King's Academy Gomer

Online Safety Policy

Approved by:	Local Governing Body	Date:	16.7.2024
Maintained by:	Georgina Mulhall	Next review due:	September 2026

1. Aims

King's Group Academies schools aim to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate our school's communities in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- 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:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **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 them for sexual, criminal, financial or other purposes
- **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
- **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:

- Teaching online safety in schools
- Preventing and tackling bullying and Cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- 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 students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

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

3. Roles and Responsibilities

3.1 The Local Governing Board (LGB)

The LGB has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The LGB 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 LGB 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 LGB will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Governing Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure 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 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:

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

The governor who oversees online safety is Mr Justin Allen.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students 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 Headteacher

The Headteacher is responsible for ensuring 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 deputies 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:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Working with the Head of IT to make sure the appropriate systems and processes are in place
- Working with the Headteacher, Head of IT and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Head of IT

The Head of IT is responsible for:

- 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 the effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this 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:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that students follow the school's terms on acceptable use (appendices 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by alerting gj-safeguarding@kgagomer.uk and ithelpdesk@kgahampshire.uk as well as reporting concerns directly impacting children on MyConcern using the procedures detailed in the child protection and safeguarding policy.

- Following the correct procedures by alerting gj-safeguarding@kgagomer.uk and ithelpdesk@kgahampshire.uk as well as reporting concerns directly impacting children on MyConcern using the procedures detailed in the child protection and safeguarding policy, if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- 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:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure 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:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent 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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2), this is included as part of our lettings agreement.

4 Policy Decisions

4.1 Reducing Online Risks

- KGA Gomer is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the DPO will ensure that appropriate DPIAs are carried out before use in school is allowed.
    - KGA Gomer will ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content.
    - Our Security monitoring system and 'Smoothwall' filtering system will:
        - Inspect everything that is typed;
        - Take screenshots and will report any suspicious use detected;
        - Detect when proxy bypass sites have been used;
        - Help stop downloads of obscene or offensive content;
        - Potentially get an early warning of predator grooming;
        - Help pick up 'cries for help' helping to:
            - identify references to suicide, self-harm and abuse;
            - Take appropriate action quickly;
            - Identify where further pastoral care is required
- KGA Gomer will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not

possible to guarantee that access to unsuitable material will never occur via a King's Academy Gomer and Gomer 's computer or device.
    - Where breaches to the filtering system occur, staff should notify both safeguarding and it support inline with section 3.5 by emailing the ithelpdesk@kgahampshire.uk
- KGA Gomer will audit technology use to establish if the online safety (e-safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed monthly by SLT, ICT support providers and DSL
- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the DSL SLT.

4.2 Authorising internet access (AUP)

- KGA Gomer will provide an AUP for any guest/visitor who needs to access the KGA Gomer computer system or internet on-site.
- All staff and students will read and sign King's Academy Gomer and Gomer's AUP before using any KGA Gomer ICT resources.
- Students will be provided with supervised internet access which is appropriate to their age and ability.
- Parents will be asked to read King's Academy Gomer and Gomer 's AUP for student access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the KGA Gomer community (such as students with special education needs) KGA Gomer will make decisions based on specific needs and understanding of the student(s).
- Volunteers, contractors, governors, members and trustees may be given access to the guest wireless network. Volunteers and Contractors will have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- Visitors may request the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

5. Online Communication and Safer Use of Technology

5.1 Managing the KGA Gomer website

KGA Gomer will ensure that information posted on our website meets the statutory requirements as identified by the Department for Education (DfE).

KGA Gomer will ensure that its website complies with guidelines for publications including:

- accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or students' personal information will not be published on King's Academy Gomer's website without explicit permission. With parental consent, images of pupils will be shared.
- The administrator account for the KGA Gomer website will be secured with an appropriately strong password and multi-factor authentication.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

5.2 Publishing images and videos online

- KGA Gomer will ensure that all images are used in accordance with King's Academy Gomer 's Photographic Image Use policy.

5.3 Managing Email

- Students may only use KGA Gomer provided email accounts for school related learning and matters which extends to them emailing their peers.

- All staff, and governors are provided with a specific KGA Gomer email address to use for any official communication.
- The use of personal email addresses by staff for any official KGA Gomer business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and/or encrypted methods.
- Sensitive or personal information will be shared via email in accordance with data protection legislation.

5.4 Official video conferencing and webcam use

- Video conferencing contact information will not be posted publicly.
- Staff will ensure that external video conferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure (not a public wifi access point).
- Students will not use, or have access to, video conferencing equipment without permission.

