Shoreham Village School

E-Safety Policy

Ratified by Governing Body

Signed:

Chair of Governors

Date: May 2023

To be reviewed: May 2025

1.1 Who will write and review the policy?

The school has appointed an e–Safety Coordinator, Mrs Gillian Lovatt-Young.
Our e–Safety Policy has been written by the school, building on the KCC e–Safety Policy and government guidance. We recognise that we have a ‘duty of care’ to educate of members of the school community on the risks and responsibilities of e-safety. E-safety covers the Internet but it also covers mobile phones and other ICT electronic technologies.

- Our School Policy has been agreed by the Senior Leadership Team and approved by governors and other stakeholders.
- The School has appointed a member of the Governing Body to take lead responsibility for e-Safety

1.2 Teaching and learning

1.2.1 Why is ICT and Internet use important?

- ICT and Internet use is part of the statutory curriculum and are necessary tools for learning and communication.
- ICT and the Internet are beneficial parts of everyday life for education, business and social interaction.
- The school has a duty to provide pupils with quality ICT and Internet access as part of their learning experience.
- Pupils use ICT and the Internet widely outside school and need to learn how to evaluate Internet information and how to conduct themselves online to take care of their own safety and security.
- The purpose of Internet use in school is to enhance the curriculum, challenge pupils and support raising educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management functions.
- ICT and Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

1.2.2 How does ICT and Internet use benefit education?

.

Benefits of using ICT and the Internet in education include:

For pupils:

- Access to learning whenever and wherever convenient
- Individualised access to learning
- Freedom to be creative and to explore the world and its cultures from within a classroom
- access to worldwide educational resources and institutions including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;

- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- An enhance curriculum; interactive learning tools; collaboration, locally, nationally and globally; self-evaluation; feedback and assessment; update on current affairs as they happen.
- Social inclusion, in class and online
- Access to learning wherever and whenever convenient
- Access to experts, role models, inspirational people and organisations in many fields for pupils and staff;

For staff:

- professional development for staff through access to national developments, educational materials, classroom strategies and effective curriculum practice;
- Immediate professional and personal support through networks and associations
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with KCC and DfE;

For parents:
By using e mail for school communications it speeds up the process and makes it environmentally responsible.

1.2.3 How can ICT and Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught that ICT and Internet use is a responsibility and what is acceptable and what is not and given clear objectives for ICT and Internet use.
- The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils. The aim is to ensure a balance between controlling access and allowing freedom to explore and use tools to their full potential.
- Staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1.2.4 How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

1.3 Managing Information Systems

1.3.1 Maintenance of information systems security:

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For KCC staff, flouting electronic use policy is regarded as a reason for dismissal.
- Workstations will be secured against user mistakes and deliberate actions.
- Servers is located securely and physical access restricted.
- The server operating system will be secured and kept up to date.
- Virus protection for the whole network is installed and current.
- Access by wireless devices is proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- Central KPSN Schools Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and KCC/EiS.

The Schools Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes in Maidstone and Canterbury. These industry leading appliances are monitored and maintained by a specialist security command centre.

- The security of the school information systems and users is reviewed regularly.
- Files held on the school network will be regularly scanned for viruses and virus protection is updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media is not used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced. This includes all users keeping passwords private, being informed not to share passwords and use of STRONG passwords. Sensitive data will be password protected.

1.3.2 Management of emails:

The school uses e mail internally for staff and pupils and externally for contacting parents and other professionals.

It is an essential part of communication. Staff and pupils are made aware that their school email accounts must only be used for school related matters.

School e mail accounts and appropriate use:

Pupils:

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive, threatening or unsuitable email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole -class or group email addresses will be used in school for communication outside of the school.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and is restricted.
  Staff:
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- Staff should not use personal email accounts during school hours or for professional purposes.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- The forwarding of chain messages is not permitted.

Pupils will be educated through the ICT curriculum to identify spam, phising and virus emails and attachments that could harm the school's network or their personal account or wellbeing.

1.3.3 Management of published content and the School website:

- The contact details on the website are in the public domain and contains the school address, email and telephone number. Staff or pupils' personal information will not be published.
- Any other information published will be carefully considered in terms of safety for the school community, copyrights and privacy policies.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

1.3.4 Use of pupils' images or work:

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- In accordance with the Data Protection Act 1998 written permission from parents or carers is obtained before images/videos of pupils are electronically published.
- Pupils work is only published with their permission or their parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School has a separate policy regarding the use of photographic images of children which outlines policies and procedures.
- Parents should follow the standard school complaints procedure if they have a concern or complaint regarding misuse of school photographs.

1.3.5 Management of social networking, social media and personal publishing:

- The school will control access to social media and social networking sites.
- Pupils will be educated to make their own informed decisions and take responsibility for their conduct online. This includes never give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Any concerns raised regarding pupils'' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour is outlined in the school Acceptable Use Policy.

1.3.6 Management of filtering:

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

1.3.7 Management of videoconferencing:

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

1.3.8 Management of emerging technologies:

- Emerging technologies will be examined for educational benefits and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

1.3.9 Protection of personal data:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the school follows principles of good practice when processing data.
This includes for example, data being kept securely and no longer than necessary and being processed accurately.

1.4 Policy Decisions

1.4.1 Authorisation of Internet access:

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the 'Staff Information Systems Code of Conduct' or School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitor to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

According to Setting Type

- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

1.4.2 Assessment of risks:

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

1.4.3 Management of incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other school in Kent.

1.4.4 Handling of e–Safety complaints:

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

1.4.5 management of internet use across the community:

- The school will liaise with local organisations to establish a common approach to e–Safety.
- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

1.4.6 management of Cyberbullying:

- Cyberbullying (along with all other forms of bullying) of any member of the school community will be taken very seriously and not tolerated. Full details are set out in the school's policies on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
    - The "bully" will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

1.4.7 Management of Learning Platforms:

- Any concerns about content on the LP may be recorded and dealt with in the following ways:
    a) The user will be asked to remove any material deemed to be inappropriate or offensive.
    b) The material will be removed by the site administrator if the user does not comply.
    c) Access to the LP for the user may be suspended.
    d) The user will need to discuss the issues with a member of Senior Leadership team before reinstatement.
    e) A pupil's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the Senior Leadership team. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

1.4.8 Management of mobile phones and personal devices:

- The use of mobile phones and other personal devices by pupils and staff in school has been decided by the school and is covered in the school Acceptable Use or Mobile Phone Policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- Mobile phones will not be used during lessons or formal school time.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student’s withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to ‘silent’ mode, Bluetooth communication should be “hidden” or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

1.5 Communication Policy

1.5.1 Introduction of this policy to pupils:

- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

1.5.2 Introduction of this policy with staff:

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

1.5.3 Enlistment of parents’ support:

- Parents’ attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents I a variety of formats.

- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the "e–Safety Contacts and References section".

This policy has regard for the standard guidelines for all schools published by KCC in January 2016 using the template on the KELSI website: http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety.

Schools e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

Has the school an e-Safety Policy that complies with Kent guidance?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y/N
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/carers or pupils sign an Acceptable Use Policy?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N

Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N
Does the school log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	

Self Evaluation Tool for Schools Online Safety Practice

Policies and practice	No	Partly	Yes	Comments/Actions /Evaluation
Is online safety clearly identified as a safeguarding issue within the school with appropriate Senior Leadership Team (SLT) strategic oversight to ensure that leaders oversee the safe use of technology and can take action immediately if they are concerned about bullying or children's well-being?	🟥	🟨	🟩	
Is the SLT aware of the statutory responsibilities regarding safeguarding which includes online safety? For example Keeping Children Safe in Education (2015) and the Prevent Duty.				
How are SLT engaged and involved with ensuring the online safety agenda is shared and communicated with stakeholders?				
Does the school have a set of robust online safety policies and practices which cover the following issues: use of mobile phones/personal devices, use of images/cameras, social media, education/training for children and staff?	🟥	🟨	🟩	
Is the online safety policy specific to the schools needs and requirements e.g. taking into account technology access and needs/requirements of pupils?	🟥	🟨	🟩	
When was the online safety policy last updated? (N.B. this is recommended to be reviewed annually)				
How were stakeholders involved in creating or reviewing the policy e.g. staff, parents/carers, children?				
Is the online safety policy cross referenced with other appropriate school policies e.g. anti-bullying policy, behaviour, searching, data security and safeguarding etc?	🟥	🟨	🟩	
How is the operation of the schools policies checked and enforced by the school?				
Have the policies been approved by the Governing Body? If so, when?	🟥	🟨	🟩	
Is the policy clearly communicated with the wider school community e.g. is the online safety policy available on the school website?	🟥	🟨	🟩	

Does the school have a robust acceptable use policy (AUP) which is appropriate for all members of the community? If so, when was it last updated? (N.B. schools may have multiple AUPs for different audiences)	🟥	🟨	🟩	
How does the school ensure that the AUP is understood and respected by pupils, staff and parents?				
Are there clear reporting mechanisms in place for online safety concerns for staff, pupils and parents/carers? If so, what are they? E.g. flowcharts, reporting buttons/emails etc and are specific members of staff identified as points of contact?	🟥	🟨	🟩	
Are there effective sanctions in place for breaching the school’s online safety policy or AUP? If so, what are they and where are they located (e.g. in the behaviour policy)?	🟥	🟨	🟩	
Does the school have an online safety Coordinator/lead (or group) with clearly defined responsibilities? If so, who are they? (NB recommended Designated Safeguarding Lead (DSL) and/or SLT)	🟥	🟨	🟩	
Does the school keep an online safety incident log?	🟥	🟨	🟩	
How is the incident logged used to inform and review practice?				
Is there a member of the Governing Body with responsibility for online safety? If so, who and have they received appropriate training?	🟥	🟨	🟩	
Does the school understand the impact level of personal data and is data managed securely and in accordance with the statutory requirements of the Data Protection Act 1998 e.g. written consent to take/share images, school provided email addresses used, school provided devices, strong passwords, encryption of personal information and use of secure email?	🟥	🟨	🟩	
Infrastructure	No	Partly	Yes	Comments/ Actions / Evaluation
Is the schools network safe and secure? E.g. devices which leave the site are encrypted, strong passwords are in place (for all but the very youngest users) and screen locks are enforced.	🟥	🟨	🟩	
Does the school use an accredited/education appropriate internet service provider and relevant filtering/monitoring products?	🟥	🟨	🟩	
How does the school monitor the school network and internet use for safeguarding or security concerns? E.g. key word monitoring, history checks etc.	🟥	🟨	🟩	
How are filtering decisions made by the school?				
How does the school manage and respond to filtering/security breaches?				
What devices does the school have e.g. tablets, laptops etc and how has the school ensured that these devices are used safely and that education, policy and procedures have been updated to reflect school technology use?				
Education and Training	No	Partly	Yes	Comments/Actions / Evaluation

Do all members of staff (including all support staff) receive regular, appropriate and up-to-date online safety training and guidance which enables them to understand how the internet/technology can be used to groom, radicalise or abuse pupils?	🟥	🟨	🟩	
How is online training delivered to all staff? How does the school ensure that this training is up-to-date?				
Has the DSL or at least one member of senior leadership staff attended appropriate training to ensure they have a higher level of expertise and understanding of online safety issues?	🟥	🟨	🟩	
How does the school ensure that all members of staff understand the school policies and procedures regarding online safety?	🟥	🟨	🟩	
Do all members of staff know how to protect their online reputation understand the expectations and boundaries regarding safe and appropriate relationships and communications with pupils/parent via social media? e.g. staff do not share any personal information with pupils/parents and all communication takes place within clear and explicit professional boundaries which are transparent and open to scrutiny?	🟥	🟨	🟩	
Do all children receive a progressive and embedded online safety education? • Is the online safety education within the school progressive and embedded throughout the curriculum for all ages? E.g. www.digital-literacy.org.uk • How are special or specific events used to support this? • Are peer mentoring programmes/schemes used?	🟥	🟨	🟩	
How does the school ensure that there are strategies in place to help keep pupils safe and to support them to develop their own understanding of these risks and in learning how to keep themselves and others safe?				
How does the school ensure that vulnerable pupils access appropriate education relating to online safety e.g. targeted or differentiated support/resources?				
Is the school able to demonstrate internal capacity for online safety awareness and education? (E.g. external speakers are used to compliment student education and are not used in isolation).	🟥	🟨	🟩	
Does the school participate in local and national events such as Safer Internet Day?	🟥	🟨	🟩	
Does the school reward positive use of technology? If so, how?	🟥	🟨	🟩	
How does the school work to help and support parents/carers understand Online safety issues and risks and their roles and responsibilities at both home and school? How has this been communicated and developed e.g. workshops, newsletters, online safety area on school website etc.?	🟥	🟨	🟩	
Does the school have online safety information for staff, pupils and parents on the school website e.g. school policies and contacts, CEOP button, links to ThinkUKnow, IWF, Childnet and UK Safer Internet Centre?	🟥	🟨	🟩	

Does the school use social networking/media as a form of communication? If so has this been risk assessed and approved by SLT and are appropriate safety measures been taken?	🟥	🟨	🟩	
Is Online safety covered as part of the home school agreement?	🟥	🟨	🟩	
Standards and inspection	No	Partly	Yes	Comments/Actions / Evaluation
Has the school conducted an audit of the current online safety and safeguarding measures? E.g. 360 safe: www.360safe.org.uk	🟥	🟨	🟩	
Does the school complete appropriate risk assessments regarding use of technology?	🟥	🟨	🟩	
How does the school monitor and review measures and practice after dealing with incidents/concerns?				
How does the school monitor, review and evaluate all of the above?				
Any other points or comments				

Next Steps

Key area for development	Justification	Action & Resources / support needed	Lead Staff & time allocation

Annex B

Year Group	E-Safety Topic/s covered:
Year 1	What do we use computers for? What is the difference between the computers and iPads? What do you enjoy doing on the computer? What is a link? What is an advertisement?
Year 2	What do you enjoy doing on a computer or iPads? Is it different at home and school? Why? What do we do if we see something that makes us feel uncomfortable? Recap on Computer use and Internet Safety Rules Reporting and Blocking
Year 3	Can you just take any picture and use it?

	Should you give your real name online? Real address? What situations would people ask you for your real name? Can you trust all the information you see / find out on the internet? When do you prefer to use an iPad or a computer? Music online and the law.
Year 4	Email safety, netiquette, chain mails, attachments, viruses, Trojans etc How would you respond to online bullying? The differences between face to face and online bullying. What would you do with a text message you don't like or that makes you feel uncomfortable? How do you use blogs? What sort of comments should you leave? What do you do if someone leaves a comment that makes you feel bad? How can you find the author of a document or website?
Year 5	When do you meet people online? When do you give your real name? Would you create a whole new online persona? Why would people not keep their real name online? Why do some websites have age restrictions? Is it wrong to break the rules to be a member? Research skills, evaluating websites, retrieval, reliability of information and acknowledging sources Films online and the law File sharing
Year 6	What does it mean to lie about your age for sites such as Facebook or Snapchat? Problems with chatrooms Staying safe when using chatrooms Introduction to concept of bad people online and grooming How do you respond to blog posts? What happens if someone leaves a comment that makes you feel bad? What should you do? Think before you post. Online gaming

E-Safety Contacts and References

This policy takes into account guidance published

- Working Together to Safeguard Children (March 2015)

  https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

- Keeping Children Safe in Education (September 2016)

  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/487799/Keeping_children_safe_in_education_draft_statutory_guidance.pdf

2. End to End e-Safety

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

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the KLZ (Kent learning Zone) including the effective management of Websense filtering.
- National Education Network standards and specifications.
- Staff Training

3. Further Information

Kent County Council Education & Safeguarding Team:

Principle Officer of Education & Safeguarding Team	Kel Arthur
Area Safeguarding Advisor	Helen Windiate
Kent County Council e-Safety Officer	Rebecca Avery – rebecca.avery@kent.gov.uk / esafetyofficer@kent.gov.uk W: 03000 415 788 Mob: 07789968705

http://www.kent.gov.uk/education-and-children/protecting-children/online-safety

Kent Community Network Helpdesk	03000415797 / 03000418707
ASK curriculum ICT staff	01622 203800
e-Safety materials and links	www.thinkuknow.co.uk
Curriculum e-safety advice	as above and www.kidsmart.org.uk/beingsmart https://www.getsafeonline.org http://www.saferinternet.org.uk/ https://www.ceop.police.uk/

Other useful organisations:

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kent Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 01622 690690 or contact your Safer Schools Partnership Officer. Also visit www.kent.police.uk or www.kent.police.uk/internetsafety

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kidsmart: www.kidsmart.org.uk

Schools Broadband Service Desk - Help with filtering and network security:
www.eiskent.co.uk Tel: 01622 206040

Schools e–Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com