E-Safety Policy

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 Pupil Behaviour, Child Protection, Safeguarding, Bullying, Curriculum, Data Protection and Security.

Good Habits

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

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through rules and procedures.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school access and use.
- Safe and secure access from the Essex Grid for Learning including the effective management of content filtering.

We have an e-Safety coordinator. In our case this will be the ICT Subject Leader supported by the IT technician and the Designated Safeguarding Person.

Our e-Safety Policy has been written by the school, building on the Essex Guidance.

The e-Safety Policy will be reviewed every two years. This policy will next be reviewed November 2016.

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 element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement 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 can Internet Use Enhance Learning?

- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- 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.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted 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.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or ICT Subject Leader.
- 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 only have access to e mail through the school learning platform.
- Children are not to use personal e mail accounts in school

Filtering

- The school will work in partnership with the Local Authority, Becta and 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.

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 and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- See Staff Code of Conduct for additional guidance on Staff Social Networking

Mobile Phones

- Pupils' mobile phones are not allowed in school, but can be left at the Office during the day.
- Adults are permitted to keep their mobile phones in their bags or about their person; however there is a clear expectation that all personal use is limited to allocated lunch and/or tea breaks in the staffroom or office areas.
- Mobile phones must not in any circumstances be taken into changing rooms or children's toilets.
- Other than in agreed exceptional circumstances, phones must be switched off and calls and texts must not be taken or made during work time.
- Adults are not permitted, in any circumstance to use their phones for taking, recording or sharing images.

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 will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images

- On entry to school and then annually, parents will be asked to give consent to children's photographs being taken within school and during school events. The consent will allow photographs to be displayed in the school environment.
- Parents will be asked to give consent for children's photographs to be published on the school Website or other published material such as newspaper reports and the school prospectus.

- Pupils' full names will not be used anywhere on the Website or Blog, particularly in association with photographs.

Information System Security

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

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 Essex LA can accept liability for the material accessed, or any consequences of Internet access.
- The school should 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

- SMART Rules for Internet access will be posted in all classrooms.
- Pupils will be made aware of the e-safety rules as appropriate to their age and stage of development.
- 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.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

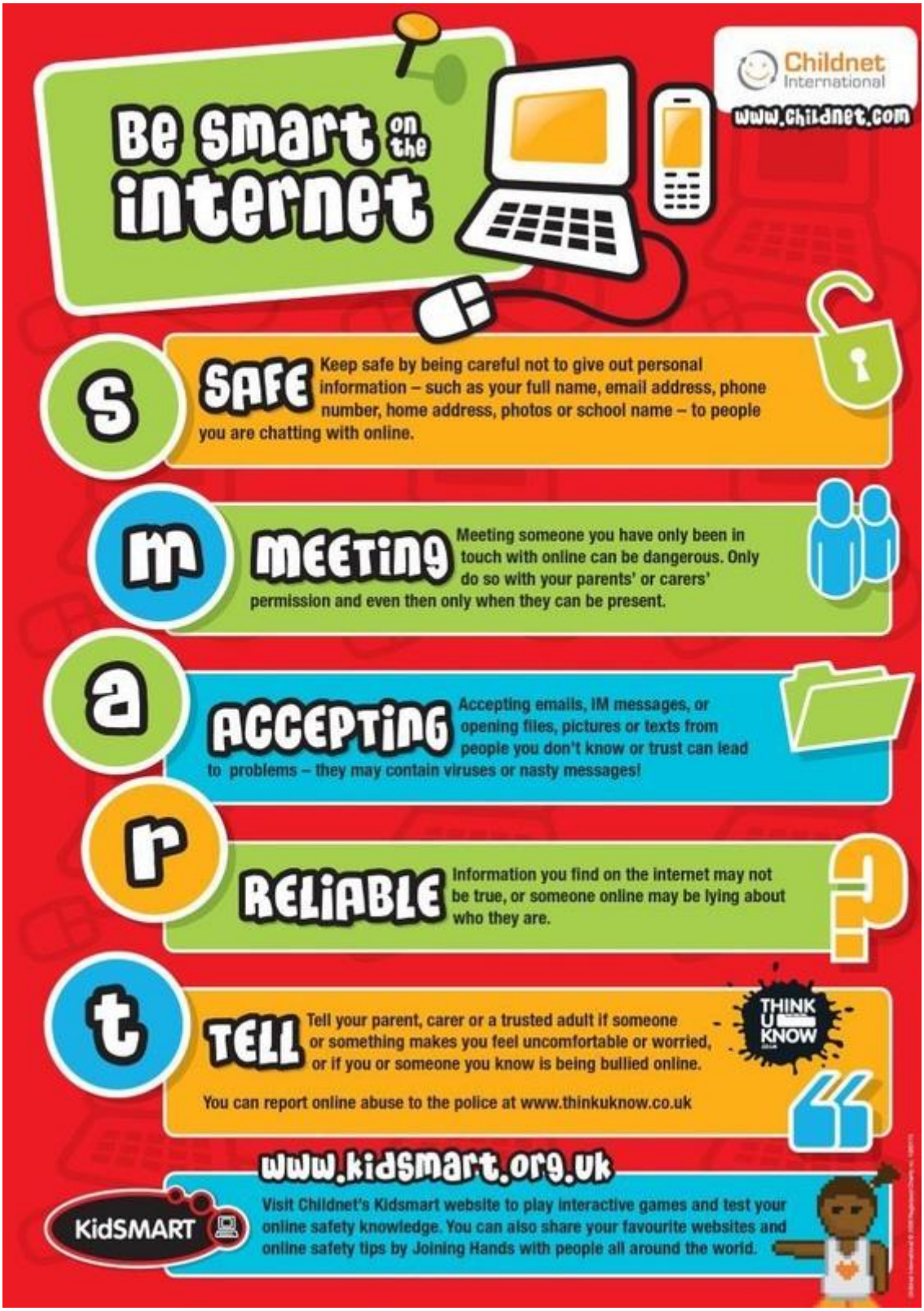
Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, e-folio and on the school Website.

e-Safety Code of Conduct for Children

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will only use ICT in school for school purposes.
- I will use only my login and I will keep any passwords secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only use my school email address in school.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell an adult immediately.
- I will not deliberately look for, save or send anything that could be considered unpleasant or nasty.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers and my parent may be contacted.


Childnet International
www.childnet.com
Be Smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
M
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
A
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
R
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
T
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
THINK U KNOW
You can report online abuse to the police at www.thinkuknow.co.uk
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Birchanger C of E (VC) Primary School
Birchwood, Birchanger
Nr. Bishops Stortford
Hertfordshire
CM23 5QL

Tel: 01279 812362
Fax: 01279 817061
E-mail: admin@birchanger.essex.sch.uk
Headteacher: Mrs. Helen Coop

Dear Parents

Acceptable Use of ICT in school

ICT, including the internet, e-mail and mobile technologies, has become an important part of learning in our school. We expect all children to be safe and responsible when using ICT and have adopted the attached SMART rules as a summary of our e-Safety Code of Conduct for Children.

Please read and discuss these rules with your child and return the slip at the bottom of the page to confirm this.

This acceptable use agreement is a summary of our e-safety policy which is available in full on our website or as a paper copy on request.

Yours faithfully

Mrs H L Coop — Headteacher
Miss S West — ICT Subject Leader

Childs name _____
We have discussed the SMART rules and _____ agrees to follow the e-safety rules and to support safe use of ICT at school.

Signed _____ parent/carer Date _____

Staff Information Systems Code of Conduct

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

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate senior leader.
- I will not install any software or hardware without seeking advice or permission.
- I will ensure that personal data is kept secure 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 school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role and comply with the school staff code of conduct.
- I understand adults should not, in any circumstance contact pupils using personal email or using social networking sites.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of 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 agree with the Information Systems Code of Conduct.

Signed: …… Print Name: …… Date: ……

e-Safety Audit for _____School

When discussing and planning e-Safety there are a number of key aspects to consider. This simple audit can help Governors, Headteachers and SLT to identify progress and plan the next steps. The audit can be personalised to meet individual school needs and ideally will be reviewed yearly.

Does the school have an e-Safety policy for Pupils? Staff? Other users of the school facilities?	Y or N
The e-Safety policies were last reviewed Date	
The e-Safety policies have been agreed by the Governors Date	Y or N
The e-Safety coordinator is ……..	
The Designated Senior Person DSP for Child Protection is ……..	
The e-Safety policies have been discussed with Date Staff Pupils Parents/ carers Other users of the school facilities All members of the school community have a copy of the e-Safety policy or know where to find one. The following are expected to sign an e-Safety Acceptable Use policy Staff Pupils Parents/ carers Other users of the school facilities	 Y or N Y or N Y or N Y or N Y or N
eSafety rules are discussed regularly and displayed throughout the school.	Y or N
All staff consistently apply the e-Safety policies and rules.	Y or N
Clear and appropriate sanctions are applied if any member of the school community does not follow the AUP	Y or N
All users are aware that the schools ICT systems are regularly monitored and any misuse will be followed up.	Y or N
The school takes a lead in educating pupils, parents/ carers and staff about e-Safety whilst celebrating the positives offered by ICT	Y or N

Completed by …….. Date ……