line grooming. Staff have also been encouraged to familiarise themselves with Leicestershire Police information https://leics.police.uk/advice-and-information/kids-and-teens/grooming-and-cse

Writing and reviewing the e-safety policy

This policy has been written in consultation with senior staff and governors. It will be reviewed on an annual basis. The ICT coordinator is the e-safety co-ordinator.

Teaching and learning

Why the Internet and digital communications (e.g. email, text messaging) are important

- Merrydale Infants recognises the importance of new technologies.
- Pupils can **Discover** (The internet is the biggest library in the world)
- Pupils can **Connect**(The internet allows pupils to connect across the planet
- Pupils can **Create** (The internet allows pupils the opportunity to become publishers)

Pupils will be taught how to evaluate Internet content

Using the 'ThinkUknow' website children will be taught to:

- Always ask a grown up before they go on the internet
- Never tell a stranger personal information
- Never to send images to strangers
- How to be aware of concerns and how to alert responsible adults.
- How to stay safe if using social network sites, which could include young children's gaming sites e.g. 'Club Penguin'.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

Published content

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

Social networking and personal publishing

- Sites such as MSN, Face book, My space, Bebo, Build a Bear etc. will not be used with children. EMBC currently block access to such sites.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for infant aged pupils.

Managing filtering

- The school will work with the LA and ASK to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
- The ICT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit.

- Staff and parents/carers should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will not be allowed (but kept under review in light of changing advances in technology).
- Staff will use a school phone where contact with pupils is required and a school digital camera to capture photographs of pupils.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- From September 2011, all staff will be required to read and sign the ‘Staff Code of Conduct for ICT
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- All persons allowed access to the internet from the school site must follow the e-safety policy.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor LCC can accept liability for any material accessed, or any consequences of Internet access. When such a situation occurs the expectation is that the incident must be reported immediately. A screening tool exists to support the user to follow in the event of unsuitable material being accessed.

- 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 and effective.

Handling e-safety complaints

- Any complaint about staff misuse must be referred to the Head teacher or Chair of Governors.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Parents will be informed of the complaints procedure
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety, when this becomes necessary.

Communications Policy

Introducing the e-safety policy to pupils

- E-Safety rules will be posted around the school and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, based on the materials from CEOP using primarily the ‘ThinkUknow’ materials.
- E-Safety training will be embedded within the ICT scheme of work.
- Each academic year there will be an e-safety week.
- One day every half term pupils will have e-safety lessons.

Staff and the e-Safety policy

- All staff who use the school’s ICT resources will be given the School e-Safety Policy and its importance explained.

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Access to the web is filtered by Capita.
- Staff may use the school's ICT resources outside contracted time for personal use e.g. to shop, book tickets and for personal email. The school's ICT resources will **NOT** be used to access social networking sites.
- Whatever staff do outside school, in their own time and using their own resources, should not bring the school or any colleague into disrepute.
- If staff use their own ICT resources to access social networking sites, they are strongly advised not to have 'friends' who are under the age of 18 (particularly ex-pupils) unless these are family members.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters.
- Information on e-safety will be given to parents at the start of year or be available on the website and attention drawn to it via the monthly newsletter.

Appendix 1: Useful resources for teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Becta
http://schools.becta.org.uk/index.php?section=is

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen

www.digizen.org/

Kent e-Safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/e-safety_home.cfm

Kidsmart
www.kidsmart.org.uk/

Kent Police – e-Safety
www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html

Leicestershire Constabulary – Internet Watch Foundation
www.leics.police.uk/advice/2_information_zone/50_internet_watch_foundation

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 2: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Kent leaflet for parents: Children, ICT & e-Safety
www.kented.org.uk/ngfl/ict/safety.htm

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

Merrydale Infants School
Staff Code of Conduct for ICT / Computing

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system that in any way contravenes the Computer Misuse Act or Data Protection Act. School devices, e.g. laptops will be monitored through Policy Central both in and out of school for appropriate use.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that school information systems may not be used to access social networking sites for personal reasons.

- I understand that my use of school information systems, Internet and email is monitored by Policy Central and recorded to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than is authorised.

- I will not install any software or hardware without permission.

- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the E-Safety Coordinator / the Designated Senior Person for Child Protection.

- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will not use any ICT systems or social media e.g Facebook or twitter to bring the school or any colleague into disrepute.

The school has exercised its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Name: …… Signed: …… Date: ……