Palace Wood Primary School

Online Safety Policy

Written by	Model policy – adapted by Emma Newell
Ratified by Governors	Summer 2023
Date of Review	Summer 2024

Commented [IF1]: Seems this table has moved?

Creating an Online Safety Ethos

Aims and policy scope

- Palace Wood believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- Palace Wood identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- Palace Wood has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- Palace Wood identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.
- Palace Wood identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

- The purpose of Palace Wood's online safety policy is to:
    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that Palace Wood is a safe and secure environment.
    - Safeguard and protect all members of Palace Wood's community online.
    - Raise awareness and educate all members of Palace Wood's community regarding the potential risks as well as benefits of technology.
    - To enable all staff to work safely and responsibly to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff 'in this policy) as well as children and parents/carers. This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets, or mobile phones.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, mobile phone policy, Acceptable Use Policies.

Writing and reviewing the online safety policy

- This online safety policy has been written by Emma Newell, involving staff, pupils, and parents/carers, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.
- It considers the DfE statutory guidance "Keeping Children Safe in Education" 2022, Early Years and Foundation Stage 2021, Working Together to Safeguard Children 2018 and the Kent Safeguarding Children Board procedures.
- Palace Wood Primary School will review this policy at least annually
  - The policy will also be revised following any national or local policy requirements, any child protection concerns, or any changes to the technical infrastructure
- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

- The Designated Safeguarding Leads (DSL): Clare Cairns, Emma Newell, Becky Tye, Lynne Emmerson, Joe Burnett, Chloe Chidley and Amie-Jane Bryer

- The Online safety (e-Safety) lead for the Governing Body is Stuart Russell.

Key responsibilities for the community

The key responsibilities of the school/setting management and leadership team are:

- Developing, owning, and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Proactively developing a robust online safety culture.
- Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.

- Ensuring that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- Working with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date, and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school/setting 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, including ensuring the safe and responsible use of devices.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation, and trends regarding online safety.
- Ensuring staff receive regular, up-to-date, and appropriate online safety training
- Coordinating participation in local and national events to promote positive online behaviour, e.g., Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Working with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with Special Educational Needs (SEN) and disabilities face online.
- Monitoring the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need

- Reporting to the school management team, Governing Body, and other agencies as appropriate, on online safety concerns and local data/figures.
- Meeting every term with the governor with a lead responsibility for safeguarding and online safety.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with the school/setting leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.

1.3.3 The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- Ensuring that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school/setting's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded, and appropriate action is taken as advised.

- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 The key responsibilities of children and young people are:

- Engaging in age-appropriate online safety education opportunities
- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues. At a level that is appropriate to their individual age, ability, and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any technology and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Abiding by the school's home school agreement.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.

Commented [IF2]: Is this happening?

- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Education and Engagement Approaches

2.1 Education and engagement with learners

The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval, and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology through the school's behaviour policy.
- Implementing appropriate peer education approaches, such as Safety Surfers.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

> **Commented [IF3]:** Are theses in place in every classroom?

2.2 Vulnerable Learners

Palace Wood Primary School recognises that some learners are 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.

Palace Wood Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners based on an individual basis of need.

When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENCO.

2.3 Training and engagement with staff

We will:

Provide and discuss the online safety policy and procedures 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 will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.

Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.

Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.

Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.

Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues, or other members of the community.

2.4 Awareness and engagement with parents and carers

Palace Wood Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We 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, transition events, fetes, and sports days.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.

Requiring them to read our acceptable use policies and discuss the implications with their children.

Online Communication and Safer Use of Technology

3.1 Managing the school/setting website

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

3.2 Publishing images and videos online

- The school will ensure that all images and videos shared online are used in accordance with the school image use policy.
- The school will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

3.3 Managing email

- Pupils may only use school provided email accounts for educational purposes
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive or personal information) will only be sent using secure and encrypted email.
- Access to school /setting email systems will always take place in accordance with data protection legislation and in line with other appropriate school/setting policies e.g., confidentiality.
- Members of the community must immediately tell a DSL if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Whole -class or group email addresses may be used for communication outside of the school

- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

3.4 Official videoconferencing and webcam use for educational purposes

- We recognise that videoconferencing *and* use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing *and* webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
    - Videoconferencing contact details will not be posted publically.
    - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Users
- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities. Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

Content
- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.

- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

4 Safer Use of Technology

4.1 Reducing Online Risks

- Palace Wood 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 the setting 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 our computers or devices.
- All members of the community are made aware of our 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 our acceptable use policies and highlighted through a variety of education and training approaches.

4.2 Appropriate and safe classroom use of the internet and any associated devices
- Internet use is a key feature of educational access, and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- The school/setting's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability
  - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
  - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.

- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age-appropriate search tools (*Google Safe Search or CBBC safe search*) as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- 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 will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

4.3 Management of school learning platforms/portals/gateways

- Leaders/managers and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement. e) A pupil's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

5 *Use of Personal Devices and Mobile Phones*

5.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of Palace Wood community to take steps to ensure that mobile phones and personal devices are used responsibly.
- Palace Wood recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools/settings.

5.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones (and smart watches) will take place in accordance with the law and other appropriate school policies
- Electronic devices of all kinds that are brought in on site are always the responsibility of the user. The school/setting accepts no responsibility for the loss, theft, or damage of such items. Nor will the school/setting accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school/setting site such as changing rooms, toilets, and swimming pools.
- The sending of abusive or inappropriate messages or 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 discipline/behaviour policy.
- Members of staff will be issued with a work phone number (the office number) and email address where contact with pupils or parents/carers is required.
- All members of Palace Wood community will be advised to take steps to protect their mobile phones or devices from loss, theft, or damage.
- All members of Palace Wood community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of Palace Wood community will be 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/settings policies.
- School/setting mobile phones and devices must always be used in accordance with the Acceptable Use Policy
- School/setting mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

5.3 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people, and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets, or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g., data protection as well as relevant school policy and procedures e.g., confidentiality, data security, Acceptable Use etc
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school/setting policy, then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school/settings allegations management policy.

5.4 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school/settings acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

6   Managing Information Systems

6.1 Managing personal data online

- Personal data will be recorded, processed, transferred, and made available according to GDPR.
- Full information regarding the school's approach to data protection and information governance can be found in the school's information security policy.

6.2 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- All pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our system.
- We require staff to change their passwords every 3 months

6.3 Filtering and Monitoring

- The governorswill ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational, and safeguarding staff.

- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- 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.
- The school uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc. The school will work with KCC and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate. Parents/carers will be informed of filtering breaches involving their child.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.
- The school works with EIS to ensure that our filtering policy is continually reviewed.

6.4 Management of applications (apps) used to record children's progress

- The headteacher/manager is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Only school/setting issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the schools expectations regarding safe and appropriate use (e.g., not sharing passwords or sharing images) prior to being given access.

6.5 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).
- 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 or pupils' 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.

6.6 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the Image use policy, Data security, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones.

6.7 Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including Confidentiality, AUPs and Code of conduct.
    - .1 The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
    - .2 Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - .3 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 (designated member of staff and role) if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

6.71 Staff
- The use of personal email addresses by staff for any official school business is not permitted.
    - .1 All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents.

7 Social Media

7.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Palace Wood 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 Palace Wood Primary School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - .1   All members of Palace Wood Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
    - .2   Use of social media by staff during lessons or break duty is not permitted.
- Concerns regarding the online conduct of any member of Palace Wood Primary School community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protection policies.

7.2 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 as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.

Reputation
- All members of staff 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):
    - .1   Setting the privacy levels of their personal sites as strictly as they can.
    - .2   Being aware of location sharing services.
    - .3   Opting out of public listings on social networking sites.
    - .4   Logging out of accounts after use.
    - .5   Keeping passwords safe and confidential.
    - .6   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 Palace Wood 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.

- 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 school's policies and the wider professional and legal framework.
  - .1 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 Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

- *Communicating with pupils, parents, and carers*
- 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.
  - .1 Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.
  - .2 If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

7.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:
  - .1 To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
  - .2 To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
  - .3 Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.

.4 To use safe passwords.

.5 To use social media sites which are appropriate for their age and abilities.

.6 How to block and report unwanted communications and report concerns both within school and externally.

