# MEREWORTH COMMUNITY PRIMARY SCHOOL

# E-SAFETY POLICY

| | |
|---|---|
| Date of Publication | March 2016 |
| Person with Responsibility | Amanda Lavelle<br>Head Teacher |
| Review Date | Term 4 2017 |
| Governing Body | School Effectiveness Committee |

| | |
|---|---|
| Chair of Governors<br>*Signature and Date* | |
| Governor with responsibility for Safety & Well-being<br>*Signature and Date* | |
| Head Teacher<br>*Signature and Date* | |

## Contents of e-Safety Policy



## Appendices

## 1. Introduction

This e-Safety policy has been discussed with staff, agreed by senior management and approved by Governors. It will be reviewed annually.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

## 2. Context and Background

**The technologies**

ICT in the 21st Century has an all-encompassing role within the lives of the children and adults. New Internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- E-mail
- Instant messaging
- Web based voice and video calling( e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites(e.g. Facebook)
- Blogs
- Podcasting ( radio/audio broadcasts downloaded to computer or MP3/4 player
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

**Our whole school approach to the safe use of ICT**

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- E-safety teaching is embedded into the school curriculum and schemes of work.

## 3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aim to embed safe practices into the culture of the school.

**Leadership Team**

The SLT ensures that the policy is implemented across the school via the usual school monitoring procedures.

**e-Safety Leader**

The school e-safety Leader is Faye Booth (PSHE subject leader).She is responsible for monitoring and reviewing the e-Safety policy, in line with safeguarding pupils and pupils' health and well-being. She is also responsible for keeping up to date on all e-safety issues and ensuring that the staff are updated as necessary.

**Governors**

The school governing body is responsible for overseeing and reviewing all school policies, including the e-safety policy**.**

**School Staff**

Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

The school will maintain a current record of all members of staff that are granted access to the school's electronic communications. All staff will read and sign the e-Safety policy Staff Agreement form before using any school ICT resources. All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Staff should ensure they are familiar with the school e-Safety policy, and ask for clarification where needed.

Class teachers should ensure that pupils are aware of e-Safety rules, introducing them at the beginning of each school year and reinforcing them during lessons.

**Pupils**

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school. They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school. E-Safety rules will be posted in all rooms with Internet access. An e-safety training programme will be established across the school to raise the awareness and importance of safe responsible internet use amongst pupils.

**Parents**

Parents are given information about the school's e-Safety policy with their admission forms. They are given an Internet agreement form and asked to support these rules with their children. Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days. Advice on useful resources and websites, filtering systems and educational

and leisure activities which include responsible use of the Internet will be made available to parents.

## 4. Technical and hardware guidance

### School Internet Provision

The school uses the standard LA Internet Service Provider, which is EISnet.

### Content Filter

EISnet use a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is possible for unsuitable material to occasionally get past the filter.

- All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

### Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate and may adversely affect the performance and reliability of school equipment.

- Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate member of staff.

### Portable storage media

- Staff are allowed to use their own portable media storage (USB keys etc.). If use of such a device results in an anti-virus message they should remove the device and immediately report to the ICT technician (Carol Spencer).

### Security and virus protection

The school subscribes to the McAfee antivirus software program. The software is monitored and updated regularly by the school technical support staff.

- The use of user logins and passwords to access the school network will be enforced
- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICT technician.

## 5. e-Safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At our school we are committed to teaching pupils to use ICT effectively and appropriately in all aspects of their education.

**Internet access at school**

**Use of the Internet by pupils**

Pupils are always actively supervised by an adult when using the Internet.

**Using the Internet for Learning**

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

Using the Internet is now a part of the Computing Curriculum (Sept 2014). We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary

**Teaching safe use of the Internet and ICT**

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Be Safe Online rules to support our teaching in this area:

These rules are:

1. I only go online with adult supervision
2. I am kind online
3. I keep information about me safe
4. I tell a grown up if something online makes me unhappy

**Suitable material**

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible we provide pupils with suggestions for suitable sites across the curriculum and staff will always check the suitability of websites before letting the children use them or using them in teaching.

