Curriculum

Online Safety Policy

Document Title	E Safety Policy
Policy Status	
Date of Issue	February 2026
Date to be Revised	February 2027

Approved_____

Kent County Council believes that the use of information and communication technologies in schools brings great benefits. Recognising the Online Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

This Online Safety Policy has been revised by the Online Safety Coordinator, building on Kent County Council (KCC) guidelines as well as the OFSTED Document. It has been agreed by the senior management and the School's Governing Body.

This Online Safety document is drawn up to protect all parties- the pupils, the parents/Carers, the staff and the school - and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Kent County Council with Schools, Academies, Connexions Kent and Medway, Children's Safeguards Team, EIS, Youth Service, Libraries, SEGfL and Kent Police. www.kent.gov.uk

The school has appointed **Mrs Holly Bellars as the Online Coordinator for Singlewell School.**

The Online Safety Policy and its implementation will be reviewed annually.

Approved_____

Contents:

Introduction

- Online Safety at Singlewell School
- Overview of technologies at Singlewell School
- Overview of roles and responsibilities for Online Safety at Singlewell School

Guidance for Staff and Visitors to Singlewell School

- A Quick Guide – Safe use of the Internet and Email at Singlewell School
- A Quick Guide – Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Use of mobile phones
- A Quick Guide – Safe use of School network, equipment and data
- A Quick Guide – Safe use of iPads at Singlewell School
- Guidance – What to do if? – Reporting Procedures
- Parents Information
- Prevent Strategy
- Use of Data in school by staff
- Online safety contacts and references

Approved_____

Online Safety at Singlewell

In today's society, children, young people and adults interact with technologies such as mobile phones, tablets, 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.

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Schools 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.

Breaches of an Online Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing body.

The Online Safety policy is essential in setting out how the school plans to develop and establish its Online Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. The current and emerging technologies that children at Singlewell School have access to when using the internet at School includes:

Overview of Technology at Singlewell

Technology used at Singlewell Primary School is recorded on an up-to-date list, found on the school asset register.

It is the duty of the school to ensure that every child in their care is safe and the same principles should apply to the "virtual" or digital world as would be applied to the physical buildings.

More importantly, in many cases, children at Singlewell School are using the technologies outside of school and it is the duty of the school to educate our pupils and parents/carers to ensure that every child is equipped with the knowledge to know how to be safe when entering the digital or virtual world.

Approved_____

- The internet
- Email
- Social networking sites
- Instant messaging
- Blogs (an online interactive diary)
- Podcasting – radio/audio broadcast downloaded to computer or MP3/4 player
- Gaming Sites
- Video Broadcasting sites
- Chat Rooms
- Music streaming and download sites
- Mobile/smart phones/tablets with camera and video functionality, email and web access
- Mobile technology e.g. games consoles that are "internet ready" – Xbox, PlayStation, Nintendo

Accessing the Policy and Guidance

All the following guides are available on request from Singlewell School or can be downloaded from the "Policies" section on https://www.singlewell.kent.sch.uk/

Contact details for questions about this Policy and Guidance

If you have any questions about Online Safety or the content of this policy please contact the Online Safety Coordinator via office@singlewell.kent.sch.uk

If you have any questions about cyberbullying, safeguarding, or child protection, please contact the Head Teacher – Mrs R Catt who is the designated person for Child Protection and Safeguarding headteacher@singlewell.kent.sch.uk .

Safeguarding Roles and Responsibilities

Contact Name	Key Area of Responsibility
Headteacher **Mrs R Catt**	Overall responsibility for Safeguarding, Confidentiality, Data Security and Whistle Blowing
Headteacher **Mrs R Catt**	Child Protection and Safeguarding Designated Person for Looked After Children
Headteacher **Mrs R Catt**	Anti-Bullying and Behaviour
Mr J Howe	Governors with Specific responsibility for Safeguarding
Mrs H Bellars	Online Safety Coordinator • Ensures they keep up to date with Online Safety issues and guidance though liaison with the Local Authority Online Safety Coordinator and through organisations such as The Child Exploitation and Online Protection (CEOP). • Ensures the Head, Senior Management and Governors are updated as necessary.