Users

- Video conferencing will be supervised appropriately for the students' age and ability.
- Parents'/carers' consent will be obtained prior to students taking part in video conferences with anyone outside of KGA Gomer community.
- Video Conferencing will take place via official and approved communication channels
- Unique login details for educational video conferencing services will only be issued by staff and kept secure.

Content

- When recording a video conference lesson, the reason for recording must be given and the recording of the video conference should be clear to all parties at the start of the conference. Recorded material will be stored securely.

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

- KGA Gomer internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- Students will use age and ability-appropriate tools to search the internet for content.
- Internet use is a key feature of educational access and all students will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- KGA Gomer will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- All staff are aware that they cannot rely on filtering alone to safeguard students and supervision, classroom management and education about safe and responsible use is essential.
- Students will be appropriately supervised when using technology, according to their ability and understanding.
- All devices will be used in accordance with King's Academy Gomer's AUP and with appropriate safety security measures in place.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- KGA Gomer will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.

- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

5.6 Management of Learning Platforms and Systems

It is important to consider data protection before adopting a cloud platform or service - See our Data Protection Policy. The Trust uses Google Workspace and so most data should be stored on Google Workspace to ensure data security unless there is a 3rd party tool in place, for example, SIMs, Provision Map Classcharts, MyConcern.

The Data Protection Officer (Judicium) and the Digital Learning Lead, analyse and document systems and procedures before they are implemented and regularly review them. The following principles apply:

- SLT, the Digital Learning Lead and staff will regularly monitor the usage of King's Academy Gomer's learning platforms and systems by students and staff in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised about acceptable conduct and use when using King's Academy Gomer's learning platforms and systems.
- Only members of the current student, parents/carers and staff community will have access to King's Academy Gomer's platforms and systems.
- When staff and students leave KGA Gomer their account and/or rights to specific KGA Gomer areas will be suspended.
- The DPO in conjunction with Judicium approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement).
- Only school-approved platforms are used by students or staff to store student work.

6. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

All schools have to teach Relationship Education and Health Education.

Primary schools:

In **Key Stage 1(KS1)**, students will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Students in **Key Stage 2 (KS2)** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, students will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Secondary schools:

In **Key Stage 3 (KS3)**, students will be taught to:

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

Students in **Key Stage 4 (KS4)** will be taught:

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

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

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

All schools

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 students with SEND.

7. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in emails and letters or other communications home (newsletter), and in information via our website or virtual learning environment (VLE - Google Classroom) as well as in person information evenings. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use

- 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 DSL.

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

8. Cyber-bullying

8.1 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.)

8.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and conduct policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8.3 Examining Electronic Devices

The Headteacher, and any member of staff authorised to do so by the Headteacher such as members of SLT and the (Deputy Designated Safeguarding Lead - DDSL team can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- 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:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the DSL.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student'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:

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

If inappropriate material is found on the device, it is up to DSL and wider DDSL and SLT 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 if 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:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student 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:

- **Not** view the image
- 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 students will be carried out in line with:

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

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

8.4 Artificial intelligence (AI)

Generative 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 Gemini.

King's Group Academies recognises that AI has many uses to help students 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.

King's Group Academies will treat any use of AI to bully students in line with our anti-bullying, behaviour and conduct and safeguarding and child protection policy.
Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the King's Group Academies.

9. Acceptable use of the Internet in school

All students, 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 of 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 students, 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.

10. Students using personal and mobile devices in school

10.1 Rationale regarding personal devices and mobile phones

Students in KS2 may bring mobile devices into school, but are not permitted to use them during:

- The school day
- On the school site - this includes both before and after school

Please note:

- They are to be handed to the Class Teacher at the start of the day - *Nb the school cannot take responsibility for personal devices*
- Where exceptions for this are requested by staff these should be sent ithelpdesk@kgahampshire.uk for prior agreement

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

The use of mobile phones and other personal devices by students and adults will be decided by the Mobile Phone policy and AUP.

KGA Gomer recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but requires that such technologies be used safely and appropriately within King's Academy Gomer and Gomer .

10.2 Expectations for safe use of personal devices and mobile phones

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is unacceptable and any breaches will be dealt with as part of the KGA Gomer discipline/behaviour policy.

Members of staff will be issued with a KGA Gomer email address where contact with students or parents/carers is required.

All members of the KGA Gomer community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

All members of the KGA Gomer community will be advised that their mobile phones and personal devices do not contain any content which may be considered offensive, derogatory or would otherwise contravene King's Academy Gomer's policies.

10.3 Students use of personal devices and mobile phones

Students in KS2 may bring mobile devices into school, but are not permitted to use them at any point during the school day and whilst they are on site.

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- Any use of mobile phones and personal devices by students will take place in accordance with the Acceptable Use Policy.
- Mobile phones will be switched off and out of sight during the school day.
- Mobile phones will not be used by students during lessons or formal KGA Gomer time unless as part of an approved and directed curriculum based activity with consent from staff.
- If a student needs to contact his/her parents/carers he/she will be allowed to use a KGA Gomer phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the academy office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by SLT.
- Wearable technologies, such as smart watches are not permitted on site during the school day - please see uniform policy for step tracker watches.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the academies' behaviour policy, which may result in the confiscation of their device for parental collection in line with our mobile phone policy.

10.4 Staff use of personal devices and mobile phones

Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of students and who will only use work-provided equipment for this purpose.

Staff will not use any personal devices directly with students and will only use work-provided equipment during lessons/educational activities.

Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.

Personal mobile phones or devices will not be used during teaching periods unless in emergency circumstances. This needs to be agreed with the Line Manager.

Staff will ensure that any content brought on-site via mobile phones and personal devices are compatible with their professional role and expectations.

If a member of staff breaches KGA Gomer policy then disciplinary action will be taken.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the relevant authorities will be contacted and allegations will be responded to following the Code of Conduct.

Where remote learning activities are put in place, staff will use KGA Gomer provided equipment. If this is not available, staff will only use personal devices with prior approval from the Headteacher. Staff will follow clear guidance outlined in the Acceptable Use Policy.

10.5 Visitors use of personal devices and mobile phones

Parents/carers and visitors must use mobile phones and personal devices in accordance with King's Academy Gomer 's policy.

Staff will be expected to challenge concerns of safe and appropriate use and will always inform the DSL of any breaches of use by visitors.

Visitors and parents/carers must receive permission from SLT to take photos or videos and in accordance with school policies.

11. Staff using work devices outside of school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Please note, the KGA Hampshire IT Team will:

- Install anti-virus and anti-spyware software
- Keeping operating systems up to date by always 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 2. If a member of staff misuses their equipment then this constitutes misconduct and will be dealt with in accordance with the staff code of conduct.

Work devices must be used for appropriate activity.

If staff have any concerns over the security of their device, they must seek advice from ithelpdesk@kgahampshire.uk

12. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on acceptable use and behaviour and conduct. 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.

13. Training

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:

- Technology is a significant component in many safeguarding and well-being issues, and that children are at risk of online abuse

- 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
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

The DSL and deputies 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.

More information about safeguarding training is set out in our child protection and safeguarding policy.

14 Managing Information Systems

14.1 Security and Management of Information Systems

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

14.2 Password Policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and students must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access KGA Gomer systems. Staff are responsible for keeping their password private.
- From Year 3, all students are provided with their own unique username and private passwords to access KGA Gomer systems. Where appropriate, students are responsible for keeping their password private.
- We require staff and students to use strong passwords for access into our systems.

15. Monitoring arrangements

Any concerns regarding online safety should be reported through the usual safeguarding procedures and using MyConcern - the category of online safety will be applied in order to be able to monitor and review frequency and type of concerns.

This policy will be reviewed every year by the Headteacher and DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly. This review is due in September 2024.

- All members of the KGA Gomer community will be informed about the procedure for reporting online safety (e-safety) concerns (such as breaches of filtering, cyberbullying, illegal content, etc.).
- A member of the safeguarding team will be informed of any online safety (e-safety) incidents involving child protection concerns, which will then be recorded.
- A DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with Keeping Children Safe in Education 2023
- Complaints about internet misuse will be dealt with under KGA Gomer complaints procedure.
- Complaints about online bullying will be dealt with under KGA Gomer Anti-bullying Policy and procedure.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- All members of the KGA Gomer community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any members of the KGA Gomer community.
- KGA Gomer will manage online safety(e-safety) incidents in accordance with the KGA Gomer behaviour for learning policy where appropriate.
- KGA Gomer will inform parents/carers of concerns as and when required.
- After any investigations are completed KGA Gomer will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then KGA Gomer will contact gj-safeguarding@kgagomer.uk and ithelpdesk@kgahampshire.uk if there is immediate danger or risk of harm.
- The use of computer systems without permission, or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the police.

16. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour and Conduct Policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and Internet acceptable use policy

Appendix 1: KS2 acceptable use agreement (students and parents/carers) - to be shared by Google Form

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS – SIGNATURE GIVEN ONLINE ON ADMISSION.
Introduction This policy outlines an acceptable code of conduct for the use of the ICT equipment and systems within King's Academy Gomer. The school provides computers and networked resources, alongside some student-owned Chromebooks (linked to EHCPs), for student use in teaching classrooms and other resource areas. As part of this facility, Internet, e-mail and school-owned software are available for use on the proviso that these resources are used for the purpose of education. It is the school policy to respect all computer software copyrights and adhere to the terms and conditions of any licence to which KGA Gomer is a party. The downloading and/or installation of unauthorised software and applications are expressly forbidden. This includes software downloads from the Internet and from email. KGA Gomer will not condone the use of any software that does not have a licence and any student found to be using, or in possession of, unlicensed software will be the subject of disciplinary procedures. **Privacy** The purpose of the provision of ICT facilities is for use in connection with teaching, learning, research, and other approved activities by the school. The school therefore reserves the right to monitor, inspect, copy and review files and activity at any time and without prior notice. Each student is given a unique username and password that allows them access to both Google Workspace for Education onto the system and which also provides them with the ability to save their work into their own secure area. This area must be used for educational purposes only. Routine checks of network storage areas will be carried out without prior notice. **Copyright** Many of the resources you find on the Internet are copyright-protected, including music and video. You may only use all or part of a copyrighted work if you have the copyright owner's permission or if your use of the work falls under a legal exemption. Check the documents you are viewing for appropriate statements indicating copyright ownership and usage. It is your responsibility to respect these rights including all copyrights. Any copyright-protected files found during routine checks will be removed and a warning will be given, repeat offenders will receive further disciplinary action.
Name of student:
I will read and follow the rules in the acceptable use agreement policy. Network and Computer Etiquette ● Be polite. Use appropriate language. ● Be safe. In using the computer network and Internet, do not reveal personal information such as your home address and telephone number.

- Be careful. Do not jeopardise the security of student access and of the computer network or other networks on the Internet. For example, don't disclose or share your password with others or impersonate another.
- Be respectful. Do not intentionally bring viruses; copyright protected material or applications into school

Security and Accountability

- Students should not use the services of the school, Internet and/or e-mail to obtain or send such material which is against the law or published school policies (articles/files which are sexist, racist, obscene, copyright protected or promote illegal behaviour).
- Students are advised that all email sent from an email account is the responsibility of the individual account holder.
- Students are advised that the use of email to send personal data (e.g. about staff or students) to a third party is expressly forbidden under the Data Protection Act.
- Students are advised that the contents of a network account home directory (H: drive) are the responsibility of the individual account holder.
- Students are advised that in the event of a security breach, they must inform a member of staff and ensure that passwords are changed in order to be as secure as possible.
- Students are expected to use their school issued Google Account only whilst on school premises.

ICT Equipment Usage

- Students must not deliberately damage or vandalise any ICT equipment.
- Students must not intentionally waste resources, including printer ink and paper.
- Students must not unplug any cables from the back of machines.
- Students should treat ICT equipment with respect as it is provided as a tool for education.
- Students should report any computer problems to a member of staff.
- Students should only use USB drives to bring in school work, if there is any breach of this or suspicion of breach, the ICT Technicians have the right to check USB drives and remove inappropriate material.

Service Usage

- Students should always respect the privacy of other users' files.
- Students should be polite and appreciate that other people might have different views than their own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Students are advised that computer-based audio services are provided for work-related and studying purposes only.
- Students are advised that their network accounts will be deleted when they leave KGA Gomer and it is the responsibility of the student to save any files before leaving.
- Students must ensure they log-off the system correctly.
- Students must not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.
- Students should not download, use or upload any material which is copyright protected.
- Students should refrain from sending or displaying offensive messages or pictures.
- Under no circumstances should students view, upload or download any material which is likely to be unsuitable. This applies to any material of a violent, dangerous or inappropriate context.
- Students should report any breach of this policy to a member of staff, who will then inform the ICT Technicians.

Internet Usage

- Students must be aware that access is a privilege, not a right and that access requires responsibility.
- The Internet is provided for educational and research purposes.
- Students must not use chat or play online games (unless authorised by a member of staff).
- Individual users of the Internet are responsible for their behaviour and communications over the network.

- Students must not share/upload any personal information of anyone (staff or student) at the school.
- Students are responsible for good behaviour on the Internet, just as they are in a classroom or a school corridor.
- General school rules apply.

Failure to Follow Policy and Breach of Agreement

The use of the school's computer network and Internet connection is a privilege, not a right. Any student user found or believed to be using the service inappropriately, will automatically have their entitlement to use this facility suspended without notice. A student user who violates this policy and breaches his/her agreement may have his or her access to the computer network and Internet terminated indefinitely.

A student user breaches the agreement not only by affirmatively violating the ICT policy, but also by failing to report any violations by other users that come to their attention. Moreover, a student user violates this policy if they permit another student to use their account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The school may also take other disciplinary action.

Signed (student):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way that could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Take photographs of students without checking with teachers first ● Share confidential information about the school, its students or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and Head of IT know if a student informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.	
● Signed (staff member/governor/volunteer/visitor):	Date: