Weald of Kent Grammar School

Online Safety Policy – October 2021

Aim of this policy

- Weald (**Weald**) believes that online safety (e-safety) is an essential element of safeguarding students and adults in the digital world, when using technology such as computers, mobile phones or games consoles.
- Weald identifies that the Internet and information communication technologies are an important part of everyday life so students must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
- Weald has a duty to provide the school community with quality Internet access to raise education standards, promote student achievement, support the professional work of staff and enhance the school's management functions. Weald also identifies that with this there is a clear duty to ensure that students are protected from potential harm online.
- The purpose of this 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 Weald is a safe and secure environment.
  - Safeguard and protect all members of the Weald's community online.
  - Raise awareness with all members of the Weald's community regarding the potential risks as well as benefits of technology.
  - Enable staff to work safely and responsibly, to role model positive behaviour online and to 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.
- The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
  - Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
  - Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
  - Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
  - Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- This policy applies to staff including the governing body, teachers, support staff, external contractors, visitors, volunteers (and other individuals who work for or provide services on behalf of Weald) as well as students and parents/carers.
- This policy applies to all access to the Internet and use of information communication devices including personal devices or where students, staff or other individuals have been provided with Weald issued devices for use off-site, such as a work laptop or mobile phone.
- This policy must be read in conjunction with other relevant Weald policies including (but not limited to) Safeguarding, Anti-bullying, Behaviour, Photographic Image Use, Acceptable Use, confidentiality, screening, searching and relevant curriculum policies including computing, Relationships and Sex Education (RSE) Policy.

This online safety policy has been written by Weald, building on KCC advice with specialist advice and input as required. It takes into account the DfE statutory guidance '<u>Keeping Children Safe in Education'</u> 2021, '<u>Working Together to Safeguard Children</u>' 2018 and the <u>Kent Safeguarding Children Board</u> procedures.

- Weald of Kent Grammar continues to operate in response to coronavirus (Covid-19); our safeguarding principles in accordance with 'Keeping Children Safe in Education' (KCSIE) 2021 and related guidance, however, remain the same. Where children are asked to learn online at home in response to a full or partial closure or self-isolation, will follow expectations as set out within the Child Protection Policy and in line with DfE Guidance, 'Safeguarding and remote education during coronavirus (COVID-19)' 2020.
- The policy has been approved and agreed by both the Senior Leadership Group and the Governing Body.
- Weald's online safety policy and its implementation will be reviewed at least annually or sooner if required.

Weald's DSL (Designated Safeguarding Lead) has overall responsibility for Online Safety. Weald of Kent's DSL is Chantelle Waul.

1.2 Key responsibilities of the community

1.2.1 Key responsibilities of Senior Leadership Group are:

- To ensure that there are appropriate and up-to-date policies regarding online safety; including an acceptable use policy, which covers acceptable use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- To ensure that online safety is embedded within the curriculum, which enables all students to develop an age-appropriate understanding of online safety.
- To support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- To ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- To ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- To audit and evaluate online safety practice to identify strengths and areas for improvement.

1.2.2 Key responsibilities of the designated safeguarding/online safety lead are:

- To act as a named point of contact on all online safety issues and liaise with other members of staff and agencies as appropriate.
- To keep up-to-date with current research, legislation and trends.
- To coordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- To ensure that online safety is promoted to parents/carers and the wider community through a variety of channels and approaches.
- To work with Weald's lead for data protection and data security to ensure that practice is in line with legislation.
- To access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep students safe online.
- To ensure that online safety incidents and subsequent actions are recorded as part of Weald's safeguarding recording structures and mechanisms. Records will be in the safeguarding and child protection folders.
- To monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- To liaise with the local authority and other local and national bodies as appropriate.
- To report online safety concerns, as appropriate, to the Senior Leadership Group and Governing Body.
- To work with the leadership team to review and update online safety policies on a regular basis (at least annually).
- To ensure that online safety is integrated with other appropriate Weald policies and procedures.
- To meet regularly with the governor with a lead responsibility for online safety.

1.2.3 Key responsibilities of staff are:

- To contribute to the development of online safety policies.
- To read Weald’s AUP and adhere to it.
- To take responsibility for the security of Weald’s systems and data.
- To have an awareness of online safety issues, and how they relate to the students in their care, including understanding the key issues related to online safety; content, contact, conduct and commerce.
- To ensure that they understand that technology is a significant component in many safeguarding and wellbeing issues and 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 can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.
- To model good practice in using new and emerging technologies and demonstrate an emphasis on positive learning opportunities rather than focusing on negatives.
- To embed online safety education in curriculum delivery wherever possible.
- To identify individuals of concern, and take appropriate action by working with the DSL.
- To know when and how to escalate online safety issues, internally and externally.
- To be able to signpost to appropriate support available for online safety issues, internally and externally.
- To maintain a professional level of conduct in their personal use of technology, both on and off site.
- To take personal responsibility for professional development in this area.

1.2.4. Additional responsibilities for staff managing the technical environment are:

- To provide technical support and perspective to the DSL and Senior Leadership Group, especially in the development and implementation of appropriate online safety policies and procedures.
- To implement appropriate security measures as directed by the Senior Leadership Group, to ensure that the IT systems are secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- To ensure that our filtering policy is applied and updated on a regular basis. The responsibility for its implementation is shared with the Senior Leadership Group.
- To ensure that our monitoring systems are applied and updated on a regular basis. The responsibility for its implementation is shared with the Senior Leadership Group.
- To ensure that appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable him/her to take appropriate safeguarding action if/when required.

1.2.5 Key responsibilities of students are:

- To read Weald’s Acceptable Use Policy (AUP) and adhere to it.
- To respect the feelings and rights of others both on and offline.
- To seek help from a trusted adult if things go wrong, and support others that may be experiencing online safety issues.
- To take responsibility for keeping themselves and others safe online.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To assess the personal risks of using any particular technology and behave safely and responsibly to limit those risks.

1.2.6. Key responsibilities of parents/carers are:

- To read Weald’s AUP, encourage their children to adhere to it, and adhere to it themselves where appropriate.

- To support Weald’s online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- To role model safe and appropriate uses of new and emerging technology.
- To identify changes in behaviour that could indicate that their child is at risk of harm online.
- To seek help and support from Weald, or other appropriate agencies, if they or their child encounters online problems or concerns.
- To contribute to the development of Weald’s online safety policy.
- To use Weald’s systems, and other network resources, safely and appropriately.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To report any known issues as soon as possible.

2. Online Communication and Safer Use of Technology

2.1 Managing the Weald of Kent Grammar Weald website

- Weald will ensure that information posted on Weald’s website meets the requirements as identified by the Department for Education (DfE).
- Weald 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 students personal information will not be published on Weald’s website without explicit permission.
- The administrator account for the Weald 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.

2.2 Publishing images and videos online

- Weald will ensure that all images are used in accordance with Weald’s Photographic Image Use policy.
- In line with Weald’s Photographic Image policy, written permission from parents/carers will always be obtained before images/videos of students are electronically published.

2.3 Managing email

- Students may only use Weald provided email accounts for educational purposes.
- All staff are provided with a specific Weald email address to use for any official communication.
- The use of personal email addresses by staff for any official Weald 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 must only be sent using secure and/or encrypted methods.
- Members of the Weald community must immediately tell a member of the Senior Leadership Group if they receive an offensive communication.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Access in Weald to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully before sending, in the same way as a letter written on Weald headed paper would be.
- Weald email addresses and other official contact details will not be used for setting up personal social media accounts or subscribing to services.

2.4 Official videoconferencing and webcam use

- All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.
- Videoconferencing contact information will not be posted publicly.

- Videoconferencing equipment will not be taken off the premises without prior permission from a 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.
- Students will not use, or have access to, videoconferencing equipment without permission.

Users

- Students will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the students' age and ability.
- Parents'/carers' consent will be obtained prior to students taking part in videoconferences with anyone outside of the Weald community.
- Videoconferencing 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.
- Unique log on and password details for the educational videoconferencing services will only be issued to staff and kept secure.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, Weald will check that recording is acceptable to avoid infringing third party intellectual property rights.
- Weald will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-Weald site, Weald will check that they are delivering material that is appropriate for the class.

2.5 Appropriate and safe classroom use of the Internet and associated devices

- Weald'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 students.
- Students will use age and ability appropriate tools to search the Internet for content.
- Internet use is a key feature of educational access and all students 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.
- Weald will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- All staff are aware that they cannot rely on filtering alone to safeguard students and supervision, classroom management and education about safe and responsible use is essential.
- Students will be appropriately supervised when using technology, according to their ability and understanding.
- All Weald owned devices will be used in accordance with Weald's AUP and with appropriate safety and security measure in place.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Weald will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- Weald will use the Internet to enable students and staff to communicate and collaborate in a safe and secure environment.

- Students 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 requirement across the curriculum.
- Staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

2.6 Management of Learning Platforms and Systems

- The Senior Leadership Group and staff will regularly monitor the usage of Weald's learning platforms and systems by students and staff in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised about acceptable conduct and use when using Weald learning platforms and systems.
- Only members of the current student, parent/carers and staff community will have access to Weald platforms and systems.
- All users will be mindful of copyright issues and will only upload appropriate content onto the portal.
- When staff and students leave Weald their account or rights to specific Weald areas will be disabled.
- Any concerns about content on Weald platforms and systems may 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 platforms/systems for the user may be suspended.
  - The user will need to discuss the issues with a member of Senior Leadership Group before reinstatement. A student's parent/carer may be informed.
  - A visitor may be invited onto the portal by a member of the Senior Leadership Group. In this instance there may be an agreed focus or a limited time slot.
  - Students may require editorial approval from staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the Weald community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the Weald community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the Weald community.
- All members of the Weald 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.
- Weald will control students and staff access to social media and social networking sites whilst on site and using Weald provided devices and systems.
- The use of social networking applications during Weald hours for personal use is not permitted.
- Inappropriate or excessive use of social media during Weald hours or whilst using Weald devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the Weald community on social media sites should be reported to the Senior Leadership Group and will be managed in accordance with existing Weald policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of Weald policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed.

Action taken will be accordance with the relevant Weald policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Official use of social media

- Official use of social media sites by Weald will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
- Official Weald social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use Weald provided email addresses to register for and manage official Weald approved social media channels.
- Staff running official Weald social media channels will ensure that they are aware of the required behaviours and expectations of use. They will ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official Weald social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official Weald social media sites will comply with legal requirements will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by Weald will be in line with existing policies, including: anti-bullying and child protection.
- Images or videos of students will only be shared on official Weald social media sites/channels in accordance with Weald's Photographic Image Use policy.
- Information about safe and responsible use of Weald social media channels will be communicated clearly and regularly to all members of the Weald community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the Weald website and take place with written approval from Senior Leadership Group.
- Senior Leadership Group staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/carers and students will be informed of any official Weald social media use, along with expectations for safe use and Weald action taken to safeguard the community.
- The Weald official social media channels are:
  - https://twitter.com/WOKGS
  - https://www.facebook.com/wealdofkentgs/
- Public communications on behalf of Weald will, where possible, be read and agreed by at least one other colleague.
- An account will link back to Weald's website and/or AUP to demonstrate that the account is official.
- Weald 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.

3.3 Staff official use of social media

- If staff are participating in online activity as part of their capacity as an employee of Weald, then they are requested to be professional at all times and that they are an ambassador for Weald.
- Staff using social media officially will disclose their official role/position, but always make it clear that they do not necessarily speak on behalf of Weald.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within Weald, including: libel; defamation; confidentiality; copyright; data protection as well as equalities laws.
- Staff must ensure that any image posted on Weald's social media channels have appropriate written parental consent.

- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of Weald unless they are authorised to do so.
- Staff using social media officially will inform their line manager, Weald's online safety (e-safety) lead and/or the head teacher of any concerns such as criticism, or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with students or parents/carers through social media and should communicate via Weald communication channels.
- Staff using social media officially will sign Weald's AUP before official social media use will take place.

3.4 Staff personal use of social media

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction (safeguarding training) and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all staff (including volunteers) as part of Weald's AUP.
- All staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the lead DSL/Senior Leadership Group.
- If ongoing contact with students is required once they have left Weald's roll, then members of staff will be expected to use existing alumni networks or use official Weald provided communication tools.
- All communication between staff and members of the Weald community on Weald business will take place via official approved communication channels (*such as Weald email addresses or phone numbers*). Staff must not use personal accounts or information to make contact with students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Headteacher.
- Any communication from students/parents received on personal social media accounts will be reported to a DSL.
- Information that staff have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with Weald's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Senior Leadership Group immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in Weald.
- Members of staff are encouraged not to identify themselves as employees of Weald on their personal social networking accounts. This is to prevent information on these sites from being linked with Weald and also to safeguard the privacy of staff and the wider Weald community.
- Members of staff will ensure that they do not represent their personal views as that of Weald on social media.
- Weald email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like Weald's social media channels will be advised to use dedicated professionals accounts where possible to avoid blurring professional boundaries.

3.5 Students use of social media

- Safe and responsible use of social media sites will be outlined for students and their parents as part of Weald's AUP.
- Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, Weald attended, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with students and written parental consent will be obtained, as required.
- Any official social media activity involving students will be moderated by Weald where possible.
- Weald is aware that many popular social media sites state that they are not for children under the age of 13, therefore, Weald will not create accounts within the school specifically for students under this age.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at Weald, will be dealt with in accordance with existing Weald policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices, including wearable technologies, among children, young people and adults will require all members of the Weald community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by Weald and covered in appropriate policies including Weald's AUP.
- Weald recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but requires that such technologies need to be used safely and appropriately within Weald.

4.2 Expectations for safe use of personal devices and mobile phones

- Electronic devices of all kinds that are brought into Weald are the responsibility of the user at all times. Weald accepts no responsibility for the loss, theft or damage of such items. Nor will Weald 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 Weald site.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Weald community and any breaches will be dealt with as part of the Weald discipline/behaviour policy.
- Members of staff will be issued with a Weald/work phone number and email address where contact with students or parents/carers is required.
- All members of the Weald community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

- All members of the Weald 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 the Weald 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 Weald's policies.
- Weald mobile phones and devices must always be used in accordance with the AUP
- Weald mobile phones and devices used for communication with parents and students must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Students use of personal devices and mobile phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by students will take place in accordance with the Acceptable Use policy.
- Mobile phones and personal devices will be switched off and kept in secured lockers, out of sight during classroom lessons and while moving between lessons.
- Wearable technologies, such as smart watches, headphones and other smart devices, are not allowed in lessons and the same rules as mobile phones apply.
- Mobile phones or personal devices will not be used by students during lessons or formal Weald time unless as part of an approved and directed curriculum based activity with consent from a member of the Senior Leadership Group. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If members of staff have an educational reason to allow students to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by Senior Leadership Group.
- If a student needs to contact his/her parents/carers he/she will be allowed to use a Weald phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the Weald office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the headteacher.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student breaches the policy, the phone or device will be confiscated and will be held in a secure place.
  - Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
  - Searches of mobile phone or personal devices will only be carried out in accordance with our policy. www.gov.uk/government/publications/searching-screening-and-confiscation)
  - Students' mobile phones or devices may be searched by a member of the Senior Leadership Group, with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. www.gov.uk/government/publications/searching-screening-and-confiscation)
  - Mobile phones and devices that have been confiscated will be released to parents or carers.
  - If there is suspicion that material on a student'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.
- Where students' mobile phones or personal devices are used when learning at home, such as in response to local or full lockdowns, this will be in accordance with our Acceptable Use Policy.

4.5 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting students, young people and their families within or outside of Weald in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with a senior leader.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with students and will only use work-provided equipment during lessons/educational activities.
- 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 Senior Leadership Group 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 Weald 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 and allegations will be responding to following the allegations management policy.

- Where remote learning activities because of Covid-19, staff will use Weald of Kent 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.

4.6 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with Weald's policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with Weald's Photographic Image Use policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

5 Policy Decisions

5.1. Reducing online risks

- Weald is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and Weald's Senior Leadership Group will ensure that appropriate risk assessments are carried out before use in school is allowed.
  - Weald will ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content.
  - Our 'Impero' monitoring system and 'lightspeed' filtering system will:
    - Inspect everything that is typed or done;
    - Take screen shots and will report any suspicious use detected;
    - Detect when proxy bypass sites have been used;
    - Help stop downloads of obscene or offensive content;
    - Potentially get an early warning of predator grooming;
    - Can help warn when students are planning to meet people they do not know;
    - Help pick up 'cries for help' helping to:
      - Reduce fears over suicide, self-harm and abuse;
      - Take appropriate action quickly;
      - Strengthen your pastoral care.

- Weald will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a Weald computer or device.
- Weald will audit technology use to establish if the online safety (e–safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the Senior Leadership Group.
- Filtering decisions, Internet access and device use by students and staff will be reviewed regularly by the Senior Leadership Group.

5.2. Internet use throughout the wider Weald community

- Weald will liaise with local organisations to establish a common approach to online safety (e–safety).
- Weald will provide an AUP for any guest/visitor who needs to access the Weald computer system or Internet on site.

5.3 Authorising Internet access

- Weald will maintain a current record of all staff and students who are granted access to Weald's electronic communications.
- All staff, students and visitors will read and sign Weald's AUP before using any Weald ICT resources.
- Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read Weald's AUP for student access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the Weald community (such as with students with special education needs) Weald will make decisions based on the specific needs and understanding of the student(s).

6 Engagement Approaches

6.1 Education and engagement with learning

- We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible Internet use amongst students 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 students in the effective use of the Internet to research; including the skills of knowledge location, retrieval and evaluation;
  - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- We will support students 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 students that network and Internet use will be monitored for safety and security purposes and in accordance with legislation;
  - Rewarding positive use of technology with House Points;
  - Implementing appropriate peer education approaches;
  - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments;
  - Seeking student 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.

6.2 Engagement and education of children and young people who are considered to be vulnerable

- Weald of Kent Grammar recognises that some students are more vulnerable online owing 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.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.
- When implementing an appropriate online safety policy and curriculum Weald will seek input from specialist staff as appropriate, including the SENCO and Student Services staff.

6.3 Engagement and education of staff

- The online safety (e-safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of Weald safeguarding practice.
- To protect staff and students, Weald will implement an AUP which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Senior Leadership Group and will have clear procedures for reporting issues or concerns.
- Weald will highlight useful online tools which staff should use with students in the classroom. These tools will vary according to the age and ability of the students.
- Staff will be made aware that their online conduct out of Weald could have an impact on their role and reputation within Weald. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

- Weald recognises that parents/carers have an essential role to play in enabling students to become safe and responsible users of the Internet and digital technology.
- Parents’ attention will be drawn to Weald’s online safety (e-safety) policy and expectations in communications, such as letters and the Weald website.
- We will build a partnership approach to online safety with parents/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;
  - 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.

7. Managing Information Systems

7.1 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 Weald’s data protection policy.

7.2 Security and Management of Information Systems

- The security of Weald 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 Weald's network will be regularly checked.
- The network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the Weald network will be enforced for all but the youngest users.
- All users will be expected to log off devices if systems are unattended.
- Weald will log and record Internet use on all Weald owned devices.

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 students 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 Weald systems. Staff are responsible for keeping their password private.
- From Year 7*,* all students are provided with their own unique username and private passwords to access Weald systems. Students are responsible for keeping their password private.
- We require staff and students to use strong passwords for access into our system.

7.3 Filtering Decisions

- Weald of Kent Governing Body and Senior Leadership Group have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit students' exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- 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 Senior Leadership Group; all changes to the filtering policy are logged and recorded.
- The Senior Leadership Group will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- Staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

7.4 Management of applications (apps) used to record student progress

- The Headteacher is ultimately responsible for the security of any data or images held of students.
- Apps/systems which store personal data will be risk assessed prior to use.
- Personal staff mobile phones or devices will not be used for any apps which record and store student's personal details, attainment or photographs.
- Only Weald issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.

- Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

8. Responding to Online Incidents and Concerns

- All members of the Weald community will be informed about the procedure for reporting online safety (e-safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- A DSL will be informed of any online safety (e-safety) incidents involving child protection concerns, which will then be recorded.
- A 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 Weald's complaints procedure.
- Complaints about online bullying will be dealt with under Weald'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).
- Students, parents and staff will be informed of Weald's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the Weald community will need to be aware of the importance of confidentiality and the need to follow the official Weald procedures for reporting concerns.
- All members of the Weald 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 Weald community.
- Weald will manage online safety (e-safety) incidents in accordance with the Weald discipline/behaviour policy where appropriate.
- Weald will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, Weald 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 Weald will contact the Education Safeguarding Team or Kent Police via 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 Weald 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 Weald then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.
- Parents and students will need to work in partnership with Weald to resolve issues.

Appendix A

9. Procedures for Responding to Specific Online Incidents or Concerns
9.1 Responding to concerns regarding Youth Produced Sexual Imagery (“Sexting”)

- Weald 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”.
- Weald 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.
- 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:
    - 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;
        - 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;
    - 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 students to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board’s procedures;
    - Ensure the DSL (or deputy) responds in line with the ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance;
    - Store the device securely;
        - 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.
    - Carry out a risk assessment which considers any vulnerability of students involved; including carrying out relevant checks with other agencies;
    - Inform parents/carers, if appropriate, about the incident and how it is being managed;
    - 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;
    - Provide the necessary safeguards and support for students, such as offering counselling or pastoral support;
    - Implement appropriate sanctions 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 UKCCIS: ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ 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.
    - Review the handling of any incidents to ensure that best practice was implemented; the Senior Leadership Group will also review and update any management procedures, where necessary.

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

- Weald will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Weald recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
    - We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to students and other members of our community on the Weald website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures;
    - If appropriate, store any devices involved securely;
    - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk;
    - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies);
    - Inform parents/carers about the incident and how it is being managed;
    - Provide the necessary safeguards and support for students, 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 child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, students 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 we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or Kent Police.
- If 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 DSL (or deputy).
- If students at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

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

- Weald will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- 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 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 (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures;
  - Store any devices involved securely;
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police.
- If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or deputy) is informed;
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk ;
  - Ensure that any copies that exist of the image, for example in emails, are deleted;
  - Report concerns, as appropriate to parents/carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
  - Ensure that the DSL (or deputy) is informed;
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk ;
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate);
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only;
  - Report concerns, as appropriate to parents/carers.
  - If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the Headteacher is informed in line with our managing allegations against staff policy;
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy;
    - Quarantine any devices until police advice has been sought.

9.4. Responding to concerns regarding radicalisation or extremism online

- Weald will take all reasonable precautions to ensure that students are safe from terrorist and extremist material when accessing the Internet in school and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a student may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with Weald's Safeguarding policy.
- If we are concerned that staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

9.5. Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the Weald's community will not be tolerated. Full details are set out in Weald 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 Weald community affected by online bullying.
- If Weald is unclear if a criminal offence has been committed, then the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- Weald will take steps to identify the bully where possible and appropriate. This may include examining Weald system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Students, staff and parents/carers will be required to work with Weald to support the approach to cyberbullying and Weald's e-safety ethos.
- Sanctions for those involved in online or cyberbullying may include the following.
    - Those involved being asked to remove any material deemed to be inappropriate or offensive.
    - A service provider being contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at Weald for the user for a period of time. Other sanctions for students and staff may also be used in accordance to Weald's anti-bullying, behaviour policy or AUP.
    - Parent/carers of students involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

9.6. Responding to concerns regarding Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Weald of Kent Grammar and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or Kent Police.

Author/s:	Ken MacSporran	**Date:**	October 2021
Next Review Date:	October 2022	**Link Trustees:**	Quality of Care Committee
Ratified:	December 2021 FTB Meeting		