7.4 Official Use of Social Media

- Palace Wood Primary School official social media channels are:
    - .1 ***Twitter: @palace_wood***
    - .2 ***Facebook: Palace Wood Primary School***
- The official use of social media sites by the school only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - .1 The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
    - .2 Leadership staff 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.
    - .1 Staff use school provided email addresses to register for and manage any official school social media channels.
    - .2 Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
    - .3 Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including Anti-bullying, Image use, Data protection, Confidentiality and Safeguarding.
    - .1 All communication on official social media platforms will be clear, transparent and open to scrutiny.
- 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.
    - .1 Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - .2 Any official social media activity involving pupils will be moderated by the school where possible
- 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

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

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

Procedures for Responding to Specific Online Incidents or Concerns

8 Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the head teacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the schools complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school/setting community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.
- Parents and children will need to work in partnership with the school to resolve issues.

8.1 Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- Palace Wood recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We 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".
- Palace Wood 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, such as NSPCC website.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
  - .1 View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
    - .1.1 If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
  - .2 Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - .1 Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
  - .2 Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
  - .3 Store the device securely.
    - .3.1.1 If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - .4 Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
  - .5 Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - .6 Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
  - .7 Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
  - .8 Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
  - .9 Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

    .9.1   Images will only be deleted once the DSL 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.

   .10 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.

8.2 Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2022.
- Palace Wood recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - .1 Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- Palace Wood recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Palace Wood also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Palace Wood will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - .1 Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - .2 If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - .3 Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - .4 Implement appropriate sanctions in accordance with our behaviour policy.
    - .5 Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - .6 If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.

.7   If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

    .7.1   If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.

.8   Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

8.3 Responding to concerns regarding Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Palace Wood 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.
- Palace Wood 's 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 intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSET team by the DSL.
- If the school are made aware of incident involving online child sexual abuse of a child then the school will:
  - .1   Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
  - .2   Immediately notify the designated safeguarding lead.
  - .3   Store any devices involved securely.
  - .4   Immediately inform Kent police via 101 (using 999 if a child is at immediate risk)
- 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.
  - .1   Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent 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 the Child Sexual Exploitation Team (CSET) by the Designated Safeguarding Lead.
  - .1   Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  - .2   Make a referral to children's social care (if needed/appropriate).

.3 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.

.4 Inform parents/carers about the incident and how it is being managed.

.5 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 ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- 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.

8.4. Responding to concerns regarding Indecent Images of Children (IIOC)

- Palace Wood 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 of 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 access accidental access to of 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/setting is made aware of Indecent Images of Children (IIOC) then the school will:
    .1 Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
    .2 Immediately notify the school Designated Safeguard Lead.
    .3 Store any devices involved securely.
    .4 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 are 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:
    .1 Ensure that the Designated Safeguard Lead is informed.
    .2 Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    .3 Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:

.1 Ensure that the Designated Safeguard Lead is informed.
.2 Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
.3 Ensure that any copies that exist of the image, for example in emails, are deleted.
.4 Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
.5 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 are 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:
  .1 Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  .2 Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  .3 Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  .4 Follow the appropriate school policies regarding conduct.

8.5. Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools 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 safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.

8.6 Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of Palace Wood's 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.
- 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 cyberbullying as evidence.

- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - .1 Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - .2 A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - .3 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.
    - .4 Parent/carers of pupils involved in online bullying will be informed.
    - .5 The Police will be contacted if a criminal offence is suspected.

8.7 Responding to concerns regarding online hate

- Online hate at Palace Wood will not be tolerated
- All incidents of online hate reported to the school will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- The Police will be contacted if a criminal offence is suspected. 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.

Appendix 1

Useful Links for Educational Settings

- **Kent Support and Guidance**

- **Kent County Council Education Safeguarding Team**:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
    - .1 esafetyofficer@kent.gov.uk Tel: 03000 415797
- Guidance for Educational Settings:
    - .1 www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
    - .2 www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
    - .3 www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
    - .4 Kent e–Safety Blog: www.kentesafety.wordpress.com

- **KSCB:**
- www.kscb.org.uk

- **Kent Police:**
- www.kent.police.uk or www.kent.police.uk/internetsafety
- 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

- **Other:**

- Kent Public Service Network (KPSN): www.kpsn.net
- 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
- CEOP:
    - .1 www.thinkuknow.co.uk
    - .2 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
    - .1 ChildLine: www.childline.org.uk
    - .2 Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
    - .1 Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk