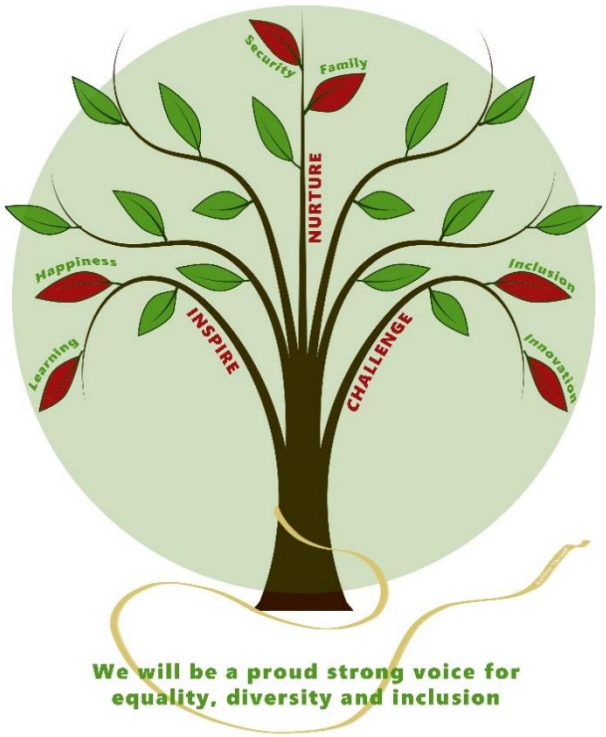
Dormansland Primary School



Online Safety Policy 2023/24

Date adopted	Autumn 2023	Next review due	Autumn 2024
Review period	Annual	Status	Non-Statutory
Written by	Mark Cook	Governor review by	Marie Langer

Introduction:

Online Safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour management, safeguarding and child protection, anti-bullying, computing, data protection and the use of photographic images.

The purpose of this policy is to:

- Safeguard and protect all members of the school community in the use of computers and other devices and the internet.
- Identify approaches to educate and raise awareness of online safety throughout the school's community.
- Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Using this policy

- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by governors.
- The Online Safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes, but is not limited to, workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.

The Designated Safeguarding Lead (DSL) and online safety lead will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Deputy Safeguarding Leads, the Safeguarding and E Safety governor and the governing body.
- Work with governors and staff to review and update online safety policies.
- Meet regularly with the governor with a lead responsibility for safeguarding.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of Conduct /Acceptable Use Policy for staff and governors.

- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety procedures.
- Read and adhere to this Online Safety Policy, the Safeguarding and Child Protection Policy, the ICT Code of Conduct /Acceptable Use Policy and the Staff Code of Conduct.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education into the curriculum.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

It is the responsibility of the Headteacher to:

- When required, develop and implement appropriate online safety policies and procedures.
- Implement appropriate security measures to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Investigate any filtering breaches and ensure that any safeguarding concerns, identified through monitoring or filtering breaches are dealt with appropriately.
- Monitor the on-line activity of staff and pupils and deal with any issues as appropriate.
- Ensure that staff adhere to this this Online Safety Policy, the Safeguarding and Child Protection Policy, the ICT Code of Conduct and the Staff Code of Conduct.

It is the responsibility the school's technical support company to:

- Provide technical support and perspective to the school, especially in the development and implementation of appropriate online safety policies and procedures.

- Implement appropriate security measures, including password policies and encryption, to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.

Pupils are taught to:

- Engage in age appropriate online safety education opportunities under the direct supervision of school staff. Understand child-friendly online safety procedures during curriculum and teaching time.
- Read and adhere to the school's pupil-friendly Acceptable Use agreements
- Seek help from a trusted adult if they experience an on-line concern.

It is the responsibility of governors to:

- Hold the school to account to ensure that robust safeguarding, Online Safety and on-line procedures and policies are in place and are being adhered to.
- Undertake safeguarding and child protection training that includes on-line and Online Safety training.
- Read and adhere to this policy and to the school's Acceptable Use Policy.

It is the responsibility of parents and carers to:

- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement statements that relate to the use of social media and other Online Safety issues.
- Identify changes in behaviour that could indicate that their child is at risk of harm online. If appropriate parents should inform the school for extra support and advice.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Education and engagement with pupils.

The school will establish and embed a progressive online safety curriculum throughout the whole school to raise awareness and promote safe and responsible internet use amongst pupils by:-

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the Personal, Social and Health Education (PSHE) and Computing programmes of study, covering use both at home school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.

- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

Vulnerable Pupils

- Dormansland Primary School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Dormansland Primary School will ensure that differentiated and ability appropriate online safety education, access, monitoring and support is provided to vulnerable pupils.

Training and engagement with staff

The school will:

- Provide and discuss the online safety with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This training will be part of the annual safeguarding and child protection training or part of regular safeguarding updates throughout the year. The training will cover the potential risks posed to pupils as well as professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Awareness and engagement with parents and carers

- Dormansland Primary School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings or transition events.
    - Drawing their attention to the school online safety policy, procedures and expectations.

Reducing Online Risks

Dormansland Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's Acceptable Use Policy and codes of conduct and highlighted through a variety of updates and training approaches

Classroom and ICT Suite Use

- Dormansland Primary School uses a wide range of technology. This includes access to:
    - Computers, laptops, ipads and chromebooks
    - Internet which may include search engines and educational websites.
    - Tablet and computer based educational applications and games.
    - Digital cameras, web cams and video cameras.
    - Programmable robots and toys.

- Members of staff will always evaluate websites, games and apps fully before use in the classroom/ICT Suite or recommending for use at home.
- The school will use the age appropriate search engine called '*Junior Safe Search for Kids'.*
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Pupils' access to the internet will be by adult demonstration, with directly supervised access to specific and approved online materials, which support the learning outcomes planned for the pupils' age and ability.
- Pupils will be taught not to give out personal details or information which may identify them or their location.
- The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

Filtering and Monitoring

- The Headteacher and governors have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.

- The Headteacher and governors are aware of the need to prevent “over blocking”, as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- Changes to the filtering and monitoring approach will be risk assessed by the Headteacher.
- The Headteacher will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. The outcomes of this monitoring will be reported to governors.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils and that effective classroom management and regular education about safe and responsible use is essential.
- The school uses educational broadband connectivity through BT Unicorn.
- The school uses LGFL webscreen as a filtering system which blocks sites which can be categorised as: adult content (pornography), criminal activity, racial hatred, radicalisation and extremism, suicide and bullying
- The school works with LGFL (technical support) to ensure that our filtering policy is continually reviewed.

Dealing with filtering breaches

- The school has a clear procedure for reporting filtering breaches.
    - Any breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
    - If any members of staff discover unsuitable sites, they will report the concern to the DSL.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: The Internet Watch Foundation (IWF), Surrey Police or The Child Exploitation and Online Protection (CEOP).

Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by monitoring internet use through individual staff log-ins
- Any concerns identified via monitoring approaches will be reported to the DSL who will respond in line with the Safeguarding and Child Protection Policy and its procedures for dealing with allegations against members of staff.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.

- Encryption for personal data sent over the Internet or taken off site, for example via portable media storage or access via appropriate secure remote access systems.
- Not using portable media without specific permission from the Headteacher.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments. Any new software downloads have to be approved and agreed by the Headteacher.
- The appropriate use of user logins and passwords to access the school network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Passwords

All members of staff will have their own unique username and private passwords to access school systems and school emails. Governors have their own username and private passwords to access school emails. Governors and members of staff are responsible for keeping their passwords private.

- We require all users to:
  - Use strong passwords for access into our system.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE) and OFSTED.
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff, pupils' and governors' personal information will not be published on our website. The contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Managing Email

- Access to school email systems will always take place in accordance with data protection legislation and in line with this policy, and staff codes of conduct/Acceptable Use Policy.
  - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

        - School email addresses and other official contact details will not be used for setting up personal social media accounts.
    - Members of the school community will immediately tell the DSL if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
    - The use of personal email addresses by staff for any official school business is not permitted. All members of staff are provided with a specific school email address, to use for all official communication.

Social Media

- The expectations' regarding safe and responsible use of social media applies to all members of Dormansland Primary School community.
- The term social media may include, but is not limited to: blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Dormansland Primary School community are expected, at all times, to engage in social media in a positive, safe and responsible manner,
- Concerns regarding the online conduct of any member of Dormansland Primary School community on social media should be reported to the DSL and will be managed in accordance with the school's Anti-bullying, Allegations Against Staff, Behaviour and Safeguarding and Child protection policies.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff, governors and volunteers as part of induction and will be revisited and communicated via regular training opportunities for staff.
- Safe and professional behaviour will be outlined for all members of staff, governors and volunteers as part of the school's codes of conduct and acceptable use policies.
- All members of staff, governors and volunteers are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may 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.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include but is not limited to
    - Setting the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the school.

- Members of staff are encouraged not to identify themselves as employees of Dormansland Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and governors.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
    - Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the DSL immediately if they consider that any content shared on social media sites conflicts with their role in the school.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted.

Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

Official School Use of Social Media

- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
    - The Headteacher and the Administration Officer have access to account information and login details for the social media channels.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use school provided email addresses to register for and manage any official school social media channels.
    - Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
    - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will be informed of any official social media use with pupils and written parental consent will be obtained, as required.

The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Adhere to the school's Staff Code of Conduct and ICT Acceptable Use Policy.
    - Be professional at all times and aware that they are an ambassador for the school.
    - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
    - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
    - Ensure that they have appropriate written consent before posting images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
- Inform the Designated Safeguarding/ Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

Use of Personal Devices and Mobile Phones

- Dormansland Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for staff, governors, volunteers and parents/carers, but technologies need to be used safely and appropriately within school.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
- All members of Dormansland Primary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage. The school accepts no responsibility for the loss, theft or damage of such items on school premises.
- All members of Dormansland Primary School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the school's codes of conduct and acceptable use policies.
- All members of Dormansland Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be

considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Safeguarding and child protection policies.

- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Not use personal devices during teaching periods, unless permission has been given by the Headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead.
- Staff and governors will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of pupils and will only use school-provided equipment for this purpose.
    - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.

Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
    - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Surrey Safeguarding Children Partnership.
- Where there is suspicion that illegal activity has taken place, the school will contact the Surrey Safeguarding Children Partnership or Surrey Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Surrey Police and/or the Surrey Safeguarding Children Partnership first, to ensure that potential investigations are not compromised.

Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL will record these issues in line with the school's Safeguarding and child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Surrey Safeguarding Children Partnership thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the DSL/Headteacher, according to the Management of Allegations and Concerns Safeguarding and child protection and Whistleblowing policies.
- Any complaint about the Headteacher's on-line misuse will be referred to the Chair of Governors according to the Management of Allegations and Concerns, Safeguarding and child protection and Whistleblowing policies.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Youth Produced Sexual Imagery or "Sexting"

- Dormansland Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- Dormansland Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding pupil produced sexual imagery.

Dealing with 'Sexting'

- If the school are made aware of an incident involving the creation or distribution of pupil produced sexual imagery, the school will:
    - Act in accordance with our Safeguarding and child protection policy and the relevant Surrey Safeguarding Child Partnership's procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store the device securely.
        - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.

        - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
        - Inform parents and carers, if appropriate, about the incident and how it is being managed.
        - Make a referral to Specialist Children's Services and/or the Police, as appropriate.
        - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
        - Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
        - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
            - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
        - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will take action regarding pupil produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
    - View any images suspected of being pupil produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of children i.e. pupil produced sexual imagery and will not allow or request pupils to do so.

Online Child Sexual Abuse and Exploitation

- Dormansland Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Dormansland Primary School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
    - Act in accordance with the school's Safeguarding and child protection policy and the relevant Surrey Safeguarding Children Partnership's procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store any devices involved securely.
    - Immediately inform Surrey police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Make a referral to Specialist Children's Services (if required/ appropriate).
    - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented.
    - Review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Surrey Safeguarding Children Partnership and/or Surrey Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation on or offline, it will be passed through to Surrey Police by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Surrey Safeguarding Children Partnership and/or Surrey Police first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

- Dormansland Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Surrey Safeguarding Children Board and/or Surrey Police.
- If made aware of IIOC, the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant Surrey Safeguarding Children Partnership procedures.
- Immediately notify the school Designated Safeguard Lead.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Surrey police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, 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 www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, 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 www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - 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.
    - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
    - Ensure that the DSL/Headteacher is informed.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school's Safeguarding and child protection, Managing of Allegations and Concerns and Whistleblowing policies.
    - Quarantine any devices until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Dormansland Primary School.
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Dormansland Primary School and will be responded to in line with the school's Anti-bullying, Behaviour, Safeguarding and Child Protection and Whistleblowing policies.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Surrey Safeguarding Children Partnership and/or Surrey Police.

Online Radicalisation and 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.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Safeguarding and Child Protection Policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the DSL/ Headteacher will be informed immediately and action will be taken in line with the Safeguarding and Child Protection and Management of Allegations and Concerns Policies.

Links to other policies:

Positive Relationships Policy

Concerns and complaints

Anti-Bullying

Management of allegations against staff

Safeguarding and Child Protection

Equalities

Data Protection

Use of Photographic Images

ICT Code of Conduct/Acceptable Use

Staff Code of Conduct

Whistleblowing

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk

- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
    - ChildLine: www.childline.org.uk
    - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
    - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

360 Safe Self-Review tool for schools: www.360safe.org.uk