Online safety policy

Hazrat Khadijatul Kubra Girls School

Approved by:	Board of trustees	**Date:**	02.12.2024
Last reviewed on:	06.11.2024		
Next review due by:	06.11.2025		

Contents

1. Aims 2
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 6
5. Educating parents/carers about online safety 6
6. Cyber-bullying 7
7. Acceptable use of the internet in school 8
8. Pupils using mobile devices in school 9
9. Staff using work devices outside school 9
10. How the school will respond to issues of misuse 9
11. Training 9
12. Monitoring arrangements 10
13. Links with other policies 10
Appendix 2: Acceptable use agreement (pupils and parents/carers) 11
Appendix 3: Acceptable use agreement (staff, trustees, volunteers and visitors) 12
Appendix 4: online safety training needs – self-audit for staff 13
Appendix 5: online safety incident report log 14

At **HKKGS**, we recognise that technology plays a significant role in the lives of children, young people and adults. Whilst technology provides many educational and social benefits, it can also expose individuals to risks. We are committed to creating a culture of online safety that safeguards and promotes the welfare of all members of our school community.

Our school aims to:

- Identify, support and monitor pupils who may be at greater risk of harm online, including vulnerable learners and those with additional safeguarding needs.
- Protect and educate the whole school community in the safe, responsible and respectful use of technology, including mobile, smart and emerging technologies.
- Foster an environment where pupils feel confident to report online safety concerns and know that these concerns will be taken seriously.
- Work in partnership with parents, carers, staff, governors and external agencies to promote safe online behaviours.
- Ensure that all members of the school community understand their responsibilities in relation to online safety and digital conduct.
- Prevent, identify and respond effectively to online safeguarding concerns, including cyberbullying, child-on-child abuse, harmful sexual behaviour, online exploitation, radicalisation, misinformation and disinformation, and emerging online risks.
- Ensure that filtering and monitoring systems are effective, proportionate and regularly reviewed to support safeguarding responsibilities.

This Online Safety Policy outlines the commitment of HKKGS to safeguarding all members of the school community online in accordance with statutory guidance, safeguarding legislation and best practice.

This policy applies to all members of the school community, including:

- Pupils
- Staff
- Governors
- Volunteers
- Parents and carers
- Visitors
- Contractors and community users

It applies whenever digital technologies are used in connection with school activities, whether on or off the school site, and includes the use of personal devices where permitted.

The Four Key Categories of Online Risk

Our approach to online safety is based upon the four categories of risk identified within national safeguarding guidance:

Content

Exposure to illegal, inappropriate, false or harmful content, including:

- Pornographic content
- Hate-based content, including racism, misogyny, antisemitism and Islamophobia
- Extremist or radicalising material
- Self-harm and suicide-related content
- Misinformation, disinformation and fake news
- Content promoting violence or criminal activity

Contact

Harmful online interactions with other individuals, including:

- Online grooming
- Child sexual exploitation
- Criminal exploitation
- Adults posing as children
- Peer pressure and coercion
- Unwanted or inappropriate contact

- Commercial exploitation and targeted advertising

Conduct

Online behaviour that may cause harm to an individual or others, including:

- Cyberbullying
- Harassment and discriminatory behaviour
- Sharing, creating or possessing nude or semi-nude images
- Harmful sexualised behaviour online
- Online abuse and intimidation
- Oversharing of personal information
- Creating, sharing or accessing inappropriate material

Commerce

Risks associated with commercial activity online, including:

- Online gambling
- Financial scams and fraud
- Phishing attacks
- Identity theft
- Misleading advertising
- In-app purchases and financial exploitation

---

2. Legislation and Guidance

This policy has been developed with regard to the following legislation, statutory guidance and national frameworks:

- **Keeping Children Safe in Education (KCSIE) 2026**
- **Working Together to Safeguard Children**
- **Education Act 1996**
- **Education and Inspections Act 2006**
- **Education Act 2011**
- **Equality Act 2010**
- **Data Protection Act 2018 (UK GDPR)**
- **Children Act 1989**
- **Children Act 2004**
- **Counter-Terrorism and Security Act 2015 (Prevent Duty)**

The policy also reflects Department for Education guidance, including:

- **Teaching Online Safety in Schools**
- **Relationships Education, Relationships and Sex Education (RSE) and Health Education**
- **Searching, Screening and Confiscation**
- **Preventing and Tackling Bullying, including Cyberbullying**
- **Meeting Digital and Technology Standards in Schools and Colleges**
- **Filtering and Monitoring Standards for Schools and Colleges**

In accordance with the **Education Act 2011**, authorised staff may examine, search and, where appropriate, delete data or files from a pupil's electronic device where there is a lawful reason to do so and where such action is necessary to safeguard pupils or maintain good order and discipline.

The school also recognises the importance of online safety within the curriculum and ensures that pupils are taught how to stay safe online through the Computing curriculum, RSHE, safeguarding education and wider pastoral provision.

This policy should be read alongside the school's:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Acceptable Use Agreements
- Mobile Phone and Smart Device Policy
- Staff Code of Conduct
- Filtering and Monitoring Policy
- Data Protection Policy

This approach ensures that online safety is embedded throughout the school's safeguarding culture and practice.

2. Legislation and Guidance

This policy has been developed in accordance with current statutory safeguarding guidance, legislation and best practice, including **Keeping Children Safe in Education 2026 (KCSIE 2026)**, which came into force on 1 September 2026. KCSIE 2026 strengthens schools' responsibilities regarding online safety, filtering and monitoring systems, safeguarding against AI-related risks, child-on-child abuse, harmful sexual behaviour, misinformation and online exploitation.

The policy also reflects guidance from the Department for Education (DfE), including:

- **Teaching Online Safety in Schools**
- **Preventing and Tackling Bullying, including Cyberbullying**
- **Relationships, Sex and Health Education (RSHE)**
- **Searching, Screening and Confiscation**
- **Meeting Digital and Technology Standards in Schools and Colleges**
- **Filtering and Monitoring Standards for Schools and Colleges**

- **Protecting Children from Radicalisation: The Prevent Duty Guidance**
- **Generative Artificial Intelligence (AI) Product Safety Expectations and Guidance** where applicable.

This policy should also be read alongside **Working Together to Safeguard Children 2026**, which sets out the expectations for effective multi-agency safeguarding practice and reinforces the responsibility of all agencies to protect and promote the welfare of children.

The policy reflects relevant legislation, including but not limited to:

- Children Act 1989
- Children Act 2004
- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Education Act 2011
- Equality Act 2010
- Counter-Terrorism and Security Act 2015 (Prevent Duty)
- Data Protection Act 2018 and UK GDPR
- Online Safety Act 2023, which places duties on online platforms to protect children from harmful and illegal content and supports the safeguarding responsibilities of schools when educating pupils about online risks.

In accordance with the Education Act 2011, authorised school staff have the power to search, examine and, where appropriate, delete data or files from a pupil's electronic device where there is a lawful reason to do so and where such action is necessary to safeguard pupils or maintain good order and discipline.

In line with **KCSIE 2026**, the Governing Body and Senior Leadership Team will ensure that:

- Appropriate filtering and monitoring systems are in place.
- The effectiveness of filtering and monitoring systems is formally reviewed and documented at least annually.
- Filtering and monitoring arrangements consider emerging technologies, including generative AI tools and AI-generated content.
- Responsibilities for filtering and monitoring are clearly identified and understood by safeguarding and IT leads.
- Online safety is embedded within the school's whole-school safeguarding approach. The school also recognises the importance of teaching online safety through a broad and balanced curriculum, including Computing, RSHE, Citizenship and safeguarding education, enabling pupils to develop the knowledge and skills necessary to keep themselves safe online now and in the future.

New additions for 2026 that Ofsted and KCSIE would expect to see referenced:

- Online Safety Act 2023
- Working Together to Safeguard Children 2026
- DfE Filtering and Monitoring Standards (updated September 2026)
- Annual filtering and monitoring review requirement

- Risks associated with AI-generated content and generative AI
- Misinformation, disinformation and deepfake content
- Enhanced references to child-on-child abuse and harmful sexual behaviour online.

