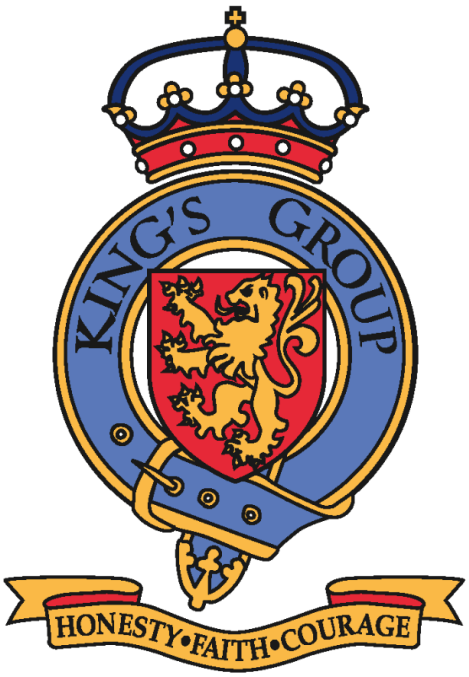

Online Safety Policy

Approved by:	Local Governing Body	Date:	June 2025
Maintained by:	Laura Phillips and Luke Mulhall	Next review due:	Sept 2026

Terminology clarification:

- **Headteacher:** Throughout this document, the term headteacher is used to refer to the most senior member of staff within an academy. Within King's Group Academies (KGA), this includes Headteachers, Executive Headteachers, Principals and Executive Principals.
- **KGA IT:** Throughout this document, KGA IT refers to the individual or service with primary responsibility for the day-to-day operation and configuration of IT systems within the Academy. This may include an IT Manager, Senior IT Technician, or a representative from a Managed Service Provider (MSP). Their role is to ensure systems are correctly configured, maintained, and functional.

1. Aims

King's Group Academies aim to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and Local Governing Body members
- 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 academy's communities in its use of technology, including mobile and smart technology (including '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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories
- **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 academies on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and academy 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 Body (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 coordinate 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 LGB should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The LGB must ensure the academy has appropriate filtering and monitoring systems in place on academy devices and academy 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 academy 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 LGB member who oversees online safety is the Safeguarding Governor.

All LGB members will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the academy's ICT systems and the Internet (see appendices)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-academy 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 academy.

3.3 The Designated Safeguarding Lead (DSL)

Details of the academy'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 the academy, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the headteacher and LGB 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 line with DfE's filtering and monitoring standards, these are in place on academy devices and academy networks
- Working with the headteacher, KGA IT staff and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the academy'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 academy's 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 the academy to the headteacher and/or LGB
- 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 KGA IT

KGA IT are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on academy devices and academy networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at the academy, including terrorist and extremist material
- Ensuring that the academy'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 academy's ICT systems every week
- 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
- Ensuring that any incidents of cyber-bullying are flagged appropriately

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the academy's ICT systems and the Internet (see appendices), and ensuring that students follow the academy's terms on acceptable use (see appendices)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes.
- Being aware of how to report any incidents of those systems, or processes failing by alerting IT and Safeguarding (contact information is available from the Academy or on their website), as well as reporting concerns directly impacting children on the safeguarding platform (My Concern/CPOMS) using the procedures detailed in the child protection and safeguarding policy.

- Following the correct procedures by alerting IT and Safeguarding (contact information is available from the academy or on their website), as well as reporting concerns directly impacting children on My Concern/CPOMS using the procedures detailed in the child protection and safeguarding policy or if they need to bypass the filtering and monitoring systems for educational purposes
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's 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' through following the processes in the academy's child protection and safeguarding policy

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 both they and their child have read, understood and agreed to the terms on acceptable use of the academy's ICT systems and Internet (appendices)

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 academy's ICT systems or the 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 of acceptable use (see appendices), which is included as part of our lettings agreement.

4 Policy Decisions

4.1 Reducing online risks

The Academy recognises that the online environment is dynamic, with new platforms, apps, tools, and risks emerging regularly. The Academy takes a proactive approach to identifying and mitigating online risks to protect its school community.

- All emerging technologies will be reviewed for educational value, and a Data Protection Impact Assessment (DPIA) will be carried out by the Data Protection Officer (DPO) before implementation.

- Appropriate filtering and monitoring systems will be in place to restrict access to harmful or inappropriate content, ensuring these systems:

    - Monitor keystrokes and user activity.
    - Capture screen content and flag concerning behaviour.
    - Detect attempts to bypass filtering controls (e.g. through proxy sites).
    - Prevent downloads of inappropriate material.
    - Identify early indicators of safeguarding concerns, including signs of grooming, self-harm, suicidal ideation, or abuse, to support early intervention and pastoral

care.