**Unsuitable Material**

The school will take all reasonable precautions to ensure that users access only the appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. The action will include:

1. Making a note of the website and any other websites linked to it.

2. Informing the ICT technician
3. Reporting the incident to the school e-safety Leader (Faye Booth), or the Head Teacher, who will then record the incident – ICT Incident Log Book in the school office and escalate the concern as appropriate.
4. Any material that the school believes is illegal must be reported to appropriate agencies such as Kent Police, the IWF or CEOP.
5. If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the county e-Safety Officer or Area Children's Officer.

**Using email at school**

Email is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe that it is important that our pupils understand the role of email, and how to use it appropriately and effectively. Pupils will be taught that they must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult. Whole-class or group email addresses will be used in primary schools for communication outside of the school. Staff will only use official school provided email accounts to communicate with parents/carers, as approved by the Senior Leadership Team.

**Social Networking and social media**

The school will control access to social media and social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school e-Safety Policy Staff Agreement form.

**Internet-enabled mobile phones and personal devices**

The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school e-Safety Policy Staff Agreement form. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the Staff Code of Conduct policy.

School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer or member of staff. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation. Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

Staff will be issued with a school phone where contact with pupils or parents/carers is required.

**Cyberbullying- Online bullying and harassment**

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. There are clear procedures in place to support anyone in the school community affected by cyberbullying. All incidents of cyberbullying reported to the school will be recorded. There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

**Contact details and privacy**

Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.

Pupils are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet.

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published. The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate. The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

**How will complaints regarding e-safety be handled?**

Complaints of Internet misuse will be dealt with under the School's Complaints Procedure. Any complaint about staff misuse will be referred to the head teacher. Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures. All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

This policy has been written in conjunction with the Safeguarding policy, Anti- bullying policy, Child Protection policy, Teaching and Learning policy, Computing policy, Complaints policy, Staff Code of Conduct and the e-Safety Staff Agreement form.

**Use of the Internet and ICT resources by school staff**

**The Internet**
Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.
We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

**Internet Availability**
To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use. The school also provides a KLZ user account that gives further access to specific resources, online tools and email.

**ICT Equipment and Resources**
The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, video camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software.

**Professional use**
Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need support or INSET in using ICT as part of their professional practice can ask for support from the ICT Co-ordinator.

**Personal use of the Internet and ICT resources**
Some equipment (including laptops) is available for loan to staff, with permission from the Computing Leader and Headteacher. The appropriate forms and agreements must be signed.
However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use. These are outlined in the staff agreement form below.

**E-mail**
We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

**Online discussion groups, bulletin boards and forums, online chat and messaging**
We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

**Social Networking**
The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Code of Conduct policy expectations and agreements.

**Data Protection and Copyright**
The school has data protection policy in place – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning.

**e-Safety Contacts and References**

- **BECTA – www.becta.org.uk/safeguarding**

- **CEOP (Child Exploitation and Online Protection Centre) – www.ceop.police.uk**

- **CFE e-Safety Officer, KCC Children, Families & Education**

  **Rebecca Avery: esafetyofficer@kent.gov.uk**

  **Tel: 01622 221469**

- Child Exploitation & Online Protection Centre – www.ceop.gov.uk
- Childline – www.childline.org.uk
- Childnet – www.childnet.com
- Children's Officer for training & Development, Child Protection
  Mike O'Connell: mike.oconnell@kent.gov.uk
  Tel: 01622 696677
- Children's Safeguard Service – www.kenttrustweb.org.uk?safeguards
- Click Clever Click Safe Campaign – http://clickcleverclicksafe.direct.gov.uk
- Cybermentors – www.cybermentors.org.uk
- Digizen – www.digizen.org.uk
- EIS, ICT Support for Schools and ICT Security Advice – www.eiskent.co.uk?ictsecurity
- Internet Watch Foundation – www.iwf.org.uk
- Kent e-Safety in Schools Guidance – www.kenttrustweb.org.uk?esafety
- Kent Public Service Network(KSPN) – www.kspn.net
- Kent safeguarding Children Board (KSCB) – www.kscb.org.uk
- Kidsmart – www.kidsmart.org.uk
- Schools Broadband Team – Help with filtering and network security – www.eiskent.co.uk
  Tel: 01622 206040
- Schools e-Safety Blog – www.kenttrustweb.org.uk?esafetyblog
- Teach Today – http://en.teachtoday.eu
- Think U Know website – www.thinkuknow.co.uk
- Virtual Global Taskforce – Report Abuse – www.virtualglobaltaskforce.com
- Kent Police: In an emergency (a life is in danger or a crime in progress) dial 999. For non urgent enquires contact Kent Police via 01622 690690 or the Safer School's Partnership Officer. Also visit www.kent.police.uk/internetsafety