Approved_____

Headteacher **Mrs R Catt** **SBM** **Miss Mason**	Health and Safety, School Security and Risk Assessment Disposal of Equipment
Mr G Kersey	Governor with specific responsibility for Health and Safety
All Governors	Governors need to have an overview understanding of Online Safety issues and strategies at this school. We ensure our Governors are aware of our local and national guidance on Online Safety and are updated at least annually on policy developments.
Cantium IT services	Manages pupil email accounts
Mrs H Bellars	Computing Coordinator Point of contact for teachers, regarding OnlineSafety and Computing teaching resources
All Staff (Teachers, Office and Administration Staff, Other Adults with a responsibility of care for pupils)	All staff are responsible for promoting and supporting safe behaviours in their classrooms/offices and following school Online Safety procedures. Central to this is fostering a "No Blame" culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Online Safety within the Curriculum:

At Singlewell Primary School, we are committed to providing a robust and comprehensive online safety education for all our pupils. To support this, we use the ***Purple Mash 2Be Safe*** curriculum. 2BeSafe is an online safety scheme of work, published by 2Simple, to meet the guidance set out within the Department for Education's - Education for a Connected World. The Education for a Connected World framework outlines eight key areas which seek to equip children and young people for digital life and the digital world. 2Simple's 2BeSafe offers a comprehensive coverage of these requirements for primary schools starting from Reception up to Year 6. The curriculum explicitly covers eight key areas: Self-Image and Identity, Online Bullying, Online Relationships, Online Reputation, Managing Online Information, Health and Wellbeing, Privacy and Security, and Copyright and Ownership. These areas are taught progressively across all year groups, every year, ensuring that pupils build knowledge and skills in a consistent and age-appropriate way as they move through the school.

A QUICK GUIDE – Safe use of the Internet and Email at Singlewell School

Internet at Singlewell

Internet is provided through EIS who have in place safety procedures such as filtering and monitoring for inappropriate websites, inappropriate images and misuse of the Internet in school. If any child is made aware of any inappropriate content, they should report this to their teacher immediately so that the correct actions can be taken.

Internet use is part of the statutory curriculum and is a necessary tool for learning. It is also a part of everyday life for education, business and social interaction. The school has a duty to provide

students with quality Internet access as part of their learning experience and as pupils use the Internet widely outside of the school setting they need to learn how to evaluate Internet information and to take care of their own safety and security. The school's Internet access will be designed to enhance and extend education and pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Email at Singlewell

For external email, there is no need for pupils to use individual accounts. A 'class' email address should be set up, and moderated by the teacher or via Purple Mash.

Primary aged pupils should not be using web-based email systems that are not moderated by the school and not approved by KCC. This includes email systems such as Hotmail or Google mail as these could allow children to exchange potentially inappropriate content without school knowledge. Staff should not use home email accounts for school business. The Kent Learning Zone offers free email accounts to all staff in KCC primary schools. Staff are not permitted to use personal email accounts for school business. Schools should ensure that more than one person has overall access to school email administrator accounts to avoid difficulties arising from staff being on leave, absent or no longer working with the school. All classes can have a class email address, linked to the teachers' email account. This can be used to email out class projects. If access to this is needed, it will be sent out by the school.

Pupils are NOT permitted to have access to other email accounts, such as Gmail, Yahoo, Hotmail etc whilst on school premises.

Pupils are NOT permitted to have access to social networking sites or instant messaging sites such as Facebook, Twitter, Instagram, WhatsApp, Snapchat whilst on school premises.

Blogging, Podcasting and Video Conferencing at Singlewell

All staff and pupils are provided with a Purple Mash login which gives them access to school resources. These resources include a safe online blogging resource, a safe online podcasting resource and a safe online video conferencing resource for schools. Teachers are able to easily monitor and filter content.

Safe use of the Internet or Email for Everyone

- Staff, visitors and pupils must not allow unauthorised individuals to access email/Internet/Network, or other school systems.
- The web address of any unsuitable websites accidentally accessed, or receipt of inappropriate materials, or filtering breach through the school network should be made known to the Computing Network Manager. The school will work with Kent County Council and the School's Broadband team to ensure that filtering policy is continually reviewed and that all sites on the Internet Watch Foundation (IWF) List are blocked.
- Do not attempt to view websites which might be considered inappropriate. These such sites would include those relating to illegal activity.
- Be polite – never send or encourage others to send abusive messages and do not send anonymous messages.
- Use appropriate language – do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.

