



Online and E-Safety Policy

DATE APPROVED BY LDBS ACADEMIES TRUST	September 2016		
REVIEW DATE Annual	September 2017		
SIGNED HEADTEACHER	<i>Jane Mutch</i>	DATE	1/11/16
SIGNED CHAIR OF GOVERNING BODY	<i>L. James</i>	DATE	1/11/16

Designated Safeguarding Lead	Jane Mutch
Deputy Designated Safeguarding Lead	Jacqui Curthoys
Police Contact Name and Number	020 8246 1901
LA Contact Name and Number	Lisa Tingle 020 8825 8155

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school's e-safety policy will operate in conjunction with other policies including those for Behaviour and Anti-Bullying, Data Protection and Child Protection and Safeguarding.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network use.
- Safe and secure broadband ultimately from the London Grid for Learning including the effective management of content filtering.

E-Safety Audit – Primary Schools

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Does the school e-Safety Policy consider CP and Prevent guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both pupils and staff?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules	Y/N
Have school e-Safety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	Y/N
Has the school filtering policy has been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

Contents

School e-Safety Policy.....	4
Why is Internet use important?.....	4
How does Internet use benefit education?	4
How can Internet use enhance learning?	4
Authorised Internet Access.....	5
World Wide Web	5
Email.....	5
Social Networking	5
Filtering.....	5
Managing Emerging Technologies.....	6
Published Content and the School Web Site.....	6
Publishing Pupils' Images and Work	6
Information System Security	6
Protecting Personal Data	6
Assessing Risks.....	7
Handling e-safety Complaints.....	7
Communication of Policy.....	7
Pupils.....	7
Staff.....	7
Parents.....	7
Flowchart for responding to internet safety incidents - Appendix A -	8
E-Safety Rules - Appendix B	9
Staff Acceptable Use Policy – Appendix C	11

School e-Safety Policy

The role of e-Safety coordinator will fall to the Designated Safeguarding Lead as the roles overlap. Our e-Safety Policy has been written by the school, building on government guidance and with the assistance of our ICT support. It has been agreed and approved by governors.

The e-Safety Policy will be reviewed annually.

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential part of 21st century life for education, business and social interaction.

Access to the Internet is therefore an for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority, EFA and DFE;
- access to learning wherever and whenever convenient

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support planned learning outcomes.

- Pupils will be tutored in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will learn about E-Safety across the computing curriculum, and how to make best and safest use of modern technology.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who have been given Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the e-safety coordinator.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- 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.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations 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.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security

Filtering

The school will work in partnership with the Internet Service Provider to ensure filtering systems are as effective as possible.

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.
- Staff should not use mobile phones to take pictures or videos of children. Staff should only use digital cameras or iPads that have been provided by the school.
- Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school.
- Mobile phones may only be used in office areas, staffroom etc. The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.

The Prevent Duty and E-Safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the Internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our curriculum. Our staff have undertaken Prevent training and are aware of the risks posed by online activity of extremists. They have a duty to take action if they believe the well being of any pupil is being compromised.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- 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 anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained on the pupil registration form before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security is reviewed regularly.
- Virus protection is installed and updated regularly.
- Security strategies will be discussed with the ICT provider.

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

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor our ICT provider can accept liability for the material accessed, or any consequences of Internet access.
- 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.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by the headteacher
- 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.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all classrooms.
- (Older) Pupils will be informed that Internet use will be monitored.

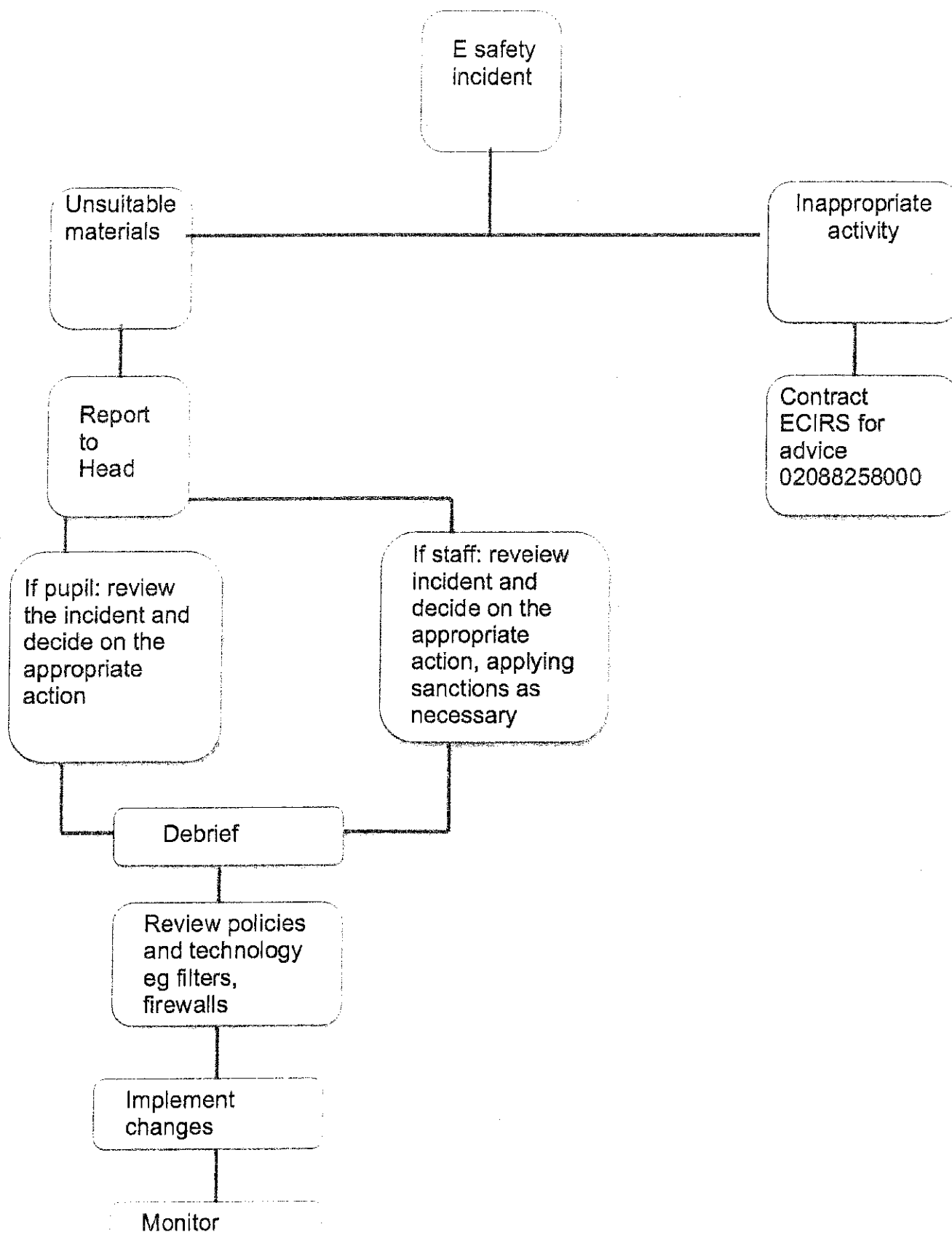
Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff will be trained in Safeguarding procedures, including elements of eSafety and The Prevent Duty.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents are told about our approach to e-safety as part of induction procedures

Appendix A - Flowchart for responding to e-safety incidents in school



Appendix B

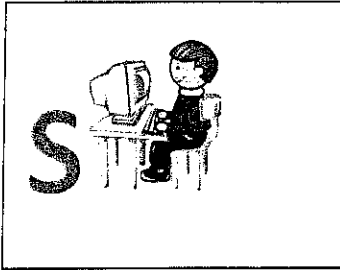
Guidelines for Safer Use of ICT in KS1

Learning to use ICT is an essential part of the school curriculum and one that children need to prepare them for life. Learning can be enhanced in many different ways through the use of ICT and developing technologies. Nevertheless this is an area that can pose particular risks and so it is very important to have clear guidelines for safer use of ICT.

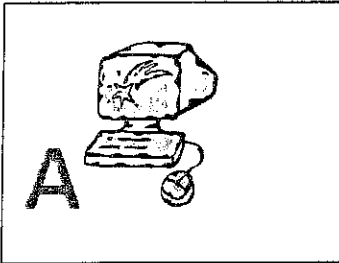
- All staff are expected to follow the school rules, based on advice from the London Grid for Learning, regarding their own use of school ICT equipment. Before being issued with ICT equipment, passwords or email accounts all staff are asked to sign an agreement (see above)
- Before children use the internet at school they will have some of the risks explained to them, in an age-appropriate way, and be asked to follow some simple rules (see below).

Parents are told about our approach to e-safety as part of induction procedures

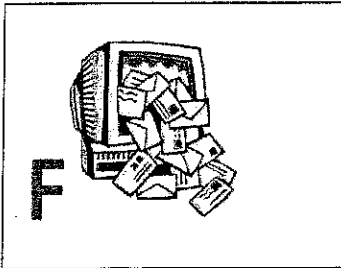
Think before you click



I will only use the Internet with an adult's permission.



I will only click on icons and links when I know they are safe.



I will only send friendly and polite messages.



If I see something I don't like on a screen, I will always tell an adult.

My Name:

My Signature:

Appendix C - Staff Use of ICT

This agreement 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 teacher and Governing Body.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised users to access email, internet, intranet, network or other school 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.
- I will only use the approved school email, school MLE 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 only use school digital cameras or iPads for taking and transferring images of pupils or staff with permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school advice.
- 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 e-safety curriculum into my teaching.
- 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 e-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

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature Date

Full Name (printed)