While the academy takes all reasonable precautions to ensure appropriate use, it acknowledges that due to the open nature of the internet, no system can be fully failproof.

- Any breaches of filtering or monitoring systems must be reported immediately to both the safeguarding and IT teams, as outlined in section 3.5, by contacting the Safeguarding and IT designated email addresses.

- Online safety logs and filtering decisions will be reviewed monthly by SLT, the DSL, and IT support providers to ensure that controls remain effective and relevant.

4.2 Authorising Internet access

The academy will ensure that all users are aware of and agree to the terms of acceptable internet use before being granted access.

- All staff and students must read and sign the Academy's Acceptable Use Policy (AUP) before accessing any ICT resources.
- Students are only permitted to access the internet under appropriate supervision, with content filtered according to their age and educational needs.
- Parents/carers are expected to review the student AUP with their child and provide consent.
- Guests and visitors requiring access to school systems or the internet will be provided with a tailored AUP and may be granted access to a guest wireless network only. All internet usage is monitored, and access to internal files or drives is not permitted.
- Volunteers, contractors, and governors may also access the guest network, but are subject to the same conditions outlined in the AUP.
- Special considerations will be made to ensure internet access is appropriate and inclusive for vulnerable users, including those with Special Educational Needs and Disabilities (SEND), based on individual needs.

5. Online Communication and Safer Use of Technology

5.1 Managing the academy website

The academy will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE), including:

- Accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Personal information will not be published on the academy's website without explicit permission.
- The administrator account for the academy's website will meet the KGA Password Policy requirement.
- 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

- The academy will ensure that all images are used in accordance with the KGA Photographic Image Use Policy. Students' full names will never be used alongside an image of them on social media or in online newsletters.

5.3 Managing Email

- Students may only use the academy's email accounts for educational purposes.

- All staff and LGB members are provided with a specific academy email address to use for any official communication.
- The use of personal email addresses by staff for any official academy 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.
- 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 the academy community.
- Video conferencing will take place via official and approved communication channels
- Unique logon 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

- The academy's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- Students will use age and ability-appropriate tools to search the Internet for content.
- Internet use is a key feature of educational access, and all students will receive age and ability-appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole Academy curriculum.
- The academy will ensure that the use of Internet-derived and AI-generated materials by staff and students complies with copyright law and acknowledges 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 are essential.
- Students will be appropriately supervised when using technology, according to their ability and understanding.
- All devices will be used in accordance with the academy's AUP and with appropriate safety and 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.
- The academy 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 academy 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 to ensure it meets our legal duty to protect data. Refer to the KGA 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 third-party tool in place, for example, Arbor, Provision Map, Classcharts, My Concern/CPOMS.

The Data Protection Lead 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 the academy'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 the academy's learning platforms and systems.
- Only members of the current student, parents/carers and staff community will have access to the academy's platforms and systems.
- When staff and students leave the academy, their account and/or rights to specific academy areas will be suspended.
- The Data Protection Lead, in conjunction with Judicium, will review planned IT systems, specifically where data is stored and the risks presented. This is collated in a DPIA (Data-Protection Impact Assessment).
- Only academy-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 Academies have to teach:

- Relationships, education and health education in Primary Academies
- Relationships and sex education and health education in Secondary Academies

Primary Academies:

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 (KS)** 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 th**e end of Primary**, 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 are 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 Academies:
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, 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 are 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 Academies

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 academy will raise parents/carers' awareness of Internet safety in letters or other communications home, and in information via our website learning platforms, as well as in-person information evenings. This Policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The Academy will let parents/carers know:

- What systems does the academy use 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 academy (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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Academy 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 when they are a witness rather than the victim.

The Academy 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 or class 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, LGB members 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 Academy 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 academy will follow the processes set out in the academy's behaviour and conduct policy. Where illegal, inappropriate or harmful material has been spread among students, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL/DDSL (Deputy Designated Safeguarding Lead) 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 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 academy rules as a banned item for which a search can be carried out, and/or
- Is there 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 Academy 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 guidance from the UK Council for Internet Safety and Department for Science, Innovation and Technology

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

- The DfE's latest guidance on searching, screening and confiscation
- Guidance from the UK Council for Internet Safety and Department for Science, Innovation and Technology
- 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 Academy's 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, Co-Pilot and Google Gemini. The academy recognises that AI has many uses, including enhancing teaching and learning, and helping to protect and safeguard students. However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming) and/or expose students to harmful content. 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.

The academy will treat any use of AI to access harmful content or bully students in line with this Policy and the Academy Behaviour Policy.
Staff should be aware of the risks of using AI tools while they are still being developed and should carry out risk assessments for any new AI tool being used by the academy. Our academy's requirements for filtering and monitoring also apply to the use of AI, in line with Keeping Children Safe in Education. Where indecent images have been shared that are AI-generated, this will be dealt with in line with our Safeguarding and Child Protection Policy.

