South Benfleet Primary School (Academy Trust)

A Policy Statement for E-Safety and Acceptable Use

Policy

E-Safety and Acceptable Use

Acknowledgement:

We acknowledge and thank Essex Local Authority for their help in producing this model policy.

The Acceptable Use Policy Agreement should be issued to the appropriate user for signature and collated by a designated member of staff.

Schools should ensure that all persons, including Governors and pupils, who join the establishment mid year are provided with the policy and agreement.

Mission Statement

The dedicated team at South Benfleet Primary School aims to provide a happy, caring, community of learners where all are welcomed and valued and where learning is fun, real, relevant and memorable.

We strive to ensure that our children acquire responsibility, tolerance and understanding and develop respect for themselves, each other, their families, our local community and the environment.

We want our pupils to be co operative and have high self esteem and develop the motivation, knowledge and skills to prepare them for the world of tomorrow

School aims:

We will aim make learning ‘Fun, real, relevant and memorable’ by:

- Children becoming motivated and enthusiastic self-learners who enjoy coming to school
- Children experiencing a wide but balanced range of learning activities
- Children being confident readers, writers and mathematicians
- Children making good progress and have high levels of achievement
- Children learning the key skills of communication, cooperation, team work, understanding, tolerance and confidence
- Children being able to learn through creative first hand experiences and having high quality visits and visitors to inspire learning
- Children being ready for the next stage of their learning journey

Racial Equality and Equal Opportunities

All children have equal access and inclusive rights to the curriculum and Religious Education regardless of their gender, race, disability or ability. We plan work that is differentiated for the performance of all groups and individuals. South Benfleet Primary School is committed to creating positive climate that will enable everyone to work free from racial intimidation and harassment and to achieve their full potential.

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; 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
- E-mail 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 ***South Benfleet Primay School*** we understand the responsibility to educate our pupils on E-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities.   Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, E-mails, instant messaging, Internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the E-mail or voicE-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the Essex County Council Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Senior Information Risk Owner (SIRO) or E-safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the SIRO.

Acceptable Use Policies

The following AUP agreements are to be given to pupils and staff, governors, visitors, etc at the start of each academic year.

In the case of pupils, it is the responsibility of the parent/carer to read through the agreement with their child, explain the content and sign and return the reply slip.

Employees of SBPS must also sign to acknowledge compliance with the school's AUP.

South Benfleet Primary School
Acceptable Use Agreement - Pupils

Our E-Safety Rules

Our school has lots of computers and Chromebooks with Internet access to help us in our learning. These rules will help to keep us safe and help us to be fair to others.

Using the computers

I will only use the login(s) I have been given.

I will not use discs or memory sticks from home on school computers without asking for permission first.

I will only open E-mail attachments from people I know, or who my teacher has approved.

Using the Internet

I will ask for permission from a teacher before using the Internet/Chromebook.

I will report anything unpleasant or worrying I may see straight away to my teacher. This helps to keep me and others safe.

I will not give my full name, home address or telephone number when completing forms on the Internet.

I will only open E-mail attachments from people I know, or who my teacher has approved.

Using E-mail

I will always ask for permission before using/sending E-mail at school.

I will not let anyone know my E-mail or home-learning passwords (MyMaths, Active Learn, etc).

I will send polite and responsible messages.

I will only send messages to people my teacher has asked for or approved.

I will not give my full name, home address or telephone number when using E-mail.

I will only open E-mail attachments from people I know, or who my teacher has approved.

I will never use E-mail to arrange to meet someone outside school hours.

I will report any unpleasant messages sent to me to my teacher, as this helps to protect me and others.

Using other ICT equipment (cameras, sound recorders, etc)

I will always ask permission before using any other computing equipment.

I will always use computing equipment sensibly and carefully.

I am NOT allowed to:

Send or display on screen unpleasant messages or pictures.

Use bad language.

Use other people’s passwords.

Go into other people’s work, folders or files.

Move or delete other people’s work, folders or files.

Mobile Phone use

I am not allowed to bring in or use mobile phones at school.

Year 5/6 children: My parents must ask for special permission if I need to bring a phone to school. This will be turned off and kept at the school office during school hours. The school does not accept responsibility for the loss of mobile phones brought into school.

Outside School
Many of these rules can be used at home, at a friend's house or anywhere where you may be using a computer or the Internet.

- **Remember our SMART rules:**

  Safe – keep safe by never giving out personal information (full name, home address, phone number, school name or photos) to people you meet online
  Meet – never meet in real-life someone you met online
  Accept – never accept emails from people or organisations you don't know.
  Reliable – check the information you find online is reliable
  Tell – tell an adult if something online or on your mobile phone makes you feel upset or uncomfortable.

For further information and advice about keeping your children safe online:

To report abuse or offensive material online:
Child Exploitation and Online protection Centre
www.ceop.gov.uk/
The Internet Watch Foundation
www.iwf.org.uk/

Childnet International:
www.childnet-int.org/

E-safety Activities for children:
www.kidsmart.org.uk/
www.thinkuknow.co.uk/

Dear Parent/ Carer

ICT including the Internet, E-mail and mobile technologies, etc has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs L.Tanner, ICT Subject Leader.

This Acceptable Use Agreement is a summary of our E-safety Policy which is available in full on request.

✂

Parent/ carer signature

We have discussed this and ……………………………………........(child name) agrees to follow the E-safety Rules and to support the safe use of ICT at South Benfleet Primary School.

Parent/ Carer Signature …….…………………..…………………………….

Class ………………………………… Date ………………………………

South Benfleet Primary School

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as E-mail, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher, and/or the school's E-safety Coordinator.

- I have read and understand the **Additional ICT Policy Inclusions**
- I will not give out my own personal details, such as mobile phone number, personal E-mail address and social networking identities to pupils.
- I will only use the approved, secure E-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the head teacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

This Acceptable Use Agreement is a summary of our E-safety Policy and Social Networking Policy, both of which are available on request.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT within the school and socially outside of school.

Signature ………………………………… Date ……………………

Full Name ……………………………….. (printed)

Job title . . . .

Additional ICT policy inclusions

Acceptable Use Policy Statement

The computer system (and additional resources such as laptops and Chromebooks) is owned by the school, and may be used by children to further their education and by staff to enhance their professional activities including teaching, research, administration and management.

The school recognises that technologies such as the Internet and E-mail has a profound effect on children's education and staff professional development and the school's Internet Access Policy has been drawn up accordingly.

The installation of software or hardware unauthorised by the school, whether legitimately licensed or not is expressly forbidden.

The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.

Internet Access Policy Statement

Providing access to Internet in school will raise educational standards and support the professional work of staff.

We use a filtered Internet Service Provider (RM) which reduces (not prevents!) children from accessing inappropriate websites and using or receiving banned words in emails. Staff need to maintain a cautious approach when allowing children to search the Internet.

- All Internet activity should be appropriate to staff professional activities or the children's education.

- Children using the Internet (including Chromebooks) will be supervised by an adult (usually the class teacher or LSA) at all times.

- Staff will check that websites pre-selected for pupil use are age and maturity appropriate.

- Pupils will be taught how to use Internet and email responsibly to reduce the risk to themselves and others.

- Pupils read and parents sign **Acceptable Use Agreement** which are displayed in the computing suite.

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person.

● The Internet and E-mail may only be accessed via the school's network between the hours of 0800 and 1800 on weekdays, and at no other time without express permission from the Headteacher in liaison with the Computing coordinator.

● Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited.

● Users are responsible for all E-mail sent and for contacts made that may result in E-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media.

● Use for personal financial gain, political purposes or advertising is excluded.

● Copyright of materials and intellectual property rights must be respected.

