Elmstead Primary School

E-Safety Policy

Approved by Governors: November 2017

Review Date: November 2020

Elmstead Primary School

E-Safety Policy

This Policy must be read in conjunction with the Child Protection Policy and Code of Conduct Policy.

Scope of the Policy

This policy applies to all members of our school community (including staff, children / pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school computing systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles & Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governing Body	Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role Safeguarding Governor and this includes E-Safety.
Headteacher, Deputy Headteacher and Inclusion Leader	• The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community • The Headteacher, Deputy Headteacher and Inclusion Leader are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. • The Headteacher is responsible for ensuring that the Deputy Headteacher, Inclusion Leader and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

Computing Subject Leader	The Computing Subject Leader is responsible for: • Day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents. • Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. • Providing training and advice for staff. • Liaising with the Local Authority. • Liaising with school technical staff. • Receiving reports of e-safety incidents . • Meeting regularly with Safeguarding Governor to discuss current issues. • Reporting to the Headteacher.
Network Manager/Safeguarding Designated Person	The Network Manager/Safeguarding Lead is responsible for ensuring: • That the school's technical infrastructure is secure and is not open to misuse or malicious attack. • That the school meets required e-safety technical requirements and any Essex County Council E-Safety Policy or Guidance that may apply. • That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. • The Essex County Council filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. • That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • That the use of the network, internet, Virtual Learning Environment, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Computing Subject Leader.
Safeguarding Designated Person	The Headteacher, Deputy Headteacher and Inclusion Leader should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from: • Sharing of personal data. • Access to illegal / inappropriate materials. • Inappropriate on-line contact with adults / strangers.

	• Potential or actual incidents of grooming. • Cyber-bullying.
Teachers	Teachers and Support Staff are responsible for ensuring that; • They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices. • They have read and understood the Staff Code of Conduct Policy. • They report any suspected misuse or problem to the Headteacher, Deputy Headteacher or Inclusion Leader for investigation/ action/sanction. • All digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems. • E-safety awareness are embedded in all aspects of the curriculum and other activities. • Pupils understand and follow the e-safety policy. • Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and implement current policies with regard to these devices. • In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
Pupils	Pupils; • Are responsible for using the school digital technology systems in accordance with the E-Safety Policy and poster (Appendix 1). • Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. • Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying. • Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
Parent/Carers	Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile

	devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events • and refrain from using social networking sites to discuss sensitive issues about the school.

Policy Statement

Education – Pupils	Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: • A planned e-safety curriculum should be provided as part of Computing, SRE and PHSE lessons and should be regularly revisited. • Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities. • Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information. • Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. • Staff should act as good role models in their use of digital technologies, the internet and mobile devices. • In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked

	as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. • Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. • Staff teaching e-safety messages must read the E-Safety Policy in conjunction with the Staff Code of Conduct Policy.
Education – Parent/Carer	Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through: • Curriculum activities • Letters, newsletters, website • Parents'/Carers' evenings/sessions • High profile events/campaigns e.g. Safer Internet Day • Reference to the relevant web sites/publications

Technical-infrastructure/equipment, filtering & monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers and wireless systems are password protected and physical access is restricted as much as possible in a working environment.
- All users will have clearly defined access rights to school technical systems and devices.
- The School Bursar is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Key members of staff are supplied with secure email addresses.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act), however, the school does ask that these photos are not shared on social media.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission .
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils’ full names will not be used anywhere on a website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject’s rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages.

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and/ pupils or parents / carers (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 may be provided with individual school email addresses for educational use.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media – Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk School staff should ensure that:
- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- The school's use of social media for professional purposes will be checked regularly by the Headteacher/Deputy Headteacher.

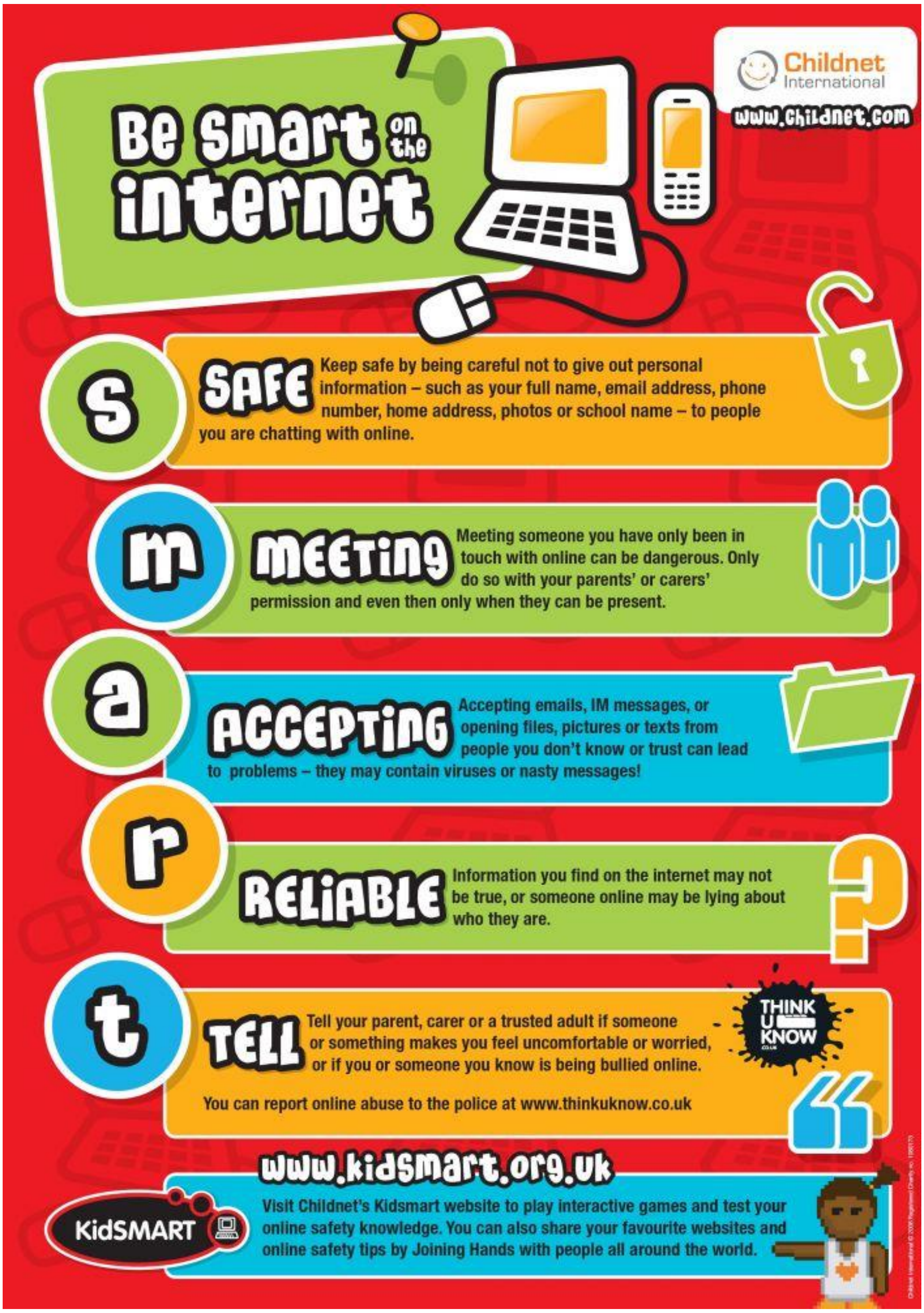
Unsuitable/Inappropriate Activities

If any member of the school community has any concerns regarding unsuitable/inappropriate activities when using technologies they should immediately report them to the designated safeguarding lead on the agreed proforma in line with normal safeguarding procedures.

Monitoring the Effectiveness of the Policy

The practical application of this policy will be reviewed every three years or when the need arises by the Computing Subject Leader, the Headteacher and/ or the nominated governor.

Appendix 1



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.

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

www.kidsmart.org.uk

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.