SHOREFIELDS SCHOOL
E-SAFETY POLICY

Staff Consulted (Date)	Governors Review (Date)	Comments	Next Review Due (Date)
	2018		2020
	Jan 2020		2023

Introduction

This policy applies to all members of the school community (including staff, students/pupils and visitors) who have access to and are users of ICT systems, both in and out of school.

E-Safety is defined for the purposes of this document as the process of limiting the risks to children and young people when using the internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection (Essex Safeguarding Children Board).

This policy is intended to be a live document which can adapt to new technology that is developed that could bring an element of risk to others.

Aims

- The aims of the policy are to ensure that:
- Pupils, students and staff are educated in the understanding of the risks associated with E Safety.
- Knowledge, policies and procedures are in place to prevent incidents of inappropriate E Safety Behaviour in school and in the wider school community
- We have effective measures to deal with inappropriate E Safety Behaviour
- We continue to monitor E Safety Approaches.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E Safety Policy and for reviewing the effectiveness of the policy. Governors will receive regular reports on E Safety via Safeguarding reporting.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including E Safety) of members of the school community.
- The Headteacher/ Senior Leaders should be aware of the procedures to be followed in the event of an E Safety Incident. Such incidents are dealt with via Safeguarding procedures
- The Headteacher/Senior Leaders are responsible for ensuring the staff receive relevant E Safety training to enable them to carry out their E Safety Roles
- The Headteacher/Senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out internal E Safety monitoring and that ensuring the infrastructure is robust and in place at all times.

Technical Staff

Are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- That the school meets the required E Safety Standard set out in the Essex Safeguarding Children Board's E Safety Policy Guidance T
- That users may only access network and devices through a secure password procedure that ensures passwords are regularly changed
- That they keep up to date with E Safety technical information and approaches

- That the use of the network/internet is regularly monitored in order that any misuse/attempted misuse can be reported.
- Delivery of up to date training

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of E-safety matters and knowledge of safeguarding procedures in place.
- They report any suspected misuse or problem through the safeguarding procedures
- They attend/engage with relevant E Safety training
- All digital communication with colleagues/students/ pupils/ parents and carers is at a professional level
- E safety approaches are embedded in all aspects of the curriculum and other activities
- Students understand and follow the E Safety guidance around the school
- They monitor, where appropriate, the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement safeguarding procedures if necessary.
- In lessons where internet use is pre-planned, students should be guided to sites checked to be suitable for their use and that processes are in place for dealing with unsuitable material that is found in internet searches.
- They are in close supervision with students using all devices (eg laptops,ipads, eyegaze etc) and the use of unrestricted internet sites (eg youtube, google etc).
- Act appropriately when engaging with social media and ensure they use no reference to the school or other colleagues or pupils.

Pupils/Students:

Where appropriate, pupils/students should:

- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. In our school this will generally mean they understand that they should tell a member of staff about anything they feel is inappropriate on the computer
- Know and understand safe practice on the use of mobile devices and digital camera
- Understand the importance of adopting good e safety practise when using digital technologies outside of school and that the school's E Safety Policy covers their actions out of school, if it relates to the school community.
- To recognise visuals around the school that offer support and advice on E Safety procedures.

Parents:

Parents have a crucial role to play in ensuring their children are safe using digital technologies. The school will take every opportunity to support parents understanding of the risks associated with E Safety through having regular parents evening, coffee Mornings, newsletters, letters and support on the school website including links to local e-safety training when available.

Parents also need to ensure they understand and sign the Photography permission letter, distributed at each annual review.

E Safety Expectations

Education - Students

Although technical procedures are there to ensure the safety of the students when accessing digital technologies, the education of students to be safe on digital devices is of paramount importance to support them in living a safe and fulfilling life with technology in the future. Therefore the school ensures that:

- A planned E Safety curriculum should be provided as part of Computing/PSHE and other lessons and it should be regularly re visited
- Key E Safety messages should be reinforced as part of planned assemblies taking place in school.
- Consistent visual E Safety Guidance Posters (Appendix) are in place in all areas where students can have access to digital technologies.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices

Education- parents

Some parents may have a limited understanding of the risks associated with the internet. As many of the risks associated with computers are as much prevalent out of school as in, the school will seek to provide a rounded and accessible support package, that will include:

- Regular 'E-Safety Bites' displayed in the School Newsletter that will give helpful information to support parents
- Coffee Morning sessions and advice training to be offered to parents to discuss E Safety issues. These will be from in house IT staff and external agencies depending on availability and subject.
- E Safety communication to be passed on when appropriate by letters, guidelines and magazines
- Parents can contact the ICT Manager for direct advice and guidance.

Acceptable Use

While using school computers certain actions can relevant for certain situations or person. To help explain the levels of appropriate accessibility the table below (Table 1) outlines Acceptable use for both students and staff. Visitors will often fall under the staff expectations, but this can be discussed with the member of the Senior Leadership Team responsible for their visit.

This table will be displayed and shared as appropriate. Staff maybe directed to the table as a quick resource on acceptable use. Although best practice is to read the table with the policy:

	STAFF				Students			
User Action	allow	exceptional	At certain times	Not allowed	allow	With staff supervision	exceptional	Not allowed
COMMUNICATIONS								
Mobiles in school	x						x	
Use of mobile in lesson		x						x
Use of mobile in social time	x							x
Taking photos on mobile		x						x
use of other devices eg tablet, console			x			x		
Use of school email for personal emails			x			X		
Messaging apps			x				In lesson	x
Social media/blogs			x				In lesson	x
OTHER RISKS								
Child abuse images – protection of children act				x				x
Grooming, incitement – sexual offences act				x				x
pornography				x				x
Racist material – Public order act				x				x
Promoting discrimination				x				x
School systems to run private business				x				x
Infringing copyright				x				x
Reveal/publish confidential data				x				x
Create or spread virus intentionally				x				x
Unfair use of systems eg excessive download				x				x
Online gaming (educational)			x			x		
Online gaming (non educational)				x			x	
Online gambling				x				x
Online shopping		x					x	
Online File sharing			x					x
Video broadcasting eg youtube		x				x		

Technical – infrastructure /equipment, filtering and monitoring

The School ICT Department are responsible for ensuring:

- The school uses an Internet Service Provider (ISP) who subscribes to the Internet Watch Foundation (IWF) filtering list. This will help to filter out some inappropriate content, but not all. Using an accredited ISP will also provide higher standards for filtering.
- Levels of internet access and supervision must be age appropriate and suitable for the young people. Filtering systems should be secure but adaptable.
- Older children and professionals may sometimes require temporary access to a normally restricted website in order to carry out research for a project or study. This decision needs to be made by a Senior Member of Staff, if temporary access is required within filtering boundaries.
- There are regular reviews and audits of the safety and security of the school's technical systems.
- An agreed process is in place for the provision of temporary access as 'guests' (e.g. trainee teachers, supply teachers and visitors etc).

Use of digital and video images

The school obtains general consent from parents/carers for their child to be photographed/filmed by means of a general consent form (Appendix A). This is completed for new learners on joining the school and then sent annually to all parents/carers to confirm their agreement. If not form is returned, it is marked as 'no consent given'.

For circumstances falling outside the normal day to day activities of the school in which pictures of the learners are requested, specific informed written consent from parents/carers is always requested. (Appendix B)

Staff (and other adults) are expected to:

- Give careful consideration as to how activities involving the taking of images are organised and undertaken.
- Only display learners' first names with their photograph in the classrooms. In all other instances, staff/other adults should avoid naming the learner. However, if a name is required then only the first name should be used.
- Ensure that images are securely stored and used only by those authorised to do so.
- Be able to justify images of learners in their possession.
- Avoid images which show a single child with no surrounding context.
- Ensure that the learner is correctly dressed to ensure that appropriate levels of integrity and decency are maintained.
- Use only equipment provided or authorised by the school. Mobile telephone or any other similar devices must NOT be used in the school to take images of children except in exceptional circumstances and then deleted and logged by the ICT Manager.
- Never take images in situations that might be construed as being secretive.
- Never take photographs/films of learners for their personal use.

Newspapers and the Internet:

The staff member working with the external media needs to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media or on the

Internet. Ensure the image is used only in its intended context. Newspapers will not print anonymous photographs and therefore if a newspaper is invited in to celebrate an event, the school must give thought to this beforehand and allow only those learners who parents/carers have given permission to be included in the photo opportunities.

College students/trainees:

As part of their training, many adult students are required to compile portfolios with photographs of children during lessons. These students should follow the practices as set out above. In addition a member of the management team will oversee the compiled images as part of the management process and consider their appropriateness.

Concerts, Presentations and other school events

- Parents/carers will be allowed to take photographs/videos at such events. However should the school decide that the event is one at which photography and videoing will not be permitted, parents/carers will be informed prior to that event.
- Parents/carers will be prompted with a verbal announcement at the start of the event that any images must be taken for personal use only and must not be put on the web/internet.
- People with no connection to the school will not be allowed to photograph – staff will question anyone they do not recognise who is using a camera or video recorder at events and productions.
- Parents will at all times be required to comply with the guidelines set out in the document 'Use your camera and video courteously

Any concerns about any inappropriate or intrusive photographs found must be reported immediately through the school's child protection procedures.

Email

The technical team have responsibility for setting up individual email accounts for teachers, TAs and students when appropriate. These need to be used in professional manner and for school based communication. Students are to have access to email when using it as part of their Computing curriculum.

Emails that include reference to Students in the school sent to external emails should only include the student's initials, for example JS (John Smith) and personal information should be carefully shared. If staff are concerned or worried about how to send emails and what to include they are encouraged to speak to a Senior member of staff or the Technical team.

Emails sent to other agencies containing personal data will be securely transmitted using the system that the LA recommended as secure.

Social media

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential to ensure the protection of pupils, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in 'Teachers Standards'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise. The school

has a duty of care to provide a safe learning environment for pupils and staff. The school could be held responsible, indirectly for acts of their employees in the course of their employment.

Staff members who harass, cyber-bully, 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:

The school is to ensure training delivered includes:

- 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 students, 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
- No photos are taken within the school grounds are uploaded to the internet, even without students being present