9. Acceptable Use of the Internet in the Academy

All students, parents/carers, staff, volunteers and LGB members are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the Internet (appendices). Visitors will be expected to read and agree to the academy's terms of acceptable use if relevant.

Use of the academy'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, LGB members 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 the appendices.

10. Personal and Mobile Phones and Personal Devices

10.1 Rationale regarding personal devices and mobile phones

Within King's Group Academies (KGA), personal devices are defined as any digital device not owned or issued by the Academy or Trust. This includes mobile phones, personal tablets, laptops, smartwatches, and any other personally owned internet-enabled technology. These are distinct from **academy-owned devices**, which are provided, configured, and managed by the Trust for official educational and operational use, with built-in security, filtering, and monitoring tools.

Staff, volunteers, and other users who choose to use personal devices on site or for Academy-related work must do so responsibly and by the relevant Mobile Phone/Mobile Device Policy for their Academy. The owner of a personal device is fully responsible for ensuring its use does not compromise the Trust's systems, data, safeguarding standards, or reputation.

All users are reminded:

- You **must read and understand** your Academy's Mobile Phone/Mobile Device Policy.
- If you are **uncertain about the appropriateness** of using a personal device for any activity, you must consult your line manager before proceeding.
- You must **safeguard both yourself and students** by ensuring your use of personal technology remains professional, transparent, and compliant with Trust policies.

KGA makes extensive use of **cloud-based platforms**, particularly **Google Workspace for Education**, to support secure, collaborative working. Users are expected to work online wherever possible, avoiding the need to download or store data locally on personal devices. However, if there is a specific operational requirement to temporarily store data or images offline, the user:

- **Accepts full responsibility** for securing that data.

- Must ensure the device is password-protected, encrypted where possible, and **not shared** with unauthorised users.

- Should refer to and comply with the Trust's **Data Protection Policies**, available at: https://www.kingsacademies.uk/

Personal responsibility is essential when using non-Trust devices. Failure to follow this guidance may result in disciplinary action and/or safeguarding concerns being raised.

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 forbidden by any member of the academy community, and any breaches will be dealt with as part of the academy behaviour policy or staff code of conduct.

Members of staff will be issued with the academy email address where contact with students or parents/carers is required.

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

All members of the academy 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 the academy's policies.

10.3 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 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. Multi-factor authentication is an exception to this, but staff should make every effort to be logged into devices before lessons.

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

If a member of staff breaches the academy policy, then the disciplinary policy will apply.

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

Where remote learning activities are in place, staff will use the academy-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.

10.4 Visitors use of personal devices and mobile phones

Parents/carers and visitors must use mobile phones and personal devices in accordance with the academy's Acceptable Use and Mobile Phone Policy.

Staff will be expected to challenge concerns with regard to safeguarding and appropriate use, and will always inform the DSL of any concerns regarding visitors' actions.

Visitors and parents/carers must receive permission from SLT to take photos or videos and in accordance with the Academy's Acceptable Use and Mobile Phone Policy.

11. Staff using work devices outside the Academy

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, using passwords that meet the KGA Password Policy. 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
- Consider installing an anti-virus / anti-spyware / firewall to prevent unauthorised access
- 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 academy's terms of acceptable use, as set out in the appendices.

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 KGA IT.

12. How the Academy will respond to issues of misuse

Where a student misuses the academy'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 academy'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 academy 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, cyber-security 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 wellbeing issues, and 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 with 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.

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

14.2 Password Policy

- All users will be informed not to share passwords or information with others and not to log in as another user at any time.
- Staff and students must always keep their passwords private and must not share them with others or leave them where others can find it.
- All members of staff will have their own unique username and private passwords to access the academy 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 the Academy systems. Where appropriate, students are responsible for keeping their passwords private.

- We require staff and students to use strong passwords for access to our systems.

15. Monitoring arrangements

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

This Policy will be reviewed every year by the DSL and a link member of SLT.

At every review, the Policy will be shared with the LGB. The review will be supported by an annual risk assessment and audit 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 2026

- All members of the academy 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.
- Complaints about Internet misuse will be dealt with under the academy's complaints procedure.
- Complaints about online bullying will be dealt with under the academy's 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 academy 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 academy community.
- The academy will manage online safety(e-safety) incidents in accordance with the academy's behaviour policy where appropriate.
- The academy will inform parents/carers of concerns as and when required.
- After any investigations are completed, the academy 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 the Academy will contact the Police, 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
- KGA Password Policy
- Mobile Phone Policy

Appendix 1 - Staff Acceptable Use Policy

Appendix 2 - Student Acceptable Use Policy

Appendix 3 - Visitor Acceptable Use Policy