Kings Langley School
Unlocking Potential for Life

Online Safety Policy

Date Agreed – September 2025

Review Date – September 2026

Contents

Online Safety Policy

Technology is a useful servant but a dangerous master.

- ***Christian Lous Lange***

Rationale

This policy exists to provide a framework for supporting our stated aim of "ensuring the happiness of every individual in our community", to promote a climate which enables all students to flourish, regardless of ability or special needs, and supports our desired outcomes of developing "strong character".

Purpose

Kings Langley School recognises that internet, mobile and digital technologies provide positive opportunities for students and young people to learn, socialise and play, but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. As a School of Character, we aim to develop students' decision making and abilities to make appropriate and good choices, which should support the targeted advice, guidance and curriculum work that students receive regarding their safety online. We are, therefore, committed to ensuring that all students, staff and governors will be supported to use internet, mobile and digital technologies safely and without detriment to their well-being or health. This is part of our safeguarding responsibility. Staff are aware that some students may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with students and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part helping children and young people navigate the online world safely and confidently.

Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.
The named Online Safety Lead in this school is **Mrs L Harris**
All breaches of this policy must be reported to **Mrs L Harris**
All breaches of this policy that may have put a child at risk must also be reported to the Designated Safeguarding Lead, **Mr G Searle**.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when students are on site in the care of the school, then the safeguarding of students is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

Scope of policy

The policy applies to:

- students
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents:

- Safeguarding: Keeping Children Safe in Education
- GDPR privacy notices for parents and students
- Data protection
- Health and safety
- Home–school agreement
- Home Learning (Homework)
- Behaviour management
- Anti-bullying
- PSHE/RSE
- Careers education and guidance

These are available on our website: *https://www.kls.herts.sch.uk/about-us/school-policies/*

Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for students, parents/carers, staff and governors and all other visitors to the school.

i) Use of email

Staff and governors should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students, parents or conduct any school business using a personal email address.

Students should use school approved accounts on the school system for educational purposes. Where required, parent/carer permission will be obtained for the pupil account to exist.

For advice on emailing, sharing personal or confidential information or the need to gain parent permission, refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and students should not open emails or attachments from suspect sources and should report their receipt to **Mr D Brookes**, ICT Strategic Lead or **Mr J Leek**, ICT Support Manager.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

ii) Visiting online sites and downloading

Staff must preview sites, software and apps before their use in school or before recommending them to students. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. When working with students searching for images, this should be done through Google Safe Search, which is the school's standard through the HfL Broadband.

Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer, **Mrs D Bell**, with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. Staff must only use pre-approved systems if creating blogs, wikis or other online content in order to communicate with students or parents/carers.

All users must observe copyright of materials from electronic sources.

When working with pupils searching for images, this should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:
Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e.

images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bombmaking, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must also not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Interfere, adapt or alter images, videos or other materials that would bring embarrassment, intimidate or threaten others
- Use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

If using the Office365 website, the password should not be automatically saved (unless it requires additional authentication such as Touch/Face ID). Staff should not be using the Mail App for instance, as this is available without any additional security. At the very least they should use the Microsoft Outlook application with Touch/Face ID setup so family members could not open the work e-mail account without this additional security.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Headteacher in liaison with the appropriate SLT members.

iii) Storage of Images

Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the

written consent of parents/carers which is secured in the first instance on a student's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time (see GDPR and data protection policies for greater clarification).

Photographs and images of students are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the Data Protection Officer. Staff and students may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some students who are at risk and must not have their image put online and others who do not want their image online. For these reasons, parents/carers must follow the school's Acceptable User Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own children.

Staff and other professionals working with students, must only use school equipment to record images of students whether on or off site (also see the GDPR and data protection policies). Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

iv) Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of students.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child. When a parent/carer is on school premises but not in a designated area, their phones must be switched off and out of sight.

Students are allowed to bring personal mobile devices to school but must not use them during school time unless they have direct permission by a teacher. In lesson times all such devices must be switched off.
Under no circumstance should students use their personal mobile devices/phones to take images of:

- any other student unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device (please also refer to the school's mobile phone policy).

Personal mobiles must never be used to access school emails and data. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device.

v) New technological devices or platforms

New personal technological devices or platforms may offer opportunities for teaching and learning. However, the school must consider the educational benefits and carry out risk assessments before the use of them is allowed.

Parents/carers, students and staff should not assume that new technological devices will be allowed to be used for school purposes and should check with the Headteacher before they are brought into school.

Where users use platforms, such as Teams or Zoom from home, there is an expectation that by logging onto this platform, they are agreeing to the school's Acceptable Use Agreement.

Staff, students and Governors must only use school emails, Teams or SharePoint to communicate to arrange meetings on these platforms.

New technology devices may be school owned/provided or personally owned and might include:

- smartphones/smart watches
- tablets
- notebook/laptops
- other technology that usually has the capability of utilising the school's wireless network

The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage. All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Student **should not** use their personal hot spotting and must not connect to the VPN whilst using their own device on school grounds to use their device at school. They should always log into the school's internet.

The school allows the following use of mobile technologies:

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only				Yes	Yes	Yes

Personal devices (when allowed) only have Internet Access and no access to the network (including printing)

* All 6th form accounts are able to connect to the KLS-BYOD wireless network on personal devices. Other students, when authorised/requested by SEND can connect to KLS-BYOD

The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices:

- All laptops are currently managed by the client/server network
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. internet only access, network access allowed, shared folder network access)

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- All school devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access (in some specific cases e.g. printing)
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the **school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school**
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- When using mobile technologies users are expected to act responsibly, safely and respectfully in line with current school acceptable use agreements and safe working practices
- New personal technological devices may offer opportunities for teaching and learning. However, the school must consider the educational benefit and carry out a risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with Network Support before they are brought into school

vi) Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a student or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the student or adult must report the incident immediately to the first available member of staff, the DSL or Headteacher. This will then pass it onto the appropriate pastoral leader in the case of students or the senior line manager for adults. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

In the case of inappropriate images, staff will not look at the images but retain the phone or device as part of further investigations.

vi) Artificial Intelligence (AI)

Generative artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard/ Microsoft Copilot. The Kings Langley School recognises that AI has many uses to help pupils learn, however it may also lend itself to cheating and plagiarism which goes against our Character Virtues.

Staff and students should only use Microsoft Copilot within our domain to ensure that we comply with GDPR guidance and the intellectual property of Kings Langley school. Staff and students are provided with clear training on how to manage the risks of GDPR/data protection, Intellectual property, safeguarding, copyright and quality assurance of outputs to be used as part of our curriculum offer. Please refer to our AI Policy for more details.

Students may use AI tools:

1. As a research tool to help them find out about new topics and ideas with teacher permission and guidance.
2. When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

Students may not use AI tools:

3. During assessments, including internal and external assessments and coursework
4. To write their homework or class assignments, where AI-generated text is presented as their own work (see our Malpractice Policy for exams and NEA)
5. As an alternative to engaging in practical learning.

Kings Langley School considers any unattributed use of AI-generated text or imagery to be plagiarism, and will follow our plagiarism procedures as set out in our exam and plagiarism guidelines.

To ensure students remain safe using AI we will integrate AI-specific modules within their E-Safety curricula, ensuring comprehensive coverage of potential risks and safeguards.

We will regularly communicate, through our newsletters and website, to keep students and parents well-informed of the latest developments in AI and E-Safety. Annual workshops for parents on Online Safety are delivered ensuring students practise safe online behaviour even at home.

Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive, age-appropriate curriculum for online safety which enables students to become informed, safe and responsible. This includes

teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum and the Relationships and Sexual Health (RSE) curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Students are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies.

Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)
- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images
- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help
- How the law can help protect against online risks and abuse

Staff and Governor training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

- New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with students
- Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B)
- Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B)
- Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix C)

Working in partnership with parents and carers

The school works closely with families to help ensure that students can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix E. The Acceptable Use Agreement explains the school's expectations and student and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to students and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged through completion of an incident form which will be recorded on C-POMs centrally. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports students and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

Appendices

A. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement, and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff, student teachers and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Data Protection Officer, **Mrs D Bell**, Online Safety Coordinator, **Mrs L Harris** or the DSL, **Mr G Searle**. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

- ☐ I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

- ☐ I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute (also see Code of Conduct policy)
- ☐ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see Online Safety policy).
- ☐ I will report any accidental access to or receipt of inappropriate materials or filtering breach to my senior line manager.
- ☐ I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required. I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to students and/or parents/carers.
- ☐ I will follow guidelines on how to use Teams or other platforms and will set the security settings that are prescribed.
- ☐ I will only use Teams a method for inviting students to online sessions (or equivalent) and will not share access codes or passwords with anyone else.
- ☐ When on Teams (or equivalent), I will only admit the appropriate students or staff into the session.
- ☐ I will not use AI tools to complete summative assessments for data drops.
- ☐ I will not upload the intellectual property of Kings Langley School or of student work into any AI tools.
- ☐ I must use AI approved tools from the KLS AI toolkit which are GDPR compliant.

Social networking

- ☐ I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or students on social networks.
- ☐ Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.
- ☐ Students may not be considered 'friends' until they have left the school for more than two years and are over the age of 19 (see also Code of Conduct Policy).
- ☐ When using social networking for personal use I will ensure my settings are not public.

- ☐ My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or students. Privileged information must remain confidential.
- ☐ I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

- ☐ I understand that there is no occasion when a password should be shared with a student or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- ☐ Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely.
- ☐ Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher, or governing body.
- ☐ Personal or sensitive data taken off site must be encrypted.
- ☐ Personal or sensitive information should not be used with any AI tools.

Images and videos

- ☐ I will only upload images or videos of staff, students or parents/carers onto school approved sites where specific permission has been granted.
- ☐ I will not take images, sound recordings or videos of school events or activities on any personal device, without express permission of the online safety co-ordinator.
- ☐ Where I have videoed a Teams (or equivalent) lesson for students to view at a later stage, this should be deleted from my device or Teams account once it has been uploaded.
- ☐ Where AI generated images are used these need to be clearly referenced and checked for bias, hallucinations and misinformation.

Use of email

- ☐ I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act.
- ☐ I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

- ☐ I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices.
- ☐ I understand that the use of personal devices in school is at the discretion of the Headteacher.
- ☐ When making business calls on my personal device, I will only use the WebEx application which is linked to my extension number on the schools phone system; access to this can be requested from the IT Support Team.
- ☐ I will only use approved personal devices in designated areas and never in front of students.
- ☐ When using personal device and not a school device to access the Office365 website, I will ensure that I do not automatically save the password (unless your device requires additional authentication such as Touch/Face ID).
- ☐ I note that I should not be using the Mail App, as this is available without any additional security. Therefore, if I choose to access school emails on a personal device, I should be using the Microsoft Outlook application with Touch/Face ID setup, so that family members cannot open the work e-mail account without this additional security.

- ☐ I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school. Such a system would ensure as the user I was not saving files locally to my own device and breaching data security.

Additional hardware/software

- ☐ I will not install any hardware or software on school equipment without permission of ICT Support Manager, Mr D Brookes

Promoting online safety

- ☐ I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.
- ☐ I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, students or parents/carers) to the DSL, Mr G Searle.

Classroom management of internet access

- ☐ I will pre-check for appropriateness of all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of students on my phone or laptop.
- ☐ If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Headteacher in liaison with the appropriate senior staff.
- ☐ I will also check the appropriateness of any suggested sites used for home learning.

Video conferencing

- ☐ I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSL. A school-owned device should be used when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature …….. Date ……

Full Name …….. (printed)

Job title ……

B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers

Kings Langley School Online safety lead: Mrs L Harris
Designated Safeguarding Lead (DSL): Mr G Searle

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record, and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the Data Protection Officer, **Mrs D Bell**, the Online Safety Co-ordinator, **Mrs L Harris** or the DSL, **Mr G Searle**. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

- ☐ I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

- ☐ I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute (also see Code Of Conduct policy).
- ☐ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see Online Safety policy).
- ☐ I will report any accidental access to or receipt of inappropriate materials or filtering breach to my senior line manager.
- ☐ I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.
- ☐ I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.
- ☐ Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the appropriate senior leader.
- ☐ I will follow guidelines on how to use Teams or other platforms and will set the security settings that are prescribed.
- ☐ I will only use Teams as a method for inviting students to online sessions (or equivalent) and will not share access codes or passwords with anyone else.
- ☐ When on Teams (or equivalent), I will only admit the appropriate students or staff into the session.
- ☐ I will not use AI tools to complete summative assessments for data drops.
- ☐ I will not upload the intellectual property of Kings Langley School or of student work into any AI tools.
- ☐ I must use AI approved tools from the KLS AI toolkit which are GDPR compliant.

Social networking

- ☐ I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or students on social networks.

- ☐ Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.
- ☐ Students may not be considered 'friends' until they have left the school for more than two years and are over the age of 19 (see also Code of Conduct policy).
- ☐ In my professional role in the school, I will never engage in one to one exchanges with students or parent/carers on personal social network sites.
- ☐ My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or students. Privileged information must remain confidential.
- ☐ I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

- ☐ I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a student or anyone who is not a staff member.

Data protection

- ☐ I will follow all requirements for data protection explained to me by the school.
- ☐ I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- ☐ I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.
- ☐ Personal or sensitive information should not be used with any AI tools.

Images and videos

- ☐ I will only upload images or videos of staff, students or parents/carers onto school approved sites where specific permission has been granted.
- ☐ I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of one-to-one tuition, students or parent/carer devices can be used, with parent/carer agreement.
- ☐ Internet, mobile and digital technologies provide helpful recording functions, but these cannot be made on a teacher's personal device. Recordings can be made with the student's and parent/carer's agreement on a school device, an organisational device approved by the Headteacher, or a young person's or parent/carer's own device.
- ☐ Where I have videoed a Teams (or equivalent) lesson for students to view at a later stage, this should be deleted from my device or Teams account once it has been uploaded.
- ☐ Where AI generated images are used these need to be clearly referenced and checked for bias, hallucinations and misinformation.

Use of Email

- ☐ I will use my professional or formal student email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act.
- ☐ I will not use my professional email addresses for personal matters.

Use of personal devices

- ☐ I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices.
- ☐ I understand that the use of personal devices in school is at the discretion of the Headteacher.
- ☐ When making business calls on my personal device, I will only use the WebEx application which is linked to my extension number on the schools phone system; access to this can be requested from the IT Support Team.
- ☐ I will only use approved personal devices in designated areas and never in front of students. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning.

Additional hardware/software

- ☐ I will not install any hardware or software on school equipment without permission of ICT Support Manager, **Mr D Brookes**.

Promoting online safety

- ☐ I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.
- ☐ I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, students or parents/carers) to the DSL, Mr G Searle.

Classroom management of internet access

- ☐ I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of students on my phone or laptop.
- ☐ If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Head teacher in liaison with the appropriate senior staff.

Video conferencing

- ☐ I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSP. A school-owned device should be used when running video-conferences, where possible.

User Signature

- ☐ I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school.
- ☐ I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature …… Date ……

Full Name …….... (Please use block capitals)

Job Title/Role ……..……

C. Requirements for visitors, volunteers and parent/carer helpers (Working directly with children or otherwise)

Kings Langley School

Online safety lead: Mrs L Harris

Designated Safeguarding Lead (DSL): Mr G Searle

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise any safeguarding concerns arising from your visit immediately with the Headteacher and/or DSL

- ☐ I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- ☐ I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- ☐ I will not give out my personal details such as mobile phone number, email address, and social media account details to students and parent/carers. Where appropriate I may share my professional contact details with parents/carers provided the DSL or headteacher is informed before I leave the school.
- ☐ I understand my visit to the school may give me access to privileged information about students, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- ☐ I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher.
- ☐ If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site.
- ☐ I will not free-surf the internet in front of students on my phone or laptop. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.
- ☐ I will not upload the intellectual property of Kings Langley School or of student work into any AI tools.
- ☐ I must use AI approved tools from the KLS AI toolkit which are GDPR compliant.
- ☐ Where AI generated images are used these need to be clearly referenced and checked for bias, hallucinations and misinformation.

D. Online Safety Acceptable Use Agreement Secondary Pupils

https://forms.office.com/e/HRTnRTXX9e

- ☐ I will only use school IT equipment at school for school purposes.
- ☐ I will not download or install software on school IT equipment.
- ☐ I will only log on to the school network, other school systems and resources using my own school user name and password.
- ☐ I will not reveal my passwords to anyone other than a parent/carer.
- ☐ I will not use my personal email address or other personal accounts on school IT equipment.
- ☐ I will make sure that all my electronic communications are responsible and sensible.
- ☐ I understand my behaviour in the virtual classroom should mirror that in the physical classroom.
- ☐ I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.
- ☐ I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff if I am in school, or parent/carer if I am not in school.
- ☐ I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will report immediately any request for personal information, to a member of staff if I am in school or parent/carer if I am not in school.
- ☐ I should never post photographs, videos or livestream without the permission of all parties involved.
- ☐ I will not upload any images, videos, sounds or words that could upset, now or in the future, any member of the school community, as this is cyberbullying. This includes AI generated images or AI tools.
- ☐ I will be respectful to everyone online. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in the school community or bring the school into disrepute.
- ☐ I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
- ☐ When I receive a Teams meeting code from a teacher, by attending that meeting, I understand I am agreeing to the Acceptable User Agreement.
- ☐ When I receive a Teams meeting code from a teacher, I will not share it with anyone else or encourage anyone to try to attend the meeting.
- ☐ Where Teams meetings are videoed for my benefit, I will only access them through Teams and only use them for their agreed purpose. I will not try to alter or adapt them to bring embarrassment, intimidation or upset to another person.
- ☐ When I attend a Teams meeting, I will be appropriately dressed and in an appropriate working area.
- ☐ I understand that when I am in a Teams meeting, that I must still adhere to the school's behaviour management policy, and if this is not the case, I will be removed from the meeting and the relevant consequences will be issued.
- ☐ I will respect the privacy and ownership of others' work on-line and will adhere to copyright at all times.
- ☐ I will not attempt to bypass the internet filtering system in school.
- ☐ I will not assume that new technologies can be brought into school and will check with staff before bringing in any device.
- ☐ If I bring in my own device to use in school, the school will not be liable for any damage of the device or if the device is stolen. It is the responsibility of the student to ensure the device is appropriately looked after and insured.
- ☐ If given permission to use a personal device in school, I will not connect to a VPN or personal hot spotting whilst using my personal device on school grounds. I will always use the school's internet provider when on the school grounds.
- ☐ I will not lie about my age to sign up for age-inappropriate games, apps or social networks.
- ☐ I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.

- ☐ I will not use AI tools to complete my school work, coursework or homework, unless I have been given permission from my teacher. I must use AI approved tools from the KLS AI toolkit.
- ☐ I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined, and my parents/carers may be contacted. If I break the law the police may be informed.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all students to be safe and responsible when using any IT. It is essential that students are aware of online risk, know how to stay safe and know where to go to report problems and access support.

Students are expected to read and discuss this agreement with you and then sign below to show they will follow the terms of the agreement. Any concerns can be discussed with Online Safety Coordinator, **Mrs L Harris.**

Please can you sign and return the parent/carer agreement below.
This document will be kept on record at the school.

Pupil agreement

Pupil name……
I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature……..

Parent/Carer agreement

Parent/Carer name…….

I have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I agree to support them in following the terms of this agreement. I also agree not to share school related information or images online or to post material that may bring the school or any individual within it into disrepute.

Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, students and parents.

I agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I understand that under no circumstance should images be taken at any time on school premises of anyone other than our own children, unless there is a pre-specified agreement. I understand that when on school premises but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent/carer signature ……

Date ……

E. Online safety policy guide - Summary of parent/carer responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- ☐ Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for students.
- ☐ Parents/carers must understand that by students accessing and attending online sessions, such as Teams, with teachers, they are accepting the Acceptable User Agreement for their child.
- ☐ Where your child receives a meeting code and password for online sessions such as Teams, the meeting codes and passwords must not be shared, and only used by the relevant child. Parents and children should not attempt to attend meetings that they are not invited to.
- ☐ Parents must ensure that their children are suitably dressed and in an appropriate working venue when students attend Teams meetings.
- ☐ Parents accept that whilst their children are attending a Teams meeting, the guidance and boundaries of the school's behaviour management must be adhered to, and where it is contravened, consequences will be issued.
- ☐ Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- ☐ Parents/carers should not assume that students can bring technological devices to school and should always check the school policy.
- ☐ All cyberbullying incidents affecting children in the school should be reported immediately. If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection. The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- ☐ The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- ☐ Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, students and parents/carers.

- ☐ Parent/carers should ensure students do not use AI tools for coursework (NEA) or homework unless given express permission by their teacher. Any work found to be using AI tools without permission will be seen as plagiarism and will be subject to the guidance from JCQ and our malpractice policy.

Please see the full online safety policy in the policies section on the school website.

F. Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- ☐ Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- ☐ Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- ☐ The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.
- ☐ A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- ☐ A senior member of staff will conduct an investigation.
- ☐ Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- ☐ Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

This should be read in conjunction with our behaviour policy.

G. Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix E (Online safety policy guide - Summary of parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts
  - As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.
  - If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the Headteacher will need to follow the school's safeguarding procedures.
  - If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.
  - Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints
  - Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:
- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law

- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

H: Guidance for staff on Safeguarding and remote education during coronavirus (COVID-19)

Useful resources

Below are resources (please note not an exhaustive list) to help schools manage and risk assess any remote teaching and working.

Government guidance on safeguarding and remote education

https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

The Key for School Leaders - Remote learning: safeguarding pupils and staff

https://schoolleaders.thekeysupport.com/covid-19/safeguard-and-support-pupils/safeguarding-while-teaching/remote-teaching-safeguarding-pupils-and-staff/?marker=content-body

NSPCC Undertaking remote teaching safely

https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely

LGfL Twenty safeguarding considerations for lesson livestreaming

https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

swgfl Remote working a guide for professionals

https://swgfl.org.uk/assets/documents/educational-professionals-remote-working.pdf

National Cyber Security Centre Video conferencing. Using services securely
https://www.ncsc.gov.uk/files/vtc_infographic.pdf

Cyber Security Standards for Schools and Colleges – KCSiE 2023

the cyber security standards for schools and colleges