**Mereworth Community Primary School**
**Staff Acceptable Use Agreement Form**

**This document covers use of school digital technologies, networks etc. both in school and out of school.**

**Access**

• I will obtain the appropriate log on details and passwords from the ICT Co-ordinator.
• I will not reveal my password(s) to anyone other than the persons responsible for staff running and maintaining the system.
• If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
• I will not allow unauthorised individuals to access school ICT systems or resources

**Appropriate Use**

• I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
• I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
• I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network
• I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-Safety coordinator or member of the SLT.

**Professional Conduct**

• I will not engage in any online activity that may compromise my professional responsibilities
• I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role
• I will never include pupils or former pupils as part of a non-professional social network or group
• I will ensure that I represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion or posting to public websites using school facilities
• I will not browse, download or send material that could be considered offensive to colleagues
• I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact

**Personal Use**

• I understand that I may use Internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes.
• I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
• I understand that the forwarding of e-mail chain letters, inappropriate 'jokes' and similar material is forbidden.
• I will not use the school Internet facilities for personal access to public discussion groups or social networking sites

**Email**

• I will only use the approved, secure email system for any school business: (currently: KLZ email)

• I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

**Use of School equipment out of school**
• I agree and accept that any computer or laptop loaned to me by the school, is provided mainly to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
• I will return school equipment regularly (to be agreed with ICT Technician) to be checked and updated
• I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software

**Teaching and Learning**
• I will always actively supervise, or arrange for suitable supervision of pupils that I have directed or allowed to use the Internet
• I will embed the school's e-safety curriculum into my teaching, using agreed resources and materials
• I will ensure I am aware of digital safeguarding issues so they are appropriately embedded in my classroom practice
• I will only use the Internet for professional purposes when pupils are present in the classroom with Internet access

**Photographs and Video**
• I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission
• I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance)

**Data protection**
• I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students working at the school.
• I will not take pupil data, photographs or video from the school premises without the full permission of the head teacher e.g. on a laptop, memory stick or any other removable media
• I will ensure that I follow school data security protocols when using any confidential data at any location other than school premises
• I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission
• I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

**Copyright**
• I will not publish or distribute work that is protected by copyright

## User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I agree to have a school user account, be connected to the Internet via the school network and be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

School .....

**Authorised Signature ( Head teacher)**

I approve this user to be set-up.

Signature ..... Date.....

Full Name .....(printed)

# Staff Laptop and ICT Equipment Loans

Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this e-Safety Policy.

This must be the case wherever the laptop, computer or other such device is being used as it remains the property of Mereworth Community Primary School at all times.

Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense.

Staff must sign the 'Staff Laptop and Computer Loans Agreement before taking the equipment away.

## Staff Laptop and ICT Equipment Loan Agreement

**I have borrowed a school laptop to use out of school in agreement with the Head teacher and the computing leader.**

Make**:**_____

Model**:**_____

Serial number**:**_____

**It is understood that I will return the equipment to school if requested to do so by either the Head teacher or Computing Leader.**

I undertake to take proper care of the equipment whilst in my possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. I agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, I will replace or arrange for the repair of the equipment at my own expense.

I will use the equipment in accordance with the schools e-Safety Policy and Staff Acceptable Use policy.

**I agree to the above conditions:**

(Signature) _____

(Print name) _____ Date:_____

Returned: _____ Date:_____

# Mereworth Community Primary

# School e-Safety Incident Log

Details of all e-Safety incidents to be recorded by the e-Safety Co-ordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere.

| Date & time | Name of pupil or staff member | Male or Female | Room and computer/ device number | Details of incident (including evidence) | Actions and reasons |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

BECTA Flowchart for responding to e-safety incidents