Approved_____

- Privacy – do not reveal any personal information e.g. home address, telephone number – about yourself or others.
- Passwords – do not reveal your password to anyone. If you think someone has learned it then contact the Computing Network Manager.
- Do not copy or look at and delete other people's files or folders.
- Electronic Mail is not guaranteed to be private. Staff must only use the approved KLZ mail, school VLE or other approved school communication systems with pupils or parents/carers and only communicate with them on appropriate and professional business.
- Do not upload inappropriate images of self or others into profiles or send in emails.
- Please report all incidents involving inappropriate materials or images, the illegal use of mobile phones, acts of cyber bullying that may affect a child, a member of staff or a visitor to Singlewell, or any other specified online safety incident. Failure to do so may result in professional sanctions.
- Do not download or install files or software from the Internet, USBs and CDs from outside of school without permission from the Computing Network Manager.
- It is the responsibility of the user (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document and to ensure that unacceptable use of the Internet does not occur.

If any of the above rules are deliberately broken, the person breaking the rules will be suspended from using the computers on the Network and the Internet from Singlewell School.

Additional Safe use of Internet and Email Specifically for Pupils

- Pupils will not be allowed access to the Internet in school unless supervised by a responsible adult.
- Pupils should ask permission before entering any website or using a search engine unless their teacher has already approved that site/search engine.
- Pupils will not be allowed access to unsupervised and/or chat rooms and should not attempt to gain access to them.

If any of the above rules are deliberately broken, the person breaking the rules will be suspended from using the computers on the network and the Internet at Singlewell School.

A QUICK GUIDE – Safe use of digital images and digital technologies, such as mobile phones, digital cameras and iPads, including publication of pupil information/photographs/video and use of website;

Images and Videos

- Digital permission via a school agreement form must be obtained from parents and carers before any photographs or videos can be used:
  On the School's Learning Platform – Purple Mash
  On the School's Website – https://www.singlewell.kent.sch.uk/
  In display material in and around the school or off site

Approved_____

In the School Prospectus or other printed promotional material

- Images of pupils and staff will be retained by the school to show good practice and for use on the school website, school prospectus or VLE unless specifically requested to be removed by a parent/carer, member of staff or person involved.
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications you should check with individual parents that they gave permission for this additional use.
- Where images are used online or in any published school produced video materials/DVDs pupils will not be identified by name.
- Pupils' names will not be used when saving images in the file names or in the tags when publishing to the school website.
- Staff and pupils sign the school's ICT and Internet Acceptable Use Policy Agreement form which includes a clause on mobile phones/personal equipment for taking pictures and videos.
- Pupils and staff will ONLY use school equipment to create digital images and videos involving members of Singlewell School.
- Digital images and videos of pupils are stored in a central location making it easy to remove photos of children who have left the school.
- Parents may take photographs or videos at school events but must ensure that if they include children other than their own, it is solely for their personal use and will not be published on the internet, including social networking sites.

Use of Mobile Phones

Pupils

Pupils are encouraged not to bring mobile phones to school unless there are exceptional circumstances. These mobile phones must be handed in to the class teacher at the beginning of the day for safe keeping and only returned at the end of the school day. The class teacher holds no responsibility for the security of devices under their supervision.

Staff

Staff are permitted to have their mobile phones on at school in case they have dependants who need to contact them and for work communication. Staff are asked to use their mobiles with discretion and avoid using their mobile phones in the presence of pupils unless warranted i.e. a school trip. The use of mobile phones during the lesson times is not permitted and phones should be on a silent mode.

Staff are not permitted to use their mobile phones to take, transfer or store photos or videos of pupils or other staff at the school.

Students, Visitors and Volunteers

Student, visitors and volunteers are not permitted to carry mobile phones on them whilst working with pupils. When pupils are in the classroom, they should be kept in the classroom cupboard, along with other belongings. Students, visitors and volunteers are not permitted to use their mobile phones to take, transfer or store photos or videos of pupils or other staff at the school. If photographs are needed for coursework or other reasons, this should be discussed with the Online Safety coordinator or Mrs R Catt – Child Protection Officer.