● Posting anonymous messages and forwarding chain letters is excluded.

● The use of the Internet, E-mail, or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden. Deliberate activity of this nature will be dealt with by the Head Teacher.

● Staff are respectfully reminded to be fully aware of their own actions on the Internet as all published information is available to everyone with a web connection.

Areas for particular concern:
Personal accounts on social networking sites (e.g., Facebook, Twitter and similar);
Staff must be mindful of revealing personal information, images, etc that could be used against their professional position or the school. Staff are advised that posting information, data, photos, etc, or discussing issues online relating to the school or the school community could lead to disciplinary action. (See Social Networking policy).

● All staff are *strongly encouraged* not to accept parents, pupils or ex-pupils as friends on social networking sites.

● If there is an incident in which a child is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels. Responsibility for handling such incidents will be taken by the Head Teacher. All staff will be made aware of the incident. Our first priority will be to give the child appropriate support.

● All teaching staff are to attend annual E-safety training and receive regular updates. The computing coordinator will attend regular CEOP accredited E-safety training.

● If the incident is accidental, the URL address and content will be reported to the Internet service provider and the LEA. Material thought to be illegal will be reported to the appropriate agency after consultation with the ISP and LEA.

● Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools, advice from the LEA, our technician, our Internet service provider and the DfES.

Internet Publishing and email Statement

The school wishes the school's web site to reflect the diversity of activities, individuals and education that can be found at South Benfleet Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles should be borne in mind:

- No video recording or photographs may be made or published without the written consent of the parents/legal guardian of the child concerned, and the child's own verbal consent.

- Surnames of children **must not** be published, especially in conjunction with photographic or video material. Staff should be very wary about using children's names and never identify children by name and class e.g. Martin, Emily in Scarlet class etc.

- No link should be made between an individual and any home address (including simply street names).

- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. **If in doubt, refer to the person responsible for child protection.**

- No material may be published on the school web site without approval of the Headteacher.

Data Protection Act

Any individual has the right in law to view information held about him or her on a computer system. Care should be taken about any sensitive information concerning child protection issues etc. If a report is composed and printed on the system, it should immediately be deleted and hard copies kept in the appropriate files in the care of the Child Protection Officer. Please refer to the Data Protection Policy for further information.

Computer Viruses

- All files downloaded from the Internet, received via E-mail or on removable media (e.g. floppy disk, CD) must be checked for any viruses using school provided anti-virus software before using them

- Never interfere with any anti-virus software installed on school ICT equipment that you use

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The school follows Becta guidelines Becta Schools - Leadership and management - Security - Data handling security guidance for schools (published Spring 2009) and the Local Authority guidance documents listed below

The safe use of new technologies - Ofsted
http://www.e-gfl.org/e-gfl/custom/files_uploaded/uploaded_resources/5723/safe_use_of_new_technologies_ofsted.pdf

Teachers and Governors Guidance
http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/HR/Workload_Agreement/Guidance_Docs/dfes-InformationManagementSkillsforSuccess.pdf

Internet filtering for Essex Schools
http://www.e-gfl.org/index.cfm?s=1&m=283&p=31,view_item&start=1&id=4816

E-safety Audit Tool - Information for Governors, Management and Teachers
http://www.nen.gov.uk/hot_topic

Security

- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed off through an authorised agency only. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
Data Protection Act 1998
http://www.ico.gov.uk/what_we_cover/data_protection.aspx
Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal included within the Asset Inventory.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website
http://www.ico.gov.uk/

Data Protection Act – data protection guide, including the 8 principles
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

E-Mail

The use of E-mail within most schools is an essential means of communication for both staff and pupils. **In the context of school, E-mail should not be considered private**. Educationally, E-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an E-mail in relation to their age and good network etiquette; ‘netiquette’.

