KINGS HILL SCHOOL
PRIMARY & NURSERY

Kings Hill School
Primary and Nursery

Online Safety Policy

Date of Policy: September 2025
Date of Review: September 2026
Reviewed to add DDSL January 2026

This policy will be reviewed **at least** annually. It will also be revised following any changes to technology use, online safety concerns and/or updates to national and local guidance or procedures.

Kings Hill School Primary and Nursery

ONLINE SAFETY POLICY

Designated Safeguarding Lead: Mrs Kate Harris; Deputy Headteacher
Deputy Designated Safeguarding Lead:
Mrs Beth McKenzie; Headteacher
Mrs Sally McCarville; Assistant Head of EYFS and Key Stage 1
Mrs Karen Marshman; Assistant Head of Key Stage 2

Governors with Safeguarding Responsibility: Mrs Stephanie Foster

1. Policy Aims and Scope

This online safety policy has been written by Kings Hill School Primary and Nursery involving staff, pupils and parents/carers, building on the The Education People online safety policy template, with specialist advice and input as required.

This policy has been written by Kings hill School and Nursery involving staff, learners and parents/carers, building on The Education People policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage, 'Working Together to Safeguard Children' and the local Safeguarding Children Multi-agency Partnership procedures. Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk).

- Kings Hill School Primary and Nursery recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out our whole school approach to online safety which will empower, protect and educate learners and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.

- Kings Hill Primary and Nursery understands that breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
  - **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
  - **Contact**: being subjected to harmful online interaction with other users, for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
  - **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
  - **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

- Kings Hill Primary and Nursey recognises that children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online.

- This policy applies to learners, parents/carers and all staff, including the governing body, leadership team, 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).

- Kings Hill School Primary and Nursery identifies that the internet and technology such as computers, tablets, mobile phones, smart watches, games consoles and social media are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks. This policy applies to all access to and use of technology, both on and off-site.

This policy links with a number of other policies, practices and action plans including but not limited to:

- Anti-bullying Policy
- Acceptable Use Policies (AUP)
- Code of Conduct
- Behaviour Policy
- Safeguarding and Child Protection Policy
- Confidentiality Statement
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Security
- Image Use Policy
- Searching, Screening and Confiscation policy

2. Responding to Emerging Risks

- Kings Hill Primary and Nursery recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - carry out an annual review of our online safety approaches which will be supported by an annual risk assessment which considers and reflects the specific risks our learners face.
  - regularly review the methods used to identify, assess and minimise online risks.
  - examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted.
  - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet access is appropriate.
  - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems, and as such identify clear procedures to follow if breaches or concerns arise.

3. Monitoring and Review

- Kings Hill Primary and Nursery will review this policy at least annually. The policy will also be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the DSLs will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

- Any issues identified will be incorporated into our action planning.

4. Roles and Responsibilities

- The school has appointed Mrs Kate Harris as Designated Safeguarding Lead and is recognised as holding overall responsibility for online safety. However, Kings Hill Primary and Nursery recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1. The Leadership and Management Team will:

- Create a whole school culture that incorporates online safety throughout
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with our network manager and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure there are robust reporting channels in place regarding online safety concerns.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety
- 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.

4.2. The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact with the school on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral staff, the network manager and the SENCO on matters of online safety as appropriate.
- Ensure referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated whole school approach is implemented.

- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep learners safe online, including the additional risks that learners with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- 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.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, school policies and procedures.
- Report online safety concerns, as appropriate, to the leadership team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet three times a year with the governor with a lead responsibility for safeguarding and online safety.

4.3. It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to our online safety policy and AUPs.
- Take responsibility for the security of IT systems and the electronic data they use, or have access to.
- Model good practice when using technology with learners.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- 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 reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4. It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and school leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures (including password policies and encryption) as directed by the leadership team to ensure that the school's IT infrastructure is secure and

not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

- Ensure that the school's filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL (and/or deputy) to enable them to take appropriate safeguarding action when required.

