E-Safety Policy

Mill Rythe Junior School
Approved by Governing Body
Date ratified: October 2019
Review date: October 2022

1. Introduction

At Mill Rythe Junior School we are committed to ensuring children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning in school
- Know how to use a range of ICT equipment safely in school
- Are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner
- Know what to do if they feel unsafe when it comes to using technology and ICT

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.

2. The Law

Our E-Safety Policy has been written by the school, using advice from HCC and government guidance. The Policy is part of the School Development Plan and related to other policies including Behaviour, Child Protection and GDPR policies.

3. Roles and Responsibilities

The Headteacher will:

- Ensure the policy is implemented, communicated and compliance with the policy Is monitored
- Appoint an e-safety co-ordinator
- Ensure staff training in e-safety is provided and updated annually as part of safeguarding training
- Ensure immediate action is always taken if any risks or dangers are identified ie reporting of inappropriate websites
- Ensure that all reported incidents of cyber bullying are properly investigated in accordance with the Behaviour Policy and recorded in the anti-bullying folder
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material

The computer lead will:

- Work in partnership with parents, the Local Authority and the Department for Education to ensure systems to protect pupils are continually reviewed and improved
- Keep up to date with relevant local and national guidance (including Ofsted guidance)
- Ensuring school practices and policies reflect these
- Moderate personal publishing sites used by pupils ie blogging, within the terms of this policy
- Publicise the Acceptable Use Agreement around the school. Ensure children are aware of and involved in developing the Acceptable Use Agreement
- Deliver staff e-safety training and act as e-safety champion, looking for opportunities to promote and ensure e-safety in all aspects of school life
- Support parents in promoting e-safety by providing relevant information and guidance
- Ensure e-safety forms part of the computer curriculum and is enhanced through whole school events, e.g. assemblies/guest speakers where appropriate
- Ensure E-safety forms a part of the school computing action plan

The Admin Officer will:

- Correctly maintain the school's Data protection Registration with the Information Commissioner

Teachers and Staff will:

- Adhere to this policy
- Keep passwords private and use their own login details
- Monitor and supervise pupils' internet usage and use of other IT resources
- Always adhere to the Acceptable Use Agreement
- Always adhere to the Child Protection Policy
- Promote e-safety and teach e-safety units as part of computing curriculum
- Engage in annual e-safety training, implementing key messages
- Only download attachments/material onto the school system if they are from a trusted source
- Only use school cameras or recording devices when capturing images, videos or sound clips of children
- Never communicate with pupils or parents via social networking sites
- Delete images and video of children from the school system within 12 months of them leaving

Governors will:

- Ensure that the school is implementing this policy effectively
- Adhere to the acceptable use agreement when in school
- Have due regard for the importance of e-safety in school

4. Teaching and Learning

The school will actively teach E-safety at an age-appropriate level through the curriculum (particularly as part of the computing and PSHE curriculum) as well as through whole school events such as assemblies and e-safety awareness days.

Each year group will cover at least one unit in ICT lessons dedicated to E-safety. E- safety will also be embedded throughout other Computing units and whenever children are using ICT in other lessons.

Units of work follow national curriculum requirements and cover themes such as: safe use of the internet, protecting yourself online, safe use of social media, becoming a critical consumer of internet material, handling and protecting yourself from cyber-bullying and rules surrounding copyright.

5. **Monitoring safe and secure systems**
The school maintains two networks – one for administrative and one for curriculum purposes – both maintained by Agile IT, the school's IT provider.

How will the security of these systems be maintained?

- Internet access is regulated by HCC supplied filtered broadband connection which blocks access to unsuitable websites
- Antivirus software has been installed on all computers and is to be maintained and updated at all times by the system administrators
- Staff passwords should be changed regularly and at intervals of not less than once per term
- Staff are to adequately safeguard confidential data saved to laptops, ie use of passwords. If personal data has to be saved to other media, eg data sticks, it is to be encrypted or password protected. Staff should only use school memory sticks to store school-related information
- Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times. As a rule of thumb, where data is displayed on screen, the room should be occupied by a member of staff. Terminals are set to automatically lock out when activity ceases
- Portable media, ie memory sticks, may not be used by children without specific permission followed by a virus check
- Unapproved software should not be put onto the school system/computers
- Teaching staff have remote access to the school server. This reduces the need for portable data storage and therefore increases security. Remote access is fully password protected. Staff are reminded to continue to abide by this policy and acceptable use agreement when accessing the school server remotely. Staff are also reminded to log out of remote access when they have finished using it.

6. **Safe use of the Internet and Web Filtering**

- All staff and pupils will have access to the internet through the school's network
- All staff, volunteers who have use of the school's IT equipment, must read and sign the Staff and Volunteer Acceptable Use Agreement annually
- All children must read and sign the Pupil Acceptable Use Agreement (parents are also sent a copy)
- Web filtering is carried out centrally by Hampshire County Council
- If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher to pass to EdICT for central booking. Children can also use 'Hector the Dolphin' software to immediately block their screen and report any sites causing concern
- If an adult finds a site that they consider unsuitable they should report it to the Headteacher
- It is important for staff and parents to realise that web filtering from HCC works on a categorisation system and is not able to filter out individual offensive words, which may result in offensive words appearing in the titles of some search results. It is incumbent upon us to ensure that we work carefully to help children search safely online

7. **The use of Email**

Staff Use of Email

- All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails
- As with any other form of communication, all emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary
- Attachments should only be downloaded where the member of staff knows and trusts the sender
- Staff emails should never be used to forward 'chain' or 'junk' email
- Staff should not communicate with pupils via email

Pupils' Use of Email (at the time of writing the policy, children do not have email addresses for use in school)

- In school, pupils may only use approved email accounts on the school system
- Pupils must immediately tell a teacher if they receive an offensive email
- Whole class or group email addressed set up by the computing lead will be used for communication outside the school. This will be used by teachers only, or teaching assistants with class teacher approval
- The forwarding of chain or spam messages is not permitted

8. **Publishing of pupil's images or work ie on the school website or Instagram**

- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line

- Pupils names will not be used in conjunction with any images or video

- Pupils' work can be published without their permission

9. **Social Networking, Social Media and Personal Publishing (blogging)**

- The filtered broadband system will not allow access to public or unregulated chat rooms. However, the school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the computing curriculum
- Pupils will not access social networking sites, eg Facebook or Twitter in school
- Pupils will be taught about how to stay safe when using such sites at home

10.**The Use of Cameras, Video and Audio Recording Equipment**

- Children and staff should never bring their own cameras or mobile phones into school for use unless given specific permission to do so by the Headteacher. Children must never take a phone into a classroom or playground except when specifically arranged for the purposes of learning
- It is never acceptable to use photographic or video devices in changing rooms or toilets
- Staff may use photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the school system. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher, nor circulate them in electronic form outside the school
- Parents are able to take photos/videos of their own children at school events with the clear understanding that they will not upload images of other children to social media or the internet.

11.**Protecting Personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- The school's Data Protection Policy must be adhered to

12.**Protecting Children from Cyber-Bullying**

- The school takes any incidents of cyber-bullying extremely seriously and, as with any other form of bullying, cyber-bullying will not be tolerated
- Any reported incidents of cyber-bullying will be dealt with in line with the school's anti-bullying policy
- The Headteacher is to be informed of any incidents of cyber-bullying reported to the school, and will record them. A designated safeguarding lead will liaise with the parents of children involved in any such incident
- Detailed records of incidents and follow up actions and monitoring will be recorded
- Support will be put in place for both the child targeting through cyber-bullying and the child responsible
- Sanctions for those involved in cyber-bullying may include asking the bully to remove any material deemed to be inappropriate or offensive or contacting the service provider to remove content. The Police will be contacted if a criminal offence is suspected
- Cyber-bullying will be addressed through the school curriculum and through the school's anti-bullying work

13.**Working in Partnership with Parents**

- Parents' attention will be drawn to the e-safety policy through the school newsletters, brochure and on the website. Regular e-safety guidance to support parents in keeping their children safe online is shared through the school newsletter
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home internet use, or highlighting e-safety at other attended events
- Parents will be requested to sign an Acceptable Use Agreement as part of the Home School Agreement

14.**Protecting School Staff**

In order to protect school staff we require that parents do not comment on school staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school has a separate complaint policy if parents wish to use this. This is reflected in our home school agreement and parents are reminded regularly through the weekly newsletter.

The school will take action if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

Appendix 1: Pupil Acceptable Use Agreement

Appendix 1: Pupil Acceptable Use agreement

Mill Rythe Junior School

ICT Pupil Acceptable Use Agreement and E-Safety Rules

- ✓ I will log on using my own username and password.
- ✓ If I find anything or anyone online that makes me feel uncomfortable, unsafe or uneasy in any way, I will **tell an adult** immediately.
- ✓ I will make sure that all online contact with other children and adults is **responsible, polite** and **sensible**.
- ✓ I will only upload or add images, video, sounds or text that are **appropriate, kind** and **truthful** and will not possibly upset someone.
- ✓ I will keep my personal details such as name, phone number or address **private** when I'm online.
- ✓ I know that my behaviour online can be checked and my parent/ carer contacted if a member of school staff is concerned.
- ✓ I will be responsible for the way I behave online, because I know that these rules are to keep me safe.

Think before you click!