Chase Terrace Primary School

Online Safety Policy

Together we Learn
Together we Aspire
Together we Succeed

Chase Terrace Primary School Online Safety Policy

Person Responsible for Computing:	**Phil Moore**
Designated Safeguarding Lead	**Tania Harrison**
Approval Body:	**Chair of Governors (using Chair's Power to Act)**
Date of approval:	**Chair of Governors (using Chair's Power to Act) November 2023**
Review date:	**November 2024**

The use of technology has become a significant component of many safeguarding issues. Child Criminal Exploitation, Child Sexual Exploitation, radicalisation, sexual predation, and technology often provides the platform that facilitates harm.

At Chase Terrace Primary School, we realise that it is essential for our children to be safeguarded from potentially harmful and inappropriate online material. We have an effective whole school/college approach to online safety which empowers us to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms for us to identify, intervene in, and escalate any concerns where appropriate.

Why does School need an Online Safety Policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

We must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good Online Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

1.1 Who will write and review the policy?

- At Chase Terrace Primary School, we have one teacher responsible for Online Safety and Computing across all age phases.
- The Online Safety Policy and its implementation will be reviewed annually.
- Our Online Safety Policy has been written by the school, building on government guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors.
- The School has appointed a member of the Governing Body to take lead responsibility for Safeguarding, including Online Safety.

End to End Online Safety

Online 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 Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering and monitoring systems

1.2 Teaching and learning

Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- At Chase Terrace, we believe that the Internet is a part of everyday life for education, business and social interaction.
- Therefore, the school has a duty to provide students with quality Internet access as part of their learning experience.
- Education at home/Remote learning: - Where children are being asked to learn online at home, our school will refer to and use the links and resources provided by the DfE; Safeguarding in schools, colleges and other providers and Safeguarding in remote education.
- Our pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources 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;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- 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 DfE;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for 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.
- Staff should 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.

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.
- The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
- **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

- Children are also taught to follow the smart rules: Safe, Meet, Accept, Reliability, Tell.
- The schools PSHE Curriculum encompasses the teaching of PREVENT and how to stay safe online.
- We ensure that online safety is a running and interrelated theme whilst devising and implementing policies and procedures. We consider online safety in other relevant policies, when planning curriculum, teacher training, the role and responsibilities of the DSL and parental engagement.
- *Even though Online Safety is integrated in to all units taught in Computing, as well as having their own individual units, we recognise that some children may need additional support with their understanding. Each year, during the Autumn Term, we carry out a gap analysis of each class and amend planning to ensure any worrying gaps are addressed swiftly.*

Making sure LGBT young people know who to report concerns to

- *Staff are aware that it is important for all young people to have a trusted adult to go to should they experience something worrying online. For LGBT+ young people, we recognise that they may find it more difficult to identify an adult, particularly if they are yet to 'come out' about their sexual orientation and/or identity.*
- *We encourage all children to report any concerns or worries they have by implementing simple and clear reporting procedures and by offering reassurance that neither sexual orientation nor their identity will affect how they are treated when they report any concerns.*
- *Remind young people if they feel they are being sexually exploited or are in contact with an adult who is trying to engage them in sexual activity, they should report it to the police or CEOP (link on the school website).*
- *We recognise that as with all young people, LGBT+ young people may confide in their friends and they too should be encouraged to seek help if they are worried that their friend is being exploited.*

1.3 Managing Information Systems

How will information systems security be maintained?

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.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date – servers replaced April 2015.
- Virus protection for the whole network must be installed and current.
- The school uses WIFI which has secured passwords so personal devices cannot be linked to the system. This is monitored daily.
- Monitoring will take place as follows using Netsupport DNA. The Designated Safeguarding Lead will be charged with monitoring any inappropriate abuse of the school network and internet on a regular/timetabled basis. Virus protection (Currently ENDPOINT anti-virus) will be updated regularly.
- 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.

How will email be managed?

- Pupils may only use approved email accounts for school purposes in relation to remote learning. *Children learn how to use email using Purple Mash 2Email. This is a safe, secure and teacher approved system.*
- Pupils must immediately tell a designated member of staff if they receive an offensive 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 primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- 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.

Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with their permission of the parents – including written permission from parents to publish websites using Weebly in line with the new curriculum.
- 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 will have a policy regarding the use of photographic images of children which outlines policies and procedures.

How will social networking, social media and personal publishing be managed?

The school will control access to social media and social networking sites.

- Pupils will be advised never to 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.
- 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 personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy which can be found on the school website.
- The school has a Twitter account which only publicises images of children after consent has been gathered from parents. No individual children's names will be put on our social media platform. (Please refer to separate 'Twitter Policy' for more details).

How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils (the demographic of the school has also been taken into consideration when considering filtering and monitoring arrangements).
- The school will work with the Schools Broadband team to ensure that filtering policy is continually reviewed.
- When checking filtering and monitoring systems we make sure that the system setup has not changed or been deactivated. The checks should include a range of: school owned devices and services, including those used off site, geographical areas across the site **and** user groups, for example, teachers, pupils and guests
- **A log of these** checks should be reviewed regularly.
- The school will have a clear procedure for reporting breaches of filtering. Staff have good relationships with their students which makes them approachable for reporting any online concerns. Our Head teacher, DSL and Online Safety Lead are also readily available for reporting issues as well as an online reporting arrangements through 'My Concern' being readily available to staff. The school website also has the CEOP internet safety reporting button for children and parents to further complement our robust reporting channels.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School **Technician** who will then record the incident and escalate the concern as appropriate (see above).
- Device monitoring can be managed by IT staff or third party providers, who need to: make sure monitoring systems are working as expected, provide reporting on pupil device activity, receive safeguarding training including online safety and record and report safeguarding concerns to the DSL.

How will videoconferencing be managed?

- 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.
- 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.
- 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.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit 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.

How should personal data be protected?

- Permission will be obtained from parents for the use of Purple Mash, Times Tables Rockstar and other sites which require pupil names to be uploaded.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

1.4 Policy Decisions

How will Internet access be authorised?

- 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 School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy (AUP) for pupil access and discuss it with their child, where appropriate. Permission is obtained once and reobtained if the rules are changed. Teachers revisit the rules regularly and AUP are on the school website for regular refreshment.
- 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.

How will risks be assessed?

- 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.

How will the school respond to any 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 DSL will record all reported incidents and actions taken on My Concern and other in any relevant areas e.g. Bullying Log.
- The DSL 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, indentify 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.

How will Online Safety complaints be handled?

- 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 Online Safety complaints and incidents will be recorded by the school, including any actions taken.
- 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.

How is the Internet used 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.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy 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. Staff will complete a bullying form to record the incident.
  - 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.

Mobile Phone Policy and Procedures

Aim

To protect children from harm by ensuring the appropriate management and use of mobile phones by everyone who comes into contact with the setting.

How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use Policy.
- 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.
- 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.
- 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.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.

Pupils Use of Personal Devices

- Students must have written permission from parents in order to bring a mobile device in to school. No mobile device should be kept on a child's person throughout the day.
- Devices must be kept locked in individual classroom cupboards. This is the responsibility on individual class teacher (Only children in Y6 are permitted to bring mobile phones into school).
- Children will not be permitted to take any electronic devices on school trips.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy.
- Mobile phone devices can be **searched for** by a senior staff member if a child is thought to be breaking school rules.
- 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.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students 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. This phone is a phone only, not a camera phone.
- 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. The Bluetooth function of a mobile phone should not be used to send images or files to other mobile phones.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Procedures

1. To minimise any risks, all personal mobiles must not be used where children are present. This applies to shared use of rooms where non-setting staff may be present at the start of the session, for example an out of school club using a classroom with teaching staff present.

2. Staff must ensure safe and secure storage of their personal belongings including mobile phones. It is recommended that personal mobile phones are security marked, password protected and insured. Each member of staff will be provided with a locker in which to store their mobile phone/personal belongings or a locked cupboard.

3. Visitors, including other professionals, contractors and parents/carers are made aware by signs and verbal reinforcement that they are not to use their mobile phone where children are present.

4. Under no circumstances are images, videos or audio recordings to be made by staff using personal phones without prior explicit written consent by the designated safeguarding lead. Only work-provided equipment will be used for this purpose.

5. Personal mobiles may be used in designated areas at break times.

6. Staff are advised to provide their work place contact number to their family members, own children's schools/settings for use in the event of an emergency.

To assist in their day to day duties, there are designated members of staff who are authorised to carry their mobile phones around school. The procedures listed above are applicable to these individuals with the exception of point 2 (storage).

Members of staff authorised to carry mobile phones around school:

Gordon McBurnie (Headteacher)
Tania Harrison (Headteacher/Deputy Headteacher
Lee Heath (Site Manager)

Use of cameras

- Personal cameras or video recorders should not be used to record classroom activities. School equipment only should be used.
- Photographs and recordings can only be transferred to and stored on a school computer/IPad or laptop before printing.
- Personal cameras and video recording equipment cannot be used when in the presence of children on school premises unless authorised by the headteacher for school assemblies, productions and sports days.
- In the case of school assemblies, productions and sports day, parents/carers are permitted to take photographs/video footage in accordance with school protocols but we strongly advise against the publication of any such photographs on social networking sites.

1.5 Communication Policy

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- An Online Safety Curriculum 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 Online Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Online Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Online 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 Online Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- The Online 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.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school prospectus and on the school website. An updated link is available for parents to keep up to date with Online Safety trends/issues is published on the school website.
- CEOP button is also on the school website should parents need to report any suspicious occurrences.
- A partnership approach to Online 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 Online Safety at other attended events e.g. parent evenings and sports days.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.

E-Safety Contacts and References

KCSIE:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1181955/Keeping_children_safe_in_education_2023.pdf

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

e–Safety Officer: Children's Safeguards Team, Families and Social Care, Kent County Council. The e-Safety Officer is Rebecca Avery email: esafetyofficer@kent.gov.uk
Tel: 01622 221469

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Officer for Training & Development, Children's Safeguards Team, Families and Social Care, Staffordshire County Council.

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

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.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