3. Roles and responsibilities

3.3 The Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety and digital safeguarding across the school.

Details of the school's DSL and Deputy DSLs are set out in the Child Protection and Safeguarding Policy.

The DSL will:

- Take the strategic lead for online safety within the school.
- Support the Headteacher in ensuring the consistent implementation of this policy.
- Review this policy annually and whenever significant legislative or safeguarding changes occur.
- Work closely with Trustees, the Headteacher and technical staff to ensure online safety arrangements remain effective.
- Understand the filtering and monitoring systems in place and contribute to regular reviews of their effectiveness.
- Maintain oversight of online safeguarding risks, including:
    - Cyberbullying
    - Child-on-child abuse
    - Harmful sexual behaviour
    - Online grooming and exploitation
    - Radicalisation and extremism
    - Misinformation and disinformation
    - AI-generated harmful content and deepfakes
    - Sharing of nude and semi-nude images
    - Online harassment and abuse.

- Ensure all online safety concerns are responded to in accordance with safeguarding procedures.
- Ensure that online safety incidents are appropriately recorded, monitored and reviewed.
- Liaise with external safeguarding agencies, the Local Authority, police and other relevant organisations where required.
- Deliver or coordinate regular training for staff, governors and volunteers.
- Provide safeguarding and online safety updates to staff at least annually and whenever significant risks emerge.
- Monitor trends and patterns in online safety incidents to identify emerging risks and required interventions.
- Undertake and contribute to annual safeguarding and online safety risk assessments.
- Advise staff on contextual safeguarding concerns linked to pupils' online activity.
- Ensure parents and carers receive appropriate information and support to enable them to safeguard their children online.
- Contribute to curriculum planning to ensure pupils receive age-appropriate online safety education.

The DSL will work alongside the school's IT support provider to ensure:

- ICT systems remain secure and protected from unauthorised access.
- Anti-virus, anti-malware and cyber security protections are regularly updated.
- Routine security audits and system checks are completed.
- Filtering and monitoring systems operate effectively and are reviewed regularly.
- Safeguarding alerts are investigated promptly.
- Access to illegal, harmful and inappropriate content is blocked where reasonably possible.
- Emerging risks associated with new technologies and AI platforms are considered within filtering and monitoring arrangements.
- This list is not intended to be exhaustive and may be adapted in response to changes in legislation, technology, safeguarding guidance and emerging online risks.

3.4 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 raise a concern on the wellbeing manager and contact the DSLs directly.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.

3.5 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure that they and their child have 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

3.6 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 3).

4. Educating Pupils About Online Safety

The school is committed to ensuring that pupils are taught how to stay safe online as part of a broad, balanced and age-appropriate curriculum. Online safety is embedded throughout the curriculum and is delivered through Computing, RSHE, Citizenship, safeguarding education, assemblies, enrichment activities and pastoral programmes, in line with Keeping Children Safe in Education 2026, Teaching Online Safety in Schools and statutory RSHE guidance.

Online safety education will be designed to empower pupils to use technology safely, responsibly, respectfully and positively, both within and beyond school.

Key Stage 3

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely.
- Protect their online identity, reputation and personal information.

- Recognise online risks relating to content, contact, conduct and commerce.
- Understand how to identify, report and seek support for online abuse, harassment, bullying and exploitation.
- Develop critical thinking skills to identify misinformation, disinformation, fake news and manipulated content.
- Understand the potential risks associated with social media, gaming platforms, livestreaming and online communities.
- Recognise the methods used by individuals who may seek to groom, exploit or manipulate young people online.
- Understand the safe and responsible use of artificial intelligence (AI) tools and emerging technologies.
- Know how to report concerns using school systems, online platforms or external reporting mechanisms where appropriate.

Key Stage 4

In Key Stage 4, pupils will be taught to:

- Understand how developments in technology affect online safety and wellbeing.
- Manage digital footprints and maintain online privacy and security.
- Critically evaluate information encountered online, including AI-generated content.
- Recognise risks associated with deepfakes, manipulated images, online scams and phishing attempts.
- Understand online behaviours that may constitute criminal offences.
- Recognise indicators of online exploitation, coercion, radicalisation and harmful influence.
- Understand the importance of digital resilience and healthy online habits.
- Access help and support services and know how to report online concerns appropriately.
- Understand their rights, responsibilities and legal obligations in online environments.

By the End of Secondary School

By the end of secondary education, pupils will know:

- Their rights, responsibilities and opportunities online, and that the same standards of behaviour expected offline also apply online.
- How to manage their online identity and protect personal information.
- That material shared online may be copied, distributed, manipulated or remain accessible indefinitely.
- Not to share content that they would not wish others to see and not to redistribute personal content shared with them.
- How and where to report online concerns and access support.
- The impact that harmful, extremist, violent or inappropriate content may have on individuals and communities.

- That sexually explicit content, including pornography, can present unrealistic and harmful portrayals of relationships and behaviour.
- That creating, possessing, sharing or requesting indecent images of children, including self-generated images, may constitute a criminal offence.
- How information, algorithms and personal data are collected, stored, shared and used online.
- How online platforms use personal information for advertising, profiling and commercial purposes.
- How to identify cyberbullying, harassment, abuse, coercive behaviour, discrimination and online exploitation, and how to seek support.
- The importance of consent, respectful communication and healthy relationships in both online and offline contexts.
- The risks associated with online gambling, financial scams, phishing, fraud and cryptocurrency-related scams.
- How emerging technologies, including artificial intelligence and generative AI, can be used safely and responsibly and how they may also be misused to create harmful or misleading content.
- How to recognise misinformation, disinformation and deepfake content and evaluate information critically before sharing it with others

Contextual and Responsive Online Safety Education

The school will ensure that online safety education reflects current safeguarding risks and emerging technologies. Teaching will be informed by local and national safeguarding trends and may include:

- Child-on-child abuse online.
- Harmful sexual behaviour.
- Online grooming and exploitation.
- Radicalisation and extremism.
- Cyberbullying and hate-based abuse.
- Misinformation and disinformation.
- Artificial intelligence (AI) and generative AI technologies.
- Deepfake and digitally manipulated images.
- Online misogyny, antisemitism, Islamophobia and other forms of discrimination.
- Online fraud, scams and financial exploitation.

The safe use of social media, online communication platforms and internet-enabled devices will also be reinforced through assemblies, tutorial programmes, enrichment activities, themed awareness events and pastoral support.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable pupils, victims of abuse and pupils with Special Educational Needs and Disabilities (SEND). The school recognises that a "one-size-fits-all" approach may not be appropriate and will provide personalised, accessible and contextualised learning opportunities to ensure all pupils can understand and apply online safety messages effectively

5. Educating Parents and Carers About Online Safety

The school recognises that parents and carers play a vital role in helping children to stay safe online. We are committed to working in partnership with families to promote a consistent approach to online safety both at school and at home.

In line with Keeping Children Safe in Education 2026, the school will provide parents and carers with regular opportunities to develop their understanding of online safety risks, emerging technologies and safeguarding concerns.

The school will raise parents' and carers' awareness of online safety through:

- Regular newsletters and safeguarding communications.
- A dedicated Online Safety/E-Safety section on the school website.
- Parent workshops, information evenings and webinars.
- Information shared through the school's communication systems and parent app.
- Parent induction materials and welcome packs.
- Awareness campaigns linked to national online safety initiatives.
- Guidance regarding emerging online risks, including the use of artificial intelligence (AI), social media platforms, gaming environments, misinformation, online exploitation and financial scams.

The school will ensure that parents and carers are informed about:

- The school's filtering and monitoring systems and safeguarding arrangements.
- The online platforms, applications and websites that their children may be asked to use for educational purposes.
- Expectations regarding acceptable use of technology.
- The reporting procedures available to pupils and families.
- Current online safety risks and trends affecting children and young people.

Where appropriate, parents and carers will be provided with guidance on:

- Managing parental controls.
- Monitoring children's online activity in an age-appropriate way.
- Supporting healthy screen use and digital wellbeing.
- Recognising indicators of online abuse, exploitation, cyberbullying and radicalisation.
- Understanding the risks and opportunities associated with artificial intelligence and generative AI technologies.

Any parent or carer with concerns regarding online safety should contact the Designated Safeguarding Lead (DSL) or Headteacher in the first instance.