4.5. It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age/ ability appropriate online safety education.
- Contribute to the development of online safety policies
- Read and adhere to the school AUPs and behavior policies
- Respect the feelings and rights of others both on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

4.6. It is the responsibility of parents and carers to:

- Read the school AUPs and encourage their children to adhere to them.
- 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 and abide by the home-school agreement and acceptable use of technology policies
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school's online safety policies.
- Use our systems, such as learning platforms and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies that their children access and use at home.

5. Education and Engagement Approaches

5.1. Education and Engagement with Learners

- Kings Hill Primary and Nursery will establish and embed a whole school culture and will empower our learners to acquire the knowledge needed to use the technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

- The school will raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS)) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance
- Ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study.
- Reinforcing online safety principles in other curriculum subjects as appropriate and whenever technology or the internet is used on site.
- Implementing appropriate peer education approaches such as digital leaders
- Creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
- Involving the DSL (or a deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.
- Making informed decisions to ensure that any educational resources used are appropriate for our learners.
- Using external visitors, where appropriate, to complement and support our internal online safety education approaches.
- Providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
- Rewarding positive use of technology.

The school will support pupils to understand and follow the AUP in a way which suits their age and ability by:

- Sharing our AUPs with them in a way that suits their age and ability.
- Displaying acceptable use posters in all rooms with internet access.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.

The school will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:

- Ensuring age appropriate education regarding safe and responsible use precedes internet access.
- Enabling them to understand what acceptable and unacceptable online behaviour looks like.
- Teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
- Educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
- Preparing them to identify possible online risks and make informed decisions about how to act and respond.
- Ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2. Vulnerable Pupils

- Kings Hill School Primary and Nursery recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- Kings Hill School Primary and Nursery will ensure that differentiated and ability appropriate online safety education, access and support is provided to all learners who require additional or targeted support.
- Staff at Kings Hill School Primary and Nursery will seek input from specialist staff as appropriate, including the DSL, SENCO and Child in Care Designated Teacher to ensure that the policy and curriculum is appropriate to our community's needs.

5.3. Training and Engagement with Staff

The school 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 which is integrated, aligned and considered as part of our overarching safeguarding approach.
- Staff training covers the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Build on existing expertise by provide opportunities for staff to contribute to and shape our online safety approaches.
- 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 school's policies when accessing school systems and devices.
- Make staff aware that their online conduct, including personal use of social media, can 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 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 community.

5.4. Awareness and Engagement with Parents and Carers

- Kings Hill School Primary and Nursery 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, transition events, fetes and sports days.
  - Drawing their attention to the school 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 school, for example, within our home school agreement.
  - Requiring them to read the school AUP and discuss its implications with their children.

6. Safer Use of Technology

6.1. Classroom Use

- Kings Hill School Primary and Nursery uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Learning platforms, remote learning platform/ tools and intranet
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- Use of video sharing platforms will be in accordance with our acceptable use of technology policies, following an informed risk assessment and with appropriate safety and security measures in place. This includes: having staff access only and using education versions for learners access.
- 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.
- Supervision of internet access and technology use will be appropriate to learners age and ability.
- **Early Years Foundation Stage and Key Stage 1**
  Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability.
- **Key Stage 2**
  Pupils will use age-appropriate search engines and online tools. Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

6.2. Managing Internet Access

- The school will maintain a written record of users who are granted access to the school's devices and systems.
- All users will read and sign an AUP, appropriate to their age, understanding and role, before being given access to the school computer system, IT resources or internet.

6.3. Filtering and Monitoring

6.3.1. Decision Making

- Kings Hill Primary and Nursery will do all we reasonably can to limit children's exposure to online risks through school provided IT systems/devices and will ensure that appropriate filtering and monitoring systems are in place.
- Kings Hill Primary and Nursery leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- 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.

6.3.2. Appropriate Filtering

- Kings Hill Primary and Nursery uses educational broadband connectivity through the KPSN.
- The school uses Light Speed filtering system which blocks access to sites which could promote or include harmful and / or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
- KPSN is a member Internet Watch Foundation (IWF) list and blocks access to illegal Child abuse and Content (CAIC).
- Kings Hill School Primary and Nursery integrates 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' as part of the Light Speed filtering.
- The school works with KCC and the Schools broadband team to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If pupils or staff discover unsuitable sites, they will be required to:
  - Turn off monitor/screen and report the concern immediate to a member of staff.
  - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and network manager.
  - The breach will be recorded and escalated as appropriate.

- Parents/carers will be informed of filtering breaches involving their child.

- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

6.3.3. Appropriate Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by physical monitoring (supervision) and spot checks on internet use using our internal filtering system. All teachers have access to Impero which they can use to view the pupils workstations in the computing suite.

- 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.

- If a concern is identified via our monitoring approaches:

    - Where the concern relates to learners, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour.
    - Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the headteacher), in line with our staff behavior and allegations policy

6.4. Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in the schools Information Security Policy.

6.5. Information security and access management

- The school takes appropriate steps to ensure necessary security protection procedures are in place, in order to safeguard our systems, staff and learners.

- Further information about technical environment safety and security can be found in the school's information security policy but includes:

    - Virus protection being updated regularly.

    - All staff laptops are fully encrypted for secure personal data taken off site and secure and Direct Access is used for remote working with two form factor authentication.

    - All removeable drives must be encrypted before they can be written to, and files are scanned for viruses upon connection.

    - Staff are restricted from downloading or installing unapproved software (as per the Staff AUP) to work devices or opening unfamiliar email attachments.

    - Regularly checking files held on the school's network.

- The appropriate use of user logins and passwords to access the school network.
    - Specific user logins and passwords will be enforced for all but Nursery and Reception year.
- All users are expected to log off or lock their screens/devices if systems are unattended.

- We will review the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies.

6.5.1. Password policy

- 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.
- From Year 1 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 all staff to:
    - Use strong passwords for access into our system.
    - Change their passwords every 90 Days
    - 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.
    - Lock access to devices when not in use.
    -

6.6. 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, telephone number and staff school email address.
- 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.

6.7. 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: the Image use policy, Data Security, AUPs and the Code of Conduct.

6.8. 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.
    - 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, Mrs Kate Harris if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.

6.8.1. Staff email

- 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.

6.8.2. Pupil Email

- Pupils will use school provided email accounts for educational purposes.

- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the school.

6.9. Educational use of Videoconferencing and/or Webcams

Kings Hill School Primary and Nursery recognise that videoconferencing and the 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.
- School videoconferencing equipment will not be taken off school premises without prior permission from the DSL or Headteacher.
- Staff will ensure that external videoconferencing opportunities and 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.

6.9.1. Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher/ member of staff before making or answering a videoconference call or message. .
- Video conferencing will take place via official and approved communication channels following a robust risk assessment. and will be supervised appropriately, according to the learners age and ability.
- 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.

6.9.2. 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, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.

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

6.10. Management of Learning Platforms

- Kings Hill Primary and Nursery uses Microsoft Teams as its official learning platform and all access and use takes place in accordance with our acceptable use policies.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP. When staff and learners leave the school, their account 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.
    - If the user does not comply, the material will be removed by the site administrator.
    - 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.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership as part of an agreed focus or a limited time slot.

6.11. Management of Applications (apps) used to Record Children's Progress

The school uses FFT Aspire, SIMs and 2simple to track pupil's progress and share appropriate information with parents and carers.

The Headteacher will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

In order to safeguard pupil's data:

- Only school issued devices issued to pupils 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.
- School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

6.12 Management of remote learning

Where children are asked to learn online at home in response to a full or partial closure:

- Kings Hill Nursery and Primary will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with learners and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers or agreed systems e.g. Microsoft Teams
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our code of conduct and Acceptable Use Policies.
- Staff and learners will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP)
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access Kings Hill Nursery and Primary will continue to be clear who from the school their child is going to be interacting with online.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

7. Social Media

7.1. Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Kings Hill School Primary and Nursery 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 apps or other online communication services.

- All members of Kings Hill School Primary and Nursery community are expected to engage in social media in a positive and responsible manner and are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

- All members of Kings Hill School Primary and Nursery 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.

- The school will control pupil and staff access to social media whilst using school provided devices and systems on site. The use of social media during school hours for personal use is only permitted during break and lunch times in areas where children cannot be e.g. staffroom. Inappropriate or excessive use of social media during work hours or whilst using school devices may result in disciplinary or legal action and removal of internet facilities.

- Concerns regarding the online conduct of any member of Kings Hill School Primary and Nursery community on social media, will be taken seriously. concerns will be managed in should be managed in accordance with our anti-bullying, allegations against staff, behaviour, home-school agreement and child protection policies.

7.2. Staff Use of Social Media

- The use of social media during school hours for personal use is permitted for staff, however, this is only permitted in the staff room during break times.

- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct and acceptable use of technology policy.

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.

- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

7.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the 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. This will include (but is not limited to):

    - Setting the privacy levels of their personal sites as strictly as they can.

    - Being aware of the implications of using location sharing services.

- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe, strong 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 Kings Hill School Primary and Nursery 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 staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- 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.

7.2.1. Communicating with pupils and parents and carers

- Staff will not use any personal social media accounts to contact pupils or their family members.
- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as 'friends' on any personal social media account.
- Any communication from learners and parents' carers received on personal social media accounts will be reported to the DSL (or deputy) and the Headteacher.
- Any pre-existing relationships or situations, which means staff cannot comply with this requirement, will be discussed with the DSL and the Headteacher. Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff
- 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.

7.3. Official Use of Social Media

- Kings Hill School Primary and Nursery school official social media channels are: Facebook page link and a Twitter link.
- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes and the use has been formally risk assessed and approved by the Headteacher prior to use.
- Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Public communications on behalf of the setting 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 learners; any official social media activity involving learners will be moderated if possible 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.
- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.
- If members of staff are managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Read, understand and sign our Acceptable Use Policy.
  - Be aware they are an ambassador for the school.
  - Be professional, responsible, credible, fair and honest, 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.
  - Follow our image use policy at all times, for example ensuring that appropriate consent has been given before sharing images.
  - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
  - Not engage with any private or direct messaging with current or past learners or their family members.

- Inform their line manager, the DSL (or deputy) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

- 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 are linked to 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.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, Image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of school will be clear, transparent and open to scrutiny.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving pupils will be moderated by the school.

7.4. Pupils' Use of Social Media

- The use of social media during school hours for personal use is not permitted for pupils.
- Kings Hill School Primary and Nursery will empower our learners to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies such as PSHE and Computing.
- The school is aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, the school will not create accounts specifically for children under this age.

Learners will be advised

- 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.

- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns on social media both within school and externally

- Any concerns regarding pupils' use of social media, will be dealt with in accordance with existing school policies including anti-bullying, child protection and behaviour.
- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
- Sanctions and/or pastoral/welfare support will be implemented and offered to learners as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.
- Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

8. Mobile and Smart Technology

8.1. Safe Use of Mobile and Smart Technology Expectations

- Kings Hill School Primary and Nursery recognises that use of mobile and smart technologies is part of everyday life for many learners, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the school community are advised to:
  - take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.
- Mobile phones and personal devices are not permitted to be used in classrooms, changing rooms, swimming pools or toilets but only in the staff room during non-class time e.g. break, lunch, PPA time
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy or Staff Code of Conduct.

- All use of mobile technology and personal devices (including but not limited to; tablets, games, consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Child Protection.

- All members of Kings Hill School Primary and Nursery 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 illegal or which would otherwise contravene the school Behaviour or Child Protection policies.

8.2. School provided mobile phones and devices

- Members of staff will be issued with a work phone number in addition to their work email address, where contact with learners or parents/carers is required

- Staff providing formal remote learning will do so using school provided equipment in accordance with our Acceptable Use Policy

- Staff running our breakfast and after-school club will be issued with a work phone number and email address as contact with pupils or parents/ carers is required. As will our site manager so they can be contacted by staff members when working around the site.

- School mobile phones and devices will be suitably protected via a pin and must only be accessed or used by members of staff.

- School mobile phones and devices will always be used in accordance with the Acceptable Use Policy and Child Protection policies.

- Where staff and/or learners are using school provided mobile phones and/or devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

8.3. Staff Use of Mobile and Smart Technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child Protection, staff code of conduct, Data Security and Acceptable use.

- Staff will be advised to:

    - Keep mobile phones and personal devices in a safe and secure place during lesson time such as in class cupboards or lockers in the staff room.

    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.

    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.

    - Not use personal devices during teaching periods, unless written 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 our behaviour 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 or Headteacher.

- Staff will only use school provided equipment (not personal devices)

  - To take photos or videos of in line with our image use policy

  - To work directly with pupils during lessons/educational activities to communicate with parents/carers

  - to communicate with parents/carers

- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.

- If a member of staff breaches the school policy, action will be taken in line with the school's code of conduct.

- 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, using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

8.4. Pupils' Use of Mobile and Smart Technology

- Pupils will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices and will be made aware of boundaries expectations and consequences for policy breeches.

- Safe and appropriate use of mobile and smart technology will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection, comouting and PSHE policy.

- Mobile phones or personal devices will not be used by pupils on site.

  - Mobile phones or personal devices will not be used by learners during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.

  - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

- Staff will only allow learners to use their mobile phones or personal devices as part of an educational activity, following a risk assessment, with approval from the Leadership Team.

- Kings Hill School Primary and Nursery expects pupil's personal devices and mobile phones to be switched off and handed in to the school office at the beginning of each school day.

- If a pupil needs to contact their parents or carers they will be allowed to use a school phone. Parents are advised to contact their child via the school office during school hours; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.

- If a learner requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher prior to use being permitted. Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.

- Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and their parents carers before use is permitted.

- Where learners' mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy and/or Remote Learning AUP.

- Mobile phones and personal devices must not be taken into examinations. Learners found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

- Any concerns regarding learners use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
    - Searches of mobile phone or personal devices will be carried out in accordance with our policy.
    - Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil and parent/carer. Content may be deleted or requested to be deleted if it contravenes our policies.
    - Mobile phones and devices that have been confiscated will be held in the school office until the end of the day.
    - Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
    - Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.
    - Where there is a concern that a child is at risk of harm, we will respond in line with our child protection policy.
    - If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

8.5. Visitors' Use of Mobile and Smart Technology

- Parents, carers and visitors (including volunteers and contractors) are expected to ensure that:

    - They only use their mobile phones and personal devices in specific areas if the school or are only permitted for specific purposes e.g. as part of multi-agency working arrangements.

- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use.
- If visitors require access to mobile and smart technology, for example when working with learners as part of multi-agency activity, this will be discussed with the headteacher prior to use being permitted.
    - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile or smart technology and will always inform the Designated Safeguarding Lead of any breaches of school policy.

9. Responding to Online Safety Incidents and Concerns

- All members of the school 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.
    - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This may include: Insert expectations and policies.
    - will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
    - will be made aware of how the school will monitor policy compliance by: Insert how this is achieved e.g. AUPs, staff training, classroom management etc.
    - are expected to adopt a partnership with the school to resolve issues.
- If appropriate, after any investigations are completed, the DSL and leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

- If we are unsure how to proceed with an incident or concern, the DSL or headteacher will seek advice from the Kent Education Safeguarding Service other agency in accordance with our child protection policy.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local schools are involved or the wider public may be at risk, the DSL and/or headteacher will speak with the police and/or the Local Authority first, to ensure that potential criminal or child protection investigations are not compromised.

9.1. Concerns about Pupil's Online Behaviour and/or Welfare

- All concerns about pupil's will be responded to and recorded in line with our child protection policy:
    - The DSL (or deputy DSL) will be informed of any online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
    - The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be implemented and/or offered to learners as appropriate. Civil or legal action will be taken if necessary.
- The school will inform parents and carers of any inline safety incidents or concerns involving their child, as and when required.

9.2. Concerns about Staff Online Behaviour and/or Welfare

- Any complaint about staff misuse will be referred to the Headteacher, according to our Allegations against Staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Where appropriate, welfare support will be offered, and where necessary, disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.

9.3. Concerns about Parent/Carer Online Behaviour and/or Welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the headteacher and/or DSL and dealt with in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy
- Where appropriate, welfare support will be offered, and where necessary, civil and/or legal action may be taken.

10. Procedures for Responding to Specific Incidents or Concerns

10.1. Online Child on Child Abuse

- Kings Hill School Primary and Nursery recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online child on child abuse concerns will be responded to in line with our child protection and behaviour policies.
- We recognise that online child on child abuse can take many forms, including but not limited to:
    - bullying, including cyberbullying, prejudice-based and discriminatory bullying
    - abuse in intimate personal relationships between peers
    - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
    - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
    - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
    - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
    - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
    - initiation/hazing type violence and rituals.
- Kings Hill School Primary and Nursery believes that abuse is abuse, including when it takes place online and it will never be tolerated or dismissed as "banter", "just having a laugh", "part of growing up" or "boys being boys" as this can lead to a culture of unacceptable behaviours and an unsafe environment for children.
- Kings Hill School Primary and Nursery believes that all staff have a role to play in challenging inappropriate online behaviours between peers.
- Kings Hill School Primary and Nursery recognises that, even if there are no reported cases of online child on child abuse, such abuse is still likely to be taking place.
- Concerns about learner's behaviour, including child on child abuse taking place online offsite will be responded to as part of a partnership approach with learners and parents/carers and in line with existing policies, for example anti-bullying, acceptable use, behaviour and child protection policies.
- Kings Hill School Primary and Nursery want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online child on child abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with

associated policies, including child protection, anti-bullying and behaviour. Learners who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

10.1.1. Child on Child Online Sexual Violence and Sexual Harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Kings Hill School Primary and Nursery will follow the guidance outlined in Part Five of KCSIE 2021 and the DfE 'Sexual Violence and Sexual Harassment Between Children in Schools and Colleges' guidance.
- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.
- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.
- Kings Hill School Primary and Nursery recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - consensual and non-consensual sharing of nude and semi-nude images and videos
    - sharing of unwanted explicit content
    - 'upskirting' (which is a criminal offence and typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation, coercion and threats.
- Kings Hill School Primary and Nursery recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and 24 services, and for things to move from platform to platform online.
- Kings Hill School Primary and Nursery 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.
- Kings Hill School Primary and Nursery 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 and the support available, by implementing a range of age and ability appropriate educational methods as part of our curriculum
- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator and any other children involved/impacted.
    - The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children and staff and any actions that are required to protect them.

- Reports will initially be managed internally by the DSL, and where necessary will be referred to Kent Education Safeguarding Service, Children's Social Care and/or the the Police.
- The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
    - If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

    - Following an immediate risk assessment the school will:
    - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
- inform parents/carers for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
- if the concern involves children and young people at a different educational school, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised.
- review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

- Kings Hill School primary and Nursery recognises that internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. Kings Hill school Primary an Nursery also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

10.1.2. Nude or Semi-nude image Sharing

The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of 18. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex. The UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance outlines how schools and colleges should respond to all incidents of consensual and non-consensual image sharing, and should be read and understood by DSLs working will all age groups, not just older learners.

Kings Hill School Primary and Nursery recognises consensual and non-consenual sharing of nude and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") can be a safeguarding issue; all concerns will be reported to and dealt with by the Designated Safeguarding Lead (or deputy DSL).

- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
  - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
  - shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
  - possesses nude and/or semi-nude imagery created by another person under the age of 18.
- When made aware of concerns regarding nude and/or semi-nude imagery, Kings Hill School Primary and Nursery will follow the advice as set out in the non-statutory UKCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- Kings Hill School Primary and Nursery will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.
- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
  - Report any concerns to the DSL immediately.
  - Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, this will be immediately reported to the DSL.
  - Not delete the imagery or ask the child to delete it.
  - Not say or do anything to blame or shame any children involved.
  - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
  - Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.
- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
  - act in accordance with our child protection policies and the relevant local procedures and in line with the UKCIS guidance.
  - carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
  - a referral will be made to Children's Social Care and/or the police immediately if:
    - the incident involves an adult (over 18).
    - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
    - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
    - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.

- The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
- If DSLs are unsure how to proceed, advice will be sought from the Kent education Safeguarding Service.
- Store any devices securely:
  - If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - If a potentially 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.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
- provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- implement sanctions where necessary and appropriate in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the UKCIS guidance.
  - 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.
  - Learners will be supported in accessing the Childline 'Report Remove' tool where necessary: Report Remove Tool for nude images.
- 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.

- We will not:
  - view any imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. If it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, and any decision making will be clearly documented.
  - send, share, save or make copies of content suspected to be an indecent image/video of a child and will not allow or request learners to do so.

10.1.3. Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Kings Hill School Primary and Nursery.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

10.2. Online Child Abuse and Exploitation

- Kings Hill School Primary and Nursery recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL, in line with our child protection policy.
- Kings Hill School Primary and Nursery will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible

grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.

- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant local safeguarding children partnership procedures.
    - store any devices containing evidence securely:
        - If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk or seek advice from the Ketn Education Safeguarding Service
    - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using school provided or personal equipment.
    - Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via the National Crime Agency CEOP Command (NCA-CEOP): www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Kent Education Safeguaridng Service and/or police.
- We will ensure that the NCA-CEOP reporting tools are visible and available to learners and other members of our community; this can be accessed via the school's website.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL.
- If members of the public or learners at other schools are believed to have been targeted, the DSL, will seek advice from the police and/or the Kent Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

10.3. Indecent Images of Children (IIOC)

- Kings Hill School Primary and Nursery will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate.

- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the police and/or the Local Authority.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant local safeguarding children partnership procedures.
    - store any devices involved securely, until advice has been sought. If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been exposed to indecent images of children, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk and/or police.
    - inform the police as appropriate, for example if images have been deliberately sent to or shared by learners.
    - report concerns as appropriate to parents and carers.
- If made aware that indecent images of children have been found on school provided devices, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and any other agencies, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children, we will:
    - ensure that the headteacher is informed in line with our managing allegations against staff policy.
    - inform the LADO and other relevant organisations, such as the police in accordance with our managing allegations against staff policy.
    - quarantine any involved school provided devices until police advice has been sought.

10.4. Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Kings Hill School Primary and Nursery and will be responded to in line with existing school policies, including child protection, anti-bullying and behaviour.

- 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 (or deputy) will obtain advice through the Kent Education Safeguarding Service and/or Kent Police.

10.5. Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy:
  - If the concerns relate to a member of staff, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies

10.6. Cybercrime

- Kings Hill School Primary and Nursery recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.
- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the Cyber Choices programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

11. Useful Links

Links for Schools

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- SWGfL: 360 Safe Self-Review tool for schools www.360safe.org.uk
- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- PSHE Association: www.pshe-association.org.uk
- National Education Network (NEN): www.nen.gov.uk
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk
- Educate against hate: https://educateagainsthate.com

- NCA-CEOP Education Resources: www.thinkuknow.co.uk
- Safer Recruitment Consortium: www.saferrecruitmentconsortium.org/

Reporting Helplines

- NCA-CEOP Safety Centre: www.ceop.police.uk/Safety-Centre
- Internet Watch Foundation (IWF): www.iwf.org.uk
- ChildLine: www.childline.org.uk
  - Report Remove Tool for nude images: www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online
- Stop it now! www.stopitnow.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Report Harmful Content: https://reportharmfulcontent.com
- Revenge Porn Helpline: https://revengepornhelpline.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Support for children and parents/carers

- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Parent Zone: https://parentzone.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
  - Net Aware: www.net-aware.org.uk
- Parents Protect: www.parentsprotect.co.uk
- Get Safe Online: www.getsafeonline.org
- NCA-CEOP Child and Parent Resources: www.thinkuknow.co.uk