Managing E-Mail

- The school gives staff their own E-mail account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious E-mails and avoids the risk of personal profile information being revealed

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary E-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal E-mail addresses

- The school requires a standard disclaimer to be attached to all E-mail correspondence. The responsibility for adding this disclaimer lies with the account holder.

- All E-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

- Staff sending E-mails to external organisations, parents or pupils are advised to cc. the Headteacher/line manager

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your E-mail account as follows:
  - Delete all E-mails of short-term value
  - Organise E-mail into folders and carry out frequent house-keeping on all folders and archives

- The forwarding of chain letters is not permitted in school.

- All pupil E-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in E-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive E-mail

- Staff must inform (the E-safety Co-ordinator/ line manager) if they receive an offensive E-mail

- Pupils should be introduced to E-mail as part of the Computing Curriculum

- However you access your school E-mail (whether directly, through webmail when away from the office or on non-school hardware) the school's AU policy applies.

Sending e-Mails

- If sending E-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section E-mailing Personal, Sensitive, Confidential or Classified Information

- Use your own school E-mail account so that you are clearly identified as the originator of a message

- Keep the number and relevance of E-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- School E-mail is not to be used for personal advertising

Receiving E-mails

- Check your E-mail regularly

- Never open attachments from an untrusted source; Consult your network manager first.

- Do not use the E-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

E-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using E-mail - E-mailing confidential data is not recommended and should be avoided wherever possible

- Where your conclusion is that E-mail must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by E-mail
  - Exercise caution when sending the E-mail and always follow these checks before releasing the E-mail:
  - Verify the details, including accurate E-mail address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to E-mail requests for information

- Do not copy or forward the E-mail to any more recipients than is absolutely necessary
- Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
- Do not identify such information in the subject line of any E-mail
- Request confirmation of safe receipt

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' E-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-safety. Internet activities are planned and well managed for these children and young people.E-safety

E-safety - Roles and Responsibilities

As E-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 E-safety co-ordinator in this school is Mrs L Tanner who has been designated this role by the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the E-safety co-ordinator to keep abreast of current issues and guidance through organisations such Essex LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ E-safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements 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: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

E-safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety.

- The school has a framework for teaching Internet skills in ICT/ PSHE lessons. .

- The school provides opportunities within a range of curriculum areas to teach about E-safety

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-safety curriculum

- Pupils are aware of the relevant legislation when using the Internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. 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 staff member, or an organisation such as Childline or CEOP report abuse button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

- Our staff receive regular information and training on E-safety issues in the form of workshops and discussions and dissemination of information

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)

- All staff are encouraged to incorporate E-safety activities and awareness within their curriculum areas

Managing the School E-safety Messages

- We endeavour to embed E-safety messages across the curriculum whenever the Internet and/or related technologies are used

- The E-safety policy will be introduced to the pupils at the start of each school year

- E-safety posters will be prominently displayed

Incident Reporting, E-safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the E-safety Co-ordinator.

Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported.

South BenfleetPrimary School
E-Safety Incident Log

Details of **all** E-Safety incidents to be recorded by the E-Safety Coordinator. This incident log will be monitored termly by the Headteacher, the SLT or Chair of Governors.

E-safety Incident Log

Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident.

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

Misuse and Infringements

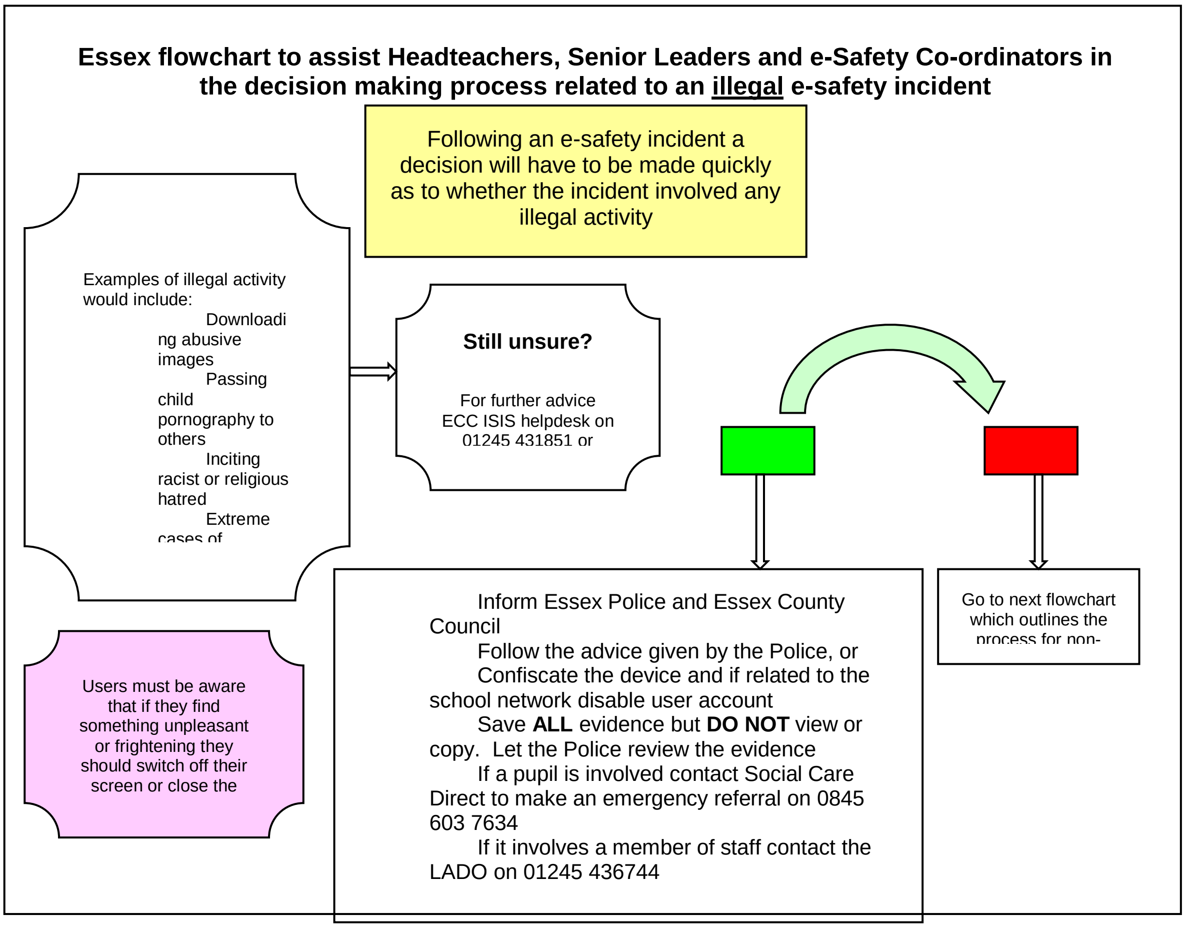
Complaints

Complaints and/ or issues relating to E-safety should be made to the E-safety co-ordinator or Headteacher. Incidents should be logged and the **Essex Flowcharts for Managing an E-safety Incident** should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

- Users are made aware of sanctions relating to misuse or misconduct through the relevant HR policies and through the Safeguarding/Whistleblowing policies and procedures.



Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an illegal e-safety incident

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity

Examples of illegal activity would include:

Downloading abusive images

Passing child pornography to others

Inciting racist or religious hatred

Extreme cases of

Still unsure?

For further advice ECC ISIS helpdesk on 01245 431851 or

Inform Essex Police and Essex County Council

Follow the advice given by the Police, or

Confiscate the device and if related to the school network disable user account

Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

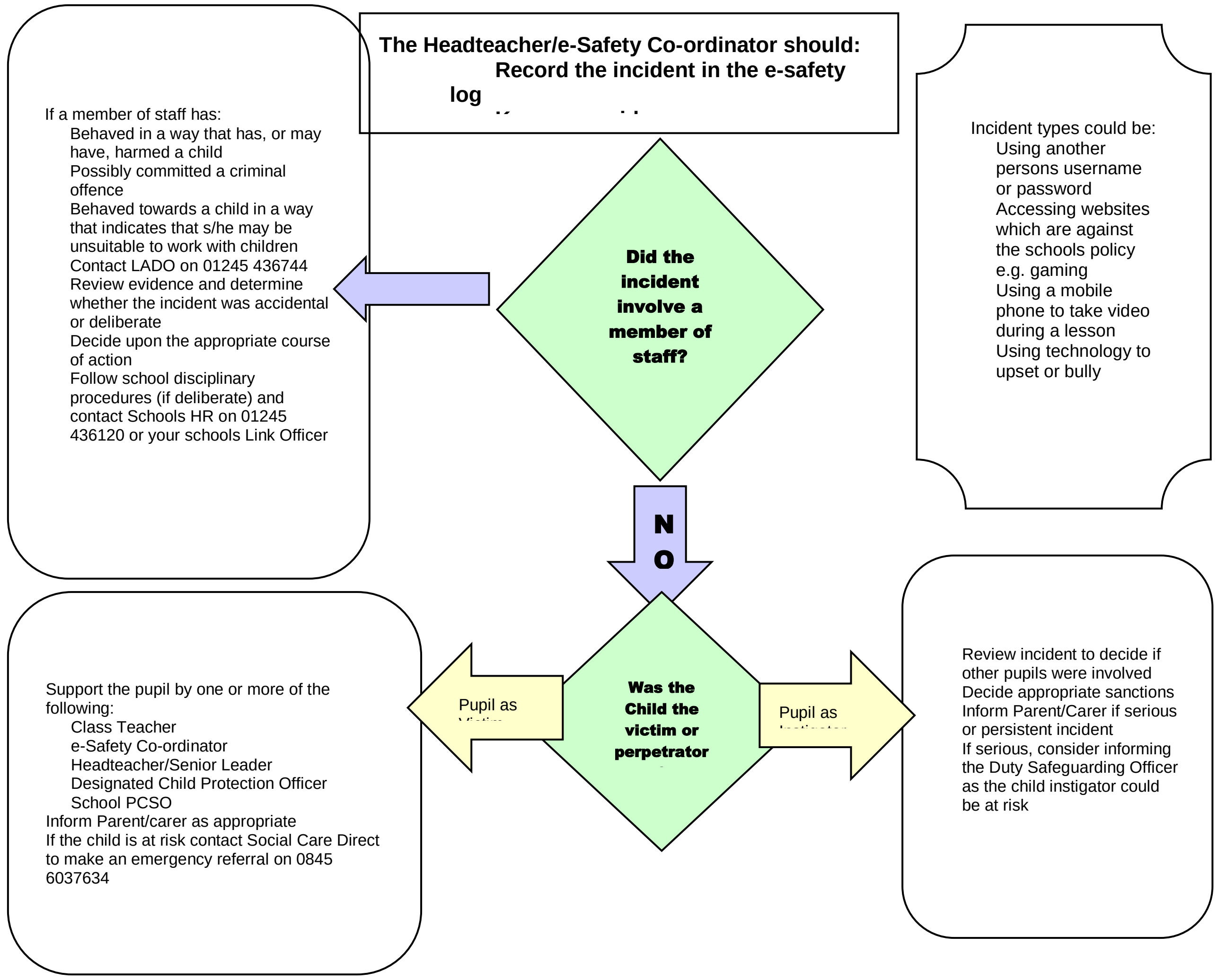
If a pupil is involved contact Social Care Direct to make an emergency referral on 0845 603 7634

If it involves a member of staff contact the LADO on 01245 436744

Go to next flowchart which outlines the process for non-

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the

Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an e-safety incident where no illegal activity has taken place



The Headteacher/e-Safety Co-ordinator should:
Record the incident in the e-safety log

If a member of staff has:
- Behaved in a way that has, or may have, harmed a child
- Possibly committed a criminal offence
- Behaved towards a child in a way that indicates that s/he may be unsuitable to work with children
- Contact LADO on 01245 436744
- Review evidence and determine whether the incident was accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact Schools HR on 01245 436120 or your schools Link Officer

Did the incident involve a member of staff?

Incident types could be:
- Using another persons username or password
- Accessing websites which are against the schools policy e.g. gaming
- Using a mobile phone to take video during a lesson
- Using technology to upset or bully

NO

Was the Child the victim or perpetrator

Pupil as

Support the pupil by one or more of the following:
- Class Teacher
- e-Safety Co-ordinator
- Headteacher/Senior Leader
- Designated Child Protection Officer
- School PCSO

Inform Parent/carer as appropriate

If the child is at risk contact Social Care Direct to make an emergency referral on 0845 6037634

Pupil as

Review incident to decide if other pupils were involved

Decide appropriate sanctions

Inform Parent/Carer if serious or persistent incident

If serious, consider informing the Duty Safeguarding Officer as the child instigator could be at risk

Internet Access

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.

Managing the Internet

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile Internet technology

- Staff will preview any recommended sites before use

- If Internet research is set for homework, specific sites should be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience

- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog - please refer to the school's Social Networking Policy.

- On-line gambling or gaming is not allowed on school equipment

Infrastucture

- School Internet access is controlled through the LA's web filtering service.

- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the E-safety coordinator or teacher as appropriate

- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the headteacher

- If there are any issues related to viruses or anti-virus software, the network manager should be informed

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting E-safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss E-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)

- Parents/ carers are expected to sign a Home School agreement

- The school disseminates information to parents relating to E-safety where appropriate in the form of;

    - Information and celebration events
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Training

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services

- Make sure you enter your personal passwords each time you logon.

- Staff should change temporary passwords at first logon

- Change passwords whenever there is any indication of possible system or password compromise

- Do not record passwords or encryption keys on paper or in an unprotected file

- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

- Passwords must contain a minimum of six characters and be difficult to guess

- User ID and passwords for staff and pupils who have left the School are removed from the system

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-safety Policy and Data Security

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and/or Learning Platforms, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure

- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access

- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others

- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print.

- Only download personal data from systems if expressly authorised to do so by your manager

- You must not post on the Internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Store all removable media securely

- Securely dispose of removable media that may hold personal data

- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school’s network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school’s network and deleted from the pupil’s device

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil’s Images and Work

On a child’s entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school’s communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school

- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

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, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Further information relating to issues associated with School websites and the safe use of images in Essex schools on the Essex Schools Infolink http://esi.essexcc.gov.uk

Storage of Images

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

Webcams

- We do not use publicly accessible webcams in school

- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults

- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
  - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available

- Ensure that all ICT equipment that you use is kept physically secure

- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive

- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted

- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles

- Privately owned ICT equipment should not be used on a school network

- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible

Internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- Pupils are only allowed to bring personal mobile phones to school with the agreement of the Headteacher and only in extreme circumstances. At all times the device must be switched off and handed to the school office during the school day. The school does not accept any liability or responsibility for mobile technology handed in.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

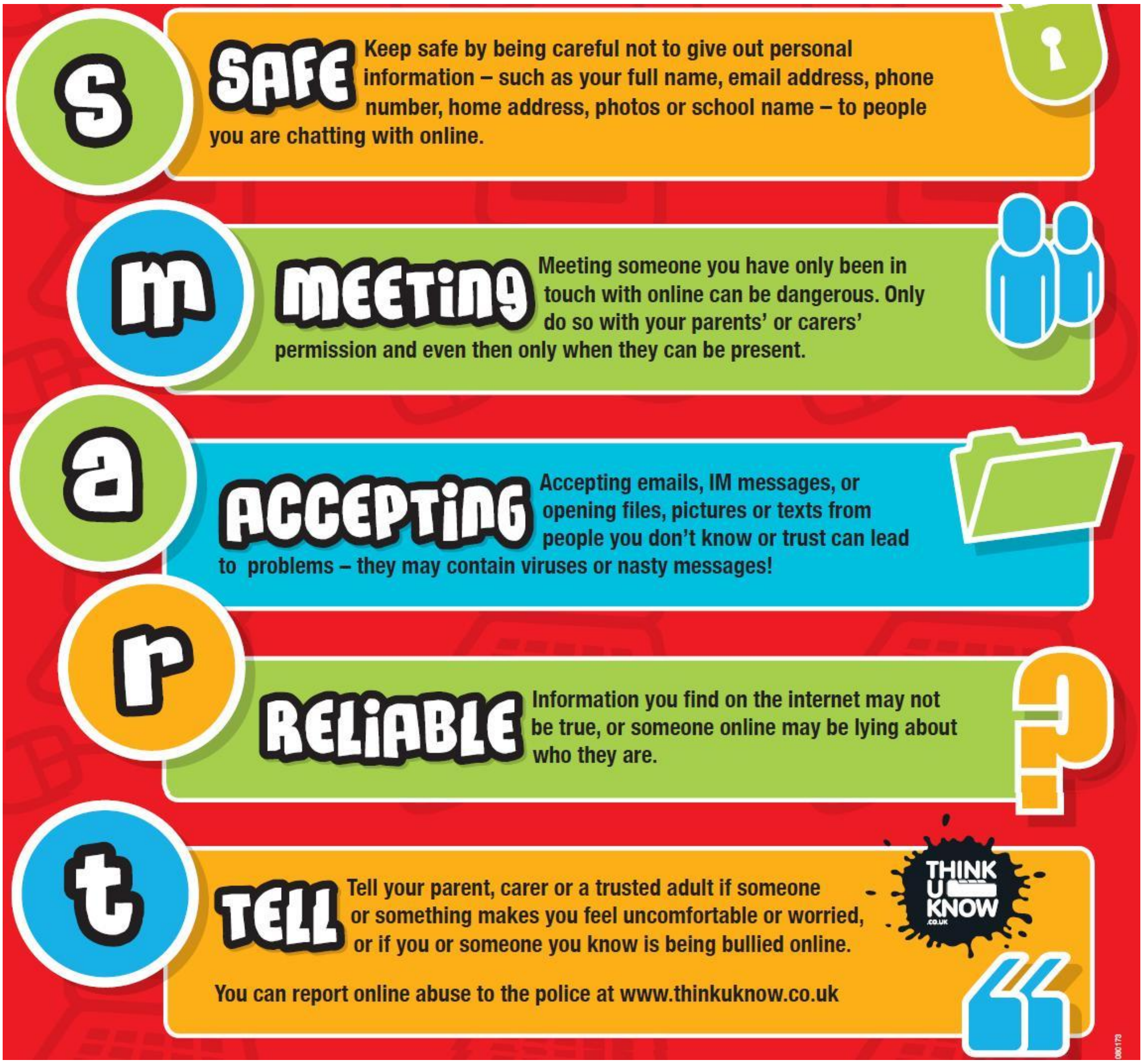
Removable Media

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

SMART RULES Poster

E-safety guidelines to be displayed throughout the school

SMART RULES



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.

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.

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!

RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

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.

You can report online abuse to the police at www.thinkuknow.co.uk

Review Procedure

There will be an on-going opportunity for staff to discuss with the E-safety coordinator any issue of E-safety that concerns them

This policy will be reviewed every 2 years and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Policy Written by: Mrs L Tanner

Date: June 2015

Review Date: Summer 2017