Concerns relating to this policy may be raised with any member of the Senior Leadership Team or through the school's complaints procedure.

6. Cyberbullying

6.1 Definition

Cyberbullying is bullying that takes place through digital devices and online platforms, including social media, messaging applications, online gaming, email, websites and other internet-enabled technologies.

Like all forms of bullying, cyberbullying is behaviour that is:

- Intentional;
- Repeated over time (although a single incident may have significant and lasting impact through repeated sharing);
- Designed to cause harm, distress or humiliation; and
- Often characterised by an imbalance of power between those involved.

Cyberbullying may include:

- Harassing or threatening messages.
- Sharing embarrassing images or videos.
- Impersonation of another person online.
- Social exclusion through digital platforms.
- Online hate incidents.
- Sharing manipulated or AI-generated content.
- Coercion, intimidation or public humiliation through online technologies.

6.2 Preventing and Addressing Cyberbullying

The school will take a proactive approach to preventing cyberbullying through education, awareness raising and effective safeguarding procedures.

To help prevent cyberbullying, we will:

- Teach pupils about respectful and responsible online behaviour through the curriculum and wider safeguarding programme.
- Educate pupils about recognising, reporting and responding safely to cyberbullying.
- Ensure pupils understand how to report concerns relating to themselves or others.
- Promote a culture where pupils feel safe seeking support.
- Address online behaviour, digital citizenship and respectful communication through assemblies, form time, RSHE and Computing.
- Ensure all staff receive regular safeguarding and online safety training, including cyberbullying awareness and emerging online risks.
- Where a cyberbullying incident occurs, the school will follow the procedures outlined within the Behaviour Policy, Anti-Bullying Policy and Child Protection and Safeguarding Policy.

Where illegal, harmful or inappropriate content has been shared, the school will take all reasonable steps to:

- Contain the incident.
- Safeguard affected pupils.
- Preserve evidence where necessary.
- Liaise with parents, carers and external agencies.
- Involve the police where criminal offences may have been committed.

The DSL will maintain appropriate records of incidents and actions taken.

6.3 Searching, Screening and Confiscation of Electronic Devices

The school will act in accordance with the latest DfE Searching, Screening and Confiscation Guidance, Keeping Children Safe in Education 2026 and the UK Council for Internet Safety (UKCIS) Sharing Nudes and Semi-Nudes Guidance.

The Headteacher and authorised staff members, including the DSL and Deputy DSLs, may search, screen or confiscate electronic devices where they have reasonable grounds to believe that:

- A device presents a risk to pupils or staff.
- A device contains material relevant to a safeguarding concern.
- A device contains evidence of misconduct or a criminal offence.
- The use of the device breaches school rules.

Before conducting a search, authorised staff will:

- Consider the urgency, proportionality and safeguarding implications of the search.
- Explain the reason for the search where appropriate.
- Provide the pupil with an opportunity to ask questions.
- Seek cooperation from the pupil whenever possible.
- Consider whether parental involvement is appropriate.

Authorised staff may examine data or files on a confiscated device where there is a lawful and safeguarding-related reason to do so.

A "good reason" may include concerns that a device has been used to:

- Cause harm to another individual.
- Facilitate bullying, harassment or abuse.
- Access or distribute harmful content.
- Undermine the safe operation of the school.
- Commit a criminal offence.

Where evidence of a crime may exist, material will not be deleted and devices will be handed to the police as soon as reasonably practicable.

Where material is not required as evidence, authorised staff may require it to be removed or may remove it where continued access presents a safeguarding risk.

Nude and Semi-Nude Images

If a member of staff suspects that a device contains a nude or semi-nude image of a child, they will:

- Not intentionally view, copy, print or share the image.
- Secure the device immediately.
- Report the concern to the DSL without delay.
- Follow the school's safeguarding procedures and current UKCIS guidance.
- Record actions taken in accordance with safeguarding procedures.

The DSL will determine the appropriate response and whether external agencies, including children's social care or the police, need to be involved.

Complaints relating to searches or deletion of content will be managed through the school's complaints procedure.

6.4 Artificial Intelligence (AI)

The school recognises