Approved_____

QUICK GUIDE – Safe use of School Network, Equipment and Data

- Computers and other devices such as cameras, scanners, digital microscopes, visualizers, Interactive Smartboards and iPads are available for all staff to use (with pupils) in school. All users are expected to respect the equipment and immediately report any damage to the Computing Network Manager.
- Equipment must not be removed from the school without permission of the Computing Network Manager.
- PASSWORDS – Do not reveal your login password to anyone. If you think someone has learned your password, please contact the Computing Network Manager. All passwords require change every term and you will be reminded of this via an electronic message.
- TRESSPASSING – Do not trespass into other users' files or folders.
- DISRUPTIONS – Do not use the network in any way that would disrupt use of the network by others.
- All pupils and staff will be made aware of the hazards of using electronic and electrical equipment.
- All pupils have read, discussed with their teacher and signed an Acceptable Use Policy.
- All staff have read and signed an Acceptable Use Policy.

Safe Use of School Laptops

- All laptops remain the property of Singlewell School and are only for the use of the member of staff that it has been assigned to.
- Only software licensed by the school, authorised by the Headteacher and installed by the school's Computing staff may be used.
- Anti-virus software is installed and will update automatically when the laptop is connected to the Internet.
- Should any faults occur, the school must be advised as soon as possible.
- All staff must follow the use of the Internet and Email guidelines as outlined in the policy above.

A QUICK GUIDE – Safe use of School iPads

- iPads are available for all staff to use with pupils in school.
- All users are expected to respect the iPads and immediately report any damage to the Computing Network Manager.
- iPads should be kept within their Griffin cases at all times to restrict the impact of wear and tear.
- iPads are currently stored in a GoCabby charging Units in the Server Room and storage units in KS2 classrooms.
- If you wish to download apps, please discuss this with the Computing Coordinator and allow for a one week time period to complete installation.
- Return the iPads as soon as your session is over and place them back on a trolley for charging.
- The Go Cabby charging trolleys are kept in classrooms overnight and can locked for extra security.

Approved_____

- School passwords and usernames will be the same across the whole network.
- You will be able to access all work from any piece of computing software with an internet connection. This is possible through the Apple Mini Mac Server.

Staff iPads

- Staff are provided with iPads to use in the classroom.
- Staff are required to hand their iPads to the Computing Lead regularly for updating.
- Staff ipads have a pin code set up on them to ensure data stored on them is kept safe.
- Staff are also required to bring their iPads to staff meetings for training when required.
- All pupil iPads should be locked away safely each evening.
- Early Years mini iPads need to in the iPad trolley and locked away each evening.

What to do if? – Reporting Procedures

How Singlewell School handles complaints regarding Online Safety

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions.
- Sanctions available include:
- Conversation with class teacher
- Conversation with Online Safety Officer
- Conversation with Headteacher
- Informing Parents/Carers
- Removal of Internet or computer access for a period of time
- Referral to Local Authority/ County Online Safety Officer/Police

Our Online Safety Coordinator acts as our first point of contact for any Online Safety complaint and incidents will be recorded by the school using our Online Safety Incident Form, including any action taken. Complaints about Internet misuse will be dealt with under the School's complaints procedure.
Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti Bullying Policy.

Complaints related to Child Protection are dealt with in accordance with school/LA Child protection procedures.

All policies are available to download from http://www.singlewell.kent.sch.uk under the "Policies" section or on request from the school office

Parents

Parents and carers form a vital element in the approach to teaching and empowering children to become safe and responsible digital citizens.

Approved_____

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. Technology can sometimes be seen as a "scary" or "frightening" issue to many adults and using the words such as "ICT" and "Technology" can sometimes put parents/carers off attending Online Safety events as they may be concerned about not having sufficient computer skills to help protect their child. Online safety or "Online Safety" is not about technology skills, it is about keeping children safe online and so parenting skills and communication and not computing/technology are the most important thing.

Sometimes families may think they are doing enough to protect their children by putting filters on search engines, installing antivirus software, having a laptop downstairs and banning children from using certain sites without considering how successful these tools are or if their children could access the internet elsewhere, so it is important to highlight that discussion and education about safe use is the key.

It is important that schools/settings focus on the importance of keeping children safe online and that online safety is not seen as a purely ICT issue. By working together, parents and carers, schools/settings and other professionals can help to reinforce online safety messages and can encourage positive behaviour wherever and whenever children go online.

Awareness-raising with families should focus on:

- The range of different ways children and young people use and access technology e.g. mobile phones, games consoles, tablets and apps etc. not just laptops and computers.
- The many positive uses of technology as otherwise online safety can easily become frightening and scaremongering so be aware that the vast majority of interactions and experiences on the internet are positive!
- The importance of developing risk awareness and risk management by children and young people (according to their age and ability) and resources parents/carers can use to help discuss online safety
- Practical tips for online safety in the home such as using filters, parental controls, creating appropriate user profiles and home computer security

The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy. One strategy is to help parents to understand more about ICT, perhaps by running courses and parent awareness sessions (although the resource implications will need to be considered) and providing information regarding online safety through a variety of channels.

Additional information including ideas and supporting resources to help schools and settings engage parents/carers in online safety can be found at http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety

What can parents/carers do to help children keep safe online?
Follow the Golden Rules

Ground Rules

- Discuss together as a family how the internet will be used in your house. Consider what information should be kept private (such as personal information, photos in school uniform etc) and decide rules for making and meeting online friends. Ensure your children know the risks of

accepting 'friend' requests from strangers online and make sure you know what your child is doing online much like you would offline. Make sure your child uses strong passwords to protect their online accounts. It is important they know they need to keep their passwords safe and not share them with anyone or use the same password for several accounts.

- Consider locating your child's computers and laptops in a family area but be aware that children access the internet on mobile phones, games consoles and tablets so use can't always be supervised.
- Be especially aware of settings rules relating to your child's use of webcams and any applications or devices which allow voice or video chat. Childnet have useful information for young people about using webcams safely www.childnet.com/young-people/secondary/hot-topics/video-chat-and-webcams

Online Safety

- Install antivirus software, secure your internet connection and use Parental Control functions for computers, mobile phones and games consoles to block unsuitable content or contact from unknown people. Research different parental control software and tools available for your home and select the tools which are most suitable to you, your child and the technology in your home. Visit www.internetmatters.org and www.saferinternet.org.uk/advice-and-resources/a-parents-guide for safety information and advice about parental controls on consoles and devices and how to report concerns.
- Make sure you read any parental guidance and safety recommendations (including age requirements – most popular social networking sites and apps are only for users aged 13+) for any apps or websites before allowing your child to use them - visit www.net-aware.org.uk
- Always remember that parental control tools are not always 100% effective and sometimes unsuitable content can get past them, so don't rely on them alone to protect your child.

Listen

- Take an active interest in your child's life online and talk openly with them about the things they do. Talk to your child and ask them to show or even teach you how they use the internet, learn which websites or tools they like to use and why. Learning together with your child can often open opportunities to discuss safe behaviour online.
- To start a conversation with your child you could tell them that you understand that some young people share images and videos online and that you're interested to know what they think about it and how they think they can keep themselves safe.

Dialogue – keep talking

- Ensure that your child knows that once a picture, video or comment is sent or posted online, then it can be very difficult to remove as other people can forward it and share it with others, without them even knowing.
- www.childnet.com and www.thinkuknow.co.uk has some really useful tips and ideas for parents/carers about starting conversations about online safety
- Always ensure your child knows how to report and block people online who may send nasty or inappropriate messages or content. Encourage your child not to retaliate or reply to cyberbullying and to keep any evidence.
- Make sure your child knows it's important that they tell an adult they trust if anything happens online that makes them feel scared, worried or uncomfortable.

Remember, the internet is an essential part of young people's lives and provides them with tremendous opportunities. The vast majority use it without coming to any harm so it's essential to

be realistic: banning the internet or web sites often will not work and it can make a child feel less able to report a problem or concern, so education around safe use is essential.

Prevent Strategy 2015

Procedures for Responding to Specific Online Incidents or Concerns

The following content is provided to enable schools and education settings to make appropriate safeguarding decisions reading online safety concerns and has been written by the Kent e-Safety Strategy Group with input from specialist services and teams. This content is not exhaustive and cannot cover every eventually so professional judgement and support from appropriate agencies such as the Education Safeguarding Team, Police, CSET and Children's Social Care is encouraged.

Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

Singlewell Primary School ensure that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating incident images of children (known as "sexting").

The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

Singlewell Primary School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead Mrs M Brown, Headteacher).

If the school is made aware of an incident involving indecent images of a child the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Board's procedures.
- Immediately notify the designated safeguarding lead.
- Store the device securely.
- Carry out a risk assessment in relation to the pupils involved.
- Consider the vulnerabilities of pupils involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.

The school will not view the image unless there is a clear need or reason to do so.

The school will not send, share or save indecent images of children and will not allow or request children to do so.

If an indecent image has been taken or shared on the school/settings network or devices, then the school will take action to block access to all users and isolate the image.

The school will need to involve or consult the police if images are considered to be illegal.

Approved_____

The school will take action regarding indecent images, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

The school will follow the guidance (including the decision making flow chart and risk assessment template) as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it".
The school will ensure that all members of the community are aware of sources of support.

Responding to concerns regarding Online Child Sexual Abuse

Singlewell Primary School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
Singlewell Primary School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
If the school is made aware of an incident involving online child sexual abuse of a child, then the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Board's procedures.
- Immediately notify the designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform Kent police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.

Approved_____

- If pupils at other schools are believed to have been targeted, then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

Responding to concerns regarding Indecent Images of Children (IIOC)

Singlewell Primary School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

The school will take action regarding Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
The school will take action to prevent accidental access to Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Board's procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the school is made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, then the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via https://www.iwf.org.uk/
    - Ensure that any copies that exist of the image, for example in emails, are deleted.

- If the school is made aware that indecent images of children have been found on the school's electronic devices, then the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via https://www.iwf.org.uk/
    - Ensure that any copies that exist of the image, for example in emails, are deleted.

Approved_____

- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

- If the school is made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school's managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation or extremism online

Radicalisation/extremism may be ethnic, social, political or religious extremism. The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of pupils.
When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of Singlewell Primary School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

All incidents of online bullying reported will be recorded on CPOMS and DSLs notified.
There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
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 act appropriately. 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 Online Safety ethos.

- Sanctions for those involved in online or cyberbullying may include:
  - Those involved will be asked to remove any material deemed to be inappropriate or offensive.

- A service provider may be contacted to remove content if those involved refuse to or are 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 involved in online bullying will be informed.
- The Police will be contacted if a criminal offence is suspected.

Use of Data and Flash Drives and Cloud-based storage

The school recognises the benefits of using external devices to allow for remote working (USB, flash drives Office 365 etc).

This policy aims to help staff use these technologies in a fitting manner. Practical advice is offered wherever possible, although it should be considered that advice on technical issues can quickly become obsolete.

If using a USB flash drive, staff must ensure that they are encrypted. This means that all data is password protected and cannot be compromised in the event of the loss or theft of the flash drive. Staff also have access to their own Office 365 account where they can save and share files securely and the use of this is encouraged as it represents the safest format.

Any USB flash drives provided by the school will be marked and individual passwords will be set for each one. These passwords will be logged and should not be changed. **Under no circumstances should the encryption be removed from the device.**

Staff shall take all necessary precautions to protect against loss or theft. Users shall report missing or stolen devices to the school office and the computing post-holder as soon as possible. If the missing or stolen property is known to contain restricted information, the requirement to report shall be immediate and you will be requested to complete a form regarding the missing device.

In the event of the USB being lost, broken or stolen you must inform the school office **immediately.** If you leave the setting the USB (if provided by the school) must be returned to the school office.

If left in the school, all external devices should be locked away in the school office or stored securely in the classroom.

Staff are reminded of their personal responsibility to only use external drive devices for work purposes if they are free from viruses. Please note that staff risk having all the files on external drive devices deleted if any viruses are detected.

Copying Files to USB-Attached Storage Devices

Approved_____

Only files relevant can be copied. Relevant files would include files in a staff member's file space which they have produced and files in others' file space to which they have been granted permission to copy.

If the external drive is used for transitional storage (for example copying data between systems), the data shall be securely deleted from the device immediately upon completion.

Staff are reminded to back up their work on a regular basis so that in the event of their external drive being lost or damaged their files are safe and that it is recommended to use their Office 365 cloud account.

Staff must not use their own personal (containing personal documents) USBs to store or transfer school data and it is encouraged that they use their Office 365 accounts to save and access documents remotely.

Online-Safety Contacts and References

Kent County Councils Education Safeguards Team: www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
Kent Online Safety Support for Education Settings
Rebecca Avery, Education Safeguarding Adviser (Online Protection)
Ashley Gorton, e-Safety Development Officer
esafetyofficer@kent.gov.uk Tel: 03000 415797

Kent Police: www.kent.police.uk In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101
Kent Public Service Network (KPSN): www.kpsn.net
Kent Safeguarding Children Board (KSCB): www.kscb.org.uk
Kent e-Safety Blog: www.kentesafety.wordpress.com
EIS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk
National Links and Resources
Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): https://www.iwf.org.uk/
Lucy Faithfull Foundation: www.lucyfaithfull.org
Know the Net: www.knowthenet.org.uk
Net Aware: www.net-aware.org.uk
NSPCC: www.nspcc.org.uk/onlinesafety
Parent Port: www.parentport.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
Think U Know: www.thinkuknow.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
UK Safer Internet Centre: www.saferinternet.org.uk

Approved_____

360 Safe Self-Review tool for schools: https://360safe.org.uk/
Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/

Approved_____

Online Safety Incident Form

Signed: ..... Date: .....

Printed Name: .....

Schools Online Safety Audit

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

Has the school an Online Safety Policy that complies with Kent guidance?	Y/N
Date of latest update:	
Date of future review:	
The school Online 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 Online Safety is:	
The Designated Child Protection Coordinator is:	
The Online Safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school Online Safety Policy?	Y/N
Has up-to-date Online 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?	Y/N
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 Online Safety incident of concern?	Y/N
Have Online Safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y/N
Is Online Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are Online 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

Approved_____

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 Online Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the school Online Safety policy and ethos on a regular basis?	Y/N

Approved_____

Letter for parents/carers

Dear Parent/Carer

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- School learning platform/intranet
- Email
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones
- Mobile Phones and Smartphones

Singlewell Primary School recognise the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However, we also recognise there are potential risks involved when using online technology and therefore have developed online safety policies and procedures alongside the school's safeguarding measures.

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. However, no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the school's internet and ICT facilities.

Full details of the school's Acceptable Use Policy and online safety policy are available on the school website www.singlewell.kent.sch.uk or on request.

We request that all parents/carers support the school's approach to online safety by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers can visit the school website www.singlewell.kent.sch.uk for more information about the school's approach to online safety as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online

Whilst the school monitors and manages technology use in school we believe that children themselves have an important role in developing responsible online behaviours. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child and that you and your child discuss the content and return the attached slip. Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

Should you wish to discuss the matter further, please do not hesitate to contact the school's Online Safety Co-ordinator Mr Evans or myself.

We understand that your child is too young to give informed consent on his/her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

Yours sincerely

Mrs B Catt
Headteacher

Approved_____

Pupil Acceptable Use Policy – Singlewell Primary School Parental Acknowledgment

I, with my child, have read and discussed Singlewell school Pupil Acceptable Use Policy.

I am aware that any internet and computer use using school equipment may be monitored for safety and security reason to safeguard both my child and the school's systems. This monitoring will take place in accordance with data protection and human rights legislation.

I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school will take all reasonable precautions to reduce and remove risks but cannot ultimately be held responsible for the content of materials accessed through the Internet and the school is not liable for any damages arising from use of the Internet facilities.

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child's safety.

I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.

I know that my child will receive, Online Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will support the schools Online Safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

Child's Name…….

Class……..……..

Parent's Signature…….

Parent's Name…….…….....

Date…….

Approved_____