



Online Safety Policy

2026-2029

Kings College Guildford

“Work Hard and be kind and push yourself”

POLICY REVIEW AND AMENDMENT LOG

Statutory or Recommended: Statutory

Review frequency: Every 3 years

Next review date: July 2029

Reviewed By	Review Date	Reviewing Governor	Date Approved by Governing Body
Kate Carriett	July 2013	Matthew Armstrong	July 2013
Anna Wallis	June 2016	Bob Arnold	26/09/2016
Anna Wallis	July 2019	Bob Arnold	26/09/2019
Anna Wallis	August 2020	Mick Michell	08/12/2020
Mollie Robberts	July 2023	Jo Oliver	12/10/2023
Rebecca Francis	September 2026	Ahmed Naas	06/10/2026

Contents

<u>1. Aims</u>	<u>3</u>
<u>2. Legislation and guidance</u>	<u>4</u>
<u>3. Roles and responsibilities</u>	<u>4</u>
<u>4. Educating pupils about online safety</u>	<u>7</u>
<u>5. Educating parents/carers about online safety</u>	<u>9</u>
<u>6. Cyber-bullying</u>	<u>10</u>
<u>7. Acceptable use of the internet in school</u>	<u>11</u>
<u>8. Pupils using mobile devices in school</u>	<u>12</u>
<u>9. Staff using work devices outside school</u>	<u>12</u>
<u>10. How the school will respond to issues of misuse</u>	<u>12</u>
<u>11. Training for staff, governors and volunteers</u>	<u>13</u>
<u>12. Monitoring arrangements</u>	<u>13</u>
<u>13. Links with other policies</u>	<u>13</u>

1. Aims

Our school aims to:

- o Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- o Identify and support groups of pupils that are potentially at greater risk of harm online than others
- o Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- o Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- o **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- o **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- o **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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
- o **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- o Teaching online safety
- o Meeting digital and technology standards
- o Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- o Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- o Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- o Reviewing filtering and monitoring provisions at least annually
- o Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- o Having effective monitoring strategies in place that meet the school's safeguarding needs

All governors will:

- o Make sure they have read and understand this policy
- o Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- o Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- o Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Principal

The Principal is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and the wider safeguarding team are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- o Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- o Working with the headteacher and governing board to review this policy every three years and make sure the procedures and implementation are updated and reviewed regularly
- o Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- o Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- o Working with the ICT manager to make sure the appropriate systems and processes are in place
- o Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- o Managing all online safety issues and incidents in line with the school's child protection policy
- o Responding to safeguarding concerns identified by filtering and monitoring
- o Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- o Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- o Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- o Liaising with other agencies and/or external services if necessary
- o Providing regular reports on online safety in school to the headteacher and/or governing board
- o Undertaking annual risk assessments that consider and reflect the risks pupils face
- o Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- o Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- o Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- o Conducting a full security check and monitoring the school's ICT systems regularly
- o Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- o Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- o Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- o Maintaining an understanding of this policy
- o Implementing this policy consistently
- o Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- o Following the correct procedures by informing our ICT system if they need to bypass the filtering and monitoring systems for educational purposes
- o Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- o Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- o Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- o Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- o Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- o What are the issues? – [UK Safer Internet Centre](#)
- o Help and advice for parents/carers – [Childnet](#)
- o Parents and carers resource sheet – [Childnet](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

4.1 Pupils will be taught about online safety as part of the curriculum

All schools have to teach:

- o [Relationships education and health education](#) in primary schools
- o [Relationships and sex education and health education](#) in secondary schools

In **KS3**, pupils will be taught to:

- o Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- o Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- o To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- o How to report a range of concerns

By the **end of secondary school**, pupils will know:

- o Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- o Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- o The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- o Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- o That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- o What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- o About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- o That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- o That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- o How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- o That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- o How information and data is generated, collected, shared and used online
- o That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- o That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- o That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable

children, victims of abuse and some pupils with SEND.

4.2 Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- o Methods that hackers use to trick people into disclosing personal information
- o Password security
- o Social engineering
- o The risks of removable storage devices (e.g. USBs)
- o Multi-factor authentication
- o How to report a cyber incident or attack
- o How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- o What systems the school uses to filter and monitor online use
- o What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

Kings College takes a staged approach to managing bullying (see stages 1 to 8 below). Throughout these stages the bully will be offered a variety of interventions to help them change their behaviour as outlined below.

Bullying Interventions/Support

The following support/interventions will be offered the bully where appropriate:

- Pastoral Support (e.g. reports; mentorship)
- Behavioural Support (e.g. 1-1 sessions)
- Referral to local support (e.g. Youth Worker, Youth Engagement Officer [Police])
- CAMHS referral
- Alternative Learning Provision(ALP)
- Social care referral
- SEND support

8 Stage Process:

1. **Unkindness Warning 1** – This is logged when a student has displayed unkind behaviour. Students are informed that the behaviour is unkind and spoken to about kind conduct within school. Students are verbally informed they have received an 'Unkindness Warning 1' and a 'Warning 1' log is issued on classcharts for tracking purposes. Students will typically receive a lunch time detention for this behaviour. Warning stages can be passed if the behaviour is deemed 'inappropriate' or extremely unkind.
2. **'Unkindness Warning 2'** – This is logged when a student has displayed unkind behaviour for a second time. Students are informed that the behaviour is unkind and spoken to about kind conduct within school. Students are verbally informed they have received an 'Unkindness Warning 2' and a 'Warning 2' log is issued on classcharts for tracking purposes. Students will typically receive a lunch time detention for this behaviour. Warning stages can be passed if the behaviour is deemed 'inappropriate' or extremely unkind.
3. **Level 1 Bullying Warning - VERBAL ADVICE SLIP** – is the third stage and is suitable for 'inappropriate' behaviour that *could* be perceived as bullying should it continue. A member of senior staff will discuss this with the student, issue the 'verbal advice slip' to the student and the slip kept in the student's file. A log is placed on Classcharts for 'Level 1 bullying' issue with details of the incident for tracking purposes. Students will typically receive a detention at this stage and parents are informed. Should the behaviour continue after the verbal advice has been given, it *will* be considered bullying, and the process will escalate to the next stage.
4. **Level 2 Bullying Warning - VERBAL WARNING SLIP** – is the fourth stage and parents will be informed at this stage. It is suitable for 'bullying' behaviour that *is* classed as bullying. Typically, this second level is issued if the same or similar behaviour did not cease since the verbal advice slip was issued. A member of senior staff issues the 'verbal warning slip' to the student, discusses the situation, contacts parents and the slip is kept in the student's file. A log is placed on SIMS for 'Level 2 Bullying' for tracking purposes. Students will typically receive an after-school detention at this stage and be placed onto Pastoral support.
5. **Level 3 Bullying Warning - WRITTEN WARNING SLIP** – is the fifth stage and parents will be required to attend a meeting with the Pastoral Lead, Assistant Principal, Vice Principal or Principal at this stage. This third level will be issued if the same or similar behaviour has continued despite the first steps in the process being followed. It could be that the student has targeted the same student(s) again or has repeated the same behaviour to a different student or group. A member of senior staff issues the 'written warning slip' to the student and parents at the meeting and the slip is kept in the student's file. A log is placed on SIMS for 'Level 3 Bullying' for tracking purposes. If the behaviour continues after the verbal warning slip has been given, the process will again escalate. Students will typically receive a fixed-term exclusion at this stage and be placed on Senior Leader Report to the member of SLT responsible for behaviour.
6. **FORMAL WRITTEN WARNING 1** – is the sixth stage and parents will be required to attend a formally recorded meeting with the Pastoral Lead or Assistant Principal. This stage will be issued if the same or similar behaviour has continued despite the previous stages being followed. It could be that the student has targeted the same student(s) again or has repeated the same or similar behaviour to a different student or group. The student will set targets to ensure the behaviour does not occur again and will meet (bi)weekly for a set period to monitor progress towards these targets. The student will complete one session of intervention which will be specific to the behaviours that have been displayed. A signed copy of intervention completion will be placed into the students file and a log for 'Formal Written Warning 1' will be placed onto ClassCharts. Should bullying behaviour continue after Formal Written Warning 1 has been given, the process will escalate to the next stage. Student will typically receive a substantial after school detention or a fixed-term exclusion at this stage.
7. **FORMAL WRITTEN WARNING 2** - is the seventh stage and parents will be required to attend a meeting with the Vice Principal or Head Teacher and possibly a member of the school's Governing Body. It is likely that the police will become involved at this stage if they haven't already. This stage will be issued

if the same or similar behaviour has continued despite the previous steps in the process being followed. It could be that the student has targeted the same student(s) again or has repeated the same or similar behaviour to a different student or group. The Head Teacher issues the Final Written Warning letter to the student and parents at the meeting and a copy of the letter is given to parents and a copy kept in the student's file. The student will be required to complete a multi-session programme of intervention within the school. The programme will be focussed on addressing the bullying behaviours and a signed copy of completion will be placed into the student's file. A log is placed on Classcharts for 'Formal Written Warning 2' for tracking purposes. Should bullying behaviour continue after the Final Written Warning Letter has been given, the process will escalate to the final stage. Students will typically receive a fixed-term exclusion at this stage as well as placed on a Behaviour Contract.

8. **Direction to Alternative Provision/Permanent Exclusion** - we are committed to maintaining a safe and happy environment for all of our students and, as such, will not allow any student to be relentlessly unkind to others. In the rare circumstance that the bullying behaviour continue despite the first four steps in the process being followed, the student/parents will be issued notice of permanent exclusion or a permanent placement at an alternative provision organised. It could be that the student has targeted the same student(s) again or has repeated the same or similar behaviour to different students.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- o Poses a risk to staff or pupils, and/or
- o Is identified in the school rules as a banned item for which a search can be carried out, and/or
- o Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- o Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from another member of the SLT team.
- o Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- o Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- o Cause harm, and/or
- o Undermine the safe environment of the school or disrupt teaching, and/or
- o Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, Principal or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- o They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- o The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- o **Not** view the image

- o Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- o The DfE's latest guidance on searching, screening and confiscation
- o UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- o Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Kings College recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Kings College will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by Kings College, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- o Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- o Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- o Making sure the device locks if left inactive for a period of time
- o Not sharing the device among family or friends
- o Installing anti-virus and anti-spyware software
- o Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies and home school agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training for staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- o Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- o Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- o Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- o Develop better awareness to assist in spotting the signs and symptoms of online abuse
- o Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- o Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL all those on the safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed by the Assistant Principal every three years. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- o Child protection and safeguarding policy
- o Behaviour policy
- o Staff disciplinary procedures
- o Data protection policy and privacy notices
- o Complaints procedure
- o ICT and internet acceptable use policy

ICT Code of Conduct

2023 - 2026

Kings College Guildford
“Work hard, be kind and push yourself”



This policy should be read alongside the Trust Data Protection policy.

ICT and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in College. These policies and agreements are designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this document and adhere at all times to its contents. Any concerns or clarification should be discussed with the Kings College Guildford's e-safety co-ordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDA's, digital cameras, e-mail, social networking and that ICT may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a College ICT system for a purpose not permitted by its owner.
- I will comply with the ICT system security and not disclose any passwords provided to me by the College or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the College's e-mail / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Principal or the Governing Body.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in College, taken off the College premises or accessed remotely. Personal data can only be taken out of College or accessed remotely when authorised by the Principal or Governing Body.
- I will not install any hardware or software without prior permission from Network Manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Principal.
- I will respect copyright and intellectual property rights.
- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the College network / learning platform without the permission of the parent/carers, member of staff or the Principal.
- I will ensure my online activity, both in College and outside College, will not bring my professional role into disrepute.
- I will ensure that all electronic communications with family, students and staff, including e-mail, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will support the College's e-safety policy and help students to be safe and responsible in their use of ICT related technologies. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the e-safety Co-ordinator, the Child Protection Liaison Officer or the Principal.
- I understand that sanctions for disregarding any of the above will be in line with the College's disciplinary procedures and serious infringements may be referred to the police.
- I understand that the school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Mobile Device Guidance for Staff, Governors or Visitors

Mobile Phone Acceptable Use Policy

The widespread ownership of mobile phones requires that school administrators, teachers, family and carers take steps to ensure that mobile phones are used responsibly at school. This Acceptable Use Policy has been designed to ensure that potential issues involving mobile phones can be clearly identified and addressed.

General Use of Mobile Phones

- Mobile phones and personally owned devices brought into College are the responsibility of the device owner. The College accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- The Bluetooth functionality of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally owned mobile devices without the prior consent of the person or people concerned.

Staff Acceptable Use of Mobile Phones

- In line with our 'Phone Free School' policy for students, staff use of mobile phones during the College day should be limited. Mobile phones will be kept out of sight during classroom lessons, assemblies, whilst moving through the corridors and when in the library.
- During free time only, and away from students, staff will be permitted to use mobile devices.
- Mobile phones should not be used in any manner or in any location that could cause disruption to the normal routine of the College.
- Staff should ensure that their phones are PIN protected in case of loss or theft. This is to protect the staff from their number falling into the wrong hands.
- When on a College trip staff will be issued with a College mobile where contact with students, family or carers is required. If staff need to contact family or carers whilst at College they will use a College based landline in departments or College offices.

Governor and Visitor Acceptable Use of Mobile Phones

- Governors and Visitors use of mobile phones on the College site and during the College day should be limited. Mobile phones will be kept out of sight whilst in classrooms, moving through the corridors and when in the library.
- If Governors and Visitors need to use mobile phones they are to do so in privacy and away from students.

- Mobile phones should not be used in any manner or in any location that could cause disruption to the normal routine of the College.
- Governors and Visitors should ensure that their phones are PIN protected in case of loss or theft. This is to protect them from their number falling into the wrong hands

Acceptable Use Agreement

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that staff will have good access to digital technologies to enhance their teaching and will, in return, expect staff to agree to be responsible users.

Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

I understand that the following provides guidance to staff on the appropriate use of the school network. However, this is not a definitive list and staff should use their judgement to ensure the safety of all.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of dangers associated with contact with strangers when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line or any other information by which I or my location could be identified (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, location etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. (Please do not delete so that this can be used should evidence be required)

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, personal financial gain, political purposes, advertising or video broadcasting (e.g. YouTube), unless I have permission to do so.



- I will not search for, create, transmit, download or print inappropriate or illegal web content such as but not limited to any offensive, obscene, pornographic or indecent images, data or other material, or any data capable of being resolved into pornographic or indecent images or material; separately

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. Copyright and intellectual property rights must be respected.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. As messages may be forwarded, messages should be regarded as public property.
- I will not take or distribute images of anyone without their permission.
- I will not send mass messages or anonymous messages.
- I am aware that the school reserves the right to monitor all my electronic communications accessed via school systems. (RIP Act 2000)

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission and I understand that, if I do use my own devices in the school I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any program or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email or message, or if I have any concerns about the validity of the email or message (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, and, in the event of illegal activities, involvement of the police.

Bring Your Own Device Terms and Conditions of Use

Note : Kings College Guildford cannot guarantee the speed of access to the internet.

- I understand that my device should have an appropriate level of security and that anti-virus is my responsibility.
- I will ensure my personal device is insured against theft, loss and damage.
- I am aware that in order to prevent unauthorised access to my device I should have a password with auto-lock.
- I understand that my personal device is my responsibility.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in this document. If you do not sign and return this agreement, access will not be granted to school systems and devices. If you breach any of these terms and conditions of use, your permission to use Kings College IT services will be terminated.

Agreement Form

This form relates to the 'ICT Code of Conduct', 'Mobile Device Guidance for Staff, Governors or Visitors', 'Acceptable Use Agreement' and the

‘Acceptable Use Policy Agreement’

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school
- I use my own equipment out of the school / academy in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name

Signed

Date

