Eastlands Primary School

Online-Safety Policy

Date	Review Date	Nominated Person	Nominated Governor
June 2019	**June 2021**	**Liz Vikmanis**	**Ian Bates**
	(annual/biannual/ triennial)	**Website publication Yes /No**	**Committee FGB**
Appendix 1 – Acceptable Use policy for pupil Appendix 2 – Acceptable Use Policy for Staff		Linked documents Use of social networking sites for staff and governors	

Introduction

Information and Communications Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the every day lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to provide our children with the skills to access life-long learning and employment.
ICT covers a wide range of resources including, but not limited to; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Eastlands Primary School we understand the responsibility to educate our pupils in Online -Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, iPods, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc).

Roles and Responsibilities

As Online -Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online -Safety coordinator in our school is Liz Vikmanis. All members of the school community have been made aware of who holds this post. It is the role of the Online-Safety coordinator to keep abreast of current issues and guidance through organisations such Warwickshire LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The Head/Online-Safety coordinator updates Senior Management and Governors; all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and reviewing the Online -Safety policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for ICT, Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying.
Our Online -Safety policy has been written by the school, in conjunction with advice from Warwickshire County Council and government guidance. It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The Online-Safety policy and its implementation will be reviewed annually.

Online -Safety skills development for staff

- Our staff receive regular information and training on Online-Safety issues through the coordinator/Headteacher at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate Online-Safety activities and awareness within their lessons.

Online-Safety information for parents/carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school website contains useful information and links to sites like Thinkuknow, Childline, CEOP and the CBBC Web Stay safe page.
- The school will send out relevant Online-Safety information through newsletters and the school website.

Community use of the Internet

- External organisations using the school's ICT facilities must adhere to the Online-Safety policy.

2. **Teaching and Learning**

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach Online-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Managing Internet Access

Information system security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Warwickshire County Council.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.
- Pupils' full names will not be used on the Eastlands School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

On the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites e.g. School performances and assemblies etc. Parents/ carers will be asked to not share photos on social media.

Social networking and personal publishing

- The school will block / filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.

- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children as 'friends' if they use these sites.

Managing filtering

- The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and continually improved.
- If pupils or staff discovers an unsuitable site, it must be reported to the Class Teacher, Online-Safety Coordinator or Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school will be sent to the school office and kept there until the end of the day.
- The sending of abusive or inappropriate text messages outside school is forbidden.
- Staff will use a school phone where contact with pupils is required.
- Staff should not use personal mobile phones during designated teaching sessions.

Protecting personal data

The school will collect personal information fairly and will advise how the school and Warwickshire LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or Warwickshire LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and Warwickshire LA.

The school will hold personal information on its systems for as long as you or your family members remain a member of the school community and remove it in the event of your leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Warwickshire County Council and as defined by the GDPR guidance

You have the right to view the personal information that the school holds about you or your family members, and to have any inaccuracies corrected.

4. Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's Online-Safety rules. These Online-Safety rules will also be displayed clearly in all networked rooms.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's Online-Safety rules and within the constraints detailed in the school's Online-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security

- Adult users are provided with an individual network and email login, username and password, which they are encouraged to change periodically.
- All pupils are provided with an individual network and email login, username and password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Children are reminded that they should not go onto any games above their age without permission e.g Roblox
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, systems.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the Online-Safety policy is adequate and that its implementation is effective.

Handling Online-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the Online-Safety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online-Safety coordinator and recorded in the Online-Safety incident logbook.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

5. Communications Policy

Introducing the Online-Safety policy to pupils

- Online-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/circle times/anti-bullying week/internet safety day.
- Pupils will be informed that network and Internet use will be monitored**.**

Staff and the Online-Safety policy

- All staff will be given the School Online-Safety policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user; discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

7. Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Online-Safety Coordinator.

This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the Online-Safety Coordinator, ICT Coordinator, Designated Child Protection Coordinator, and Governor with responsibility for ICT and Child Protection. Ongoing incidents will be reported to the full governing body.

Appendix 1

	NAME OF SCHOOL	**EASTLANDS PRIMARY SCHOOL**
	ACCEPTABLE USE POLICY (AUP) PUPIL AGREEMENT FORM	

Please complete and return this form to the school.

Pupil's Name		**Class Teacher**	
As a school user of the Internet, I agree to follow the school rules on its' use. I will use the network in a responsible way and observe all the restrictions explained to me by my school.			
Pupil Name (print)			
Pupil Signature		**Date**	SEPTEMBER 201_

Parents Name			
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email, Learning Platform. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.			
Parents Name (print)			
Parents Signature		**Date**	SEPTEMBER 201_

PUPIL GUIDELINES FOR SAFE INTERNET/EMAIL USE

- I will only use the Internet when there is a teacher present.
- I will always ask for permission before accessing the Internet/Email.
- I will only use my own usernames and passwords to log on to the system/email and keep them secret.
- I will not access other people's files.
- I will only email people I know, or my teacher has approved and ensure that the messages that I send will be polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using the Email.
- I will not give personal details (like my home address, telephone or mobile number), or the personal details of any other person to anyone, or arrange to meet someone unless my parent/carer or teacher has given me permission.
- I will only download, use or upload material when I have been given the owner's permission.
- I will only view, download, store or upload material that is lawful, and appropriate for other users. If I am not sure about this, or come across any potentially offensive materials, I will inform my class teacher straight away.
- I will avoid any acts of vandalism. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.
- Always quote the source of any information gained from the Internet i.e. the web address, in the documents you produce.
- Use the Internet for research and school purposes only.
- I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.

- I understand that the school may check my computer files/Emails and will monitor the Internet sites that I visit.
- I understand that if I don't follow these rules, my access to the school computer system/Internet/Email may be suspended, and my parents/carers will be informed.

Name of School	**EASTLANDS PRIMARY SCHOOL**
AUP review Date	**SEPTEMBER 201_**
Date of next Review	**SEPTEMBER 201_**

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- 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 not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (Which is currently: We-Learn)
- 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.
- 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.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- 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, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- 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 ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- 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.
- I will embed the school's Online-Safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

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

I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; 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: September 201_

Full Name: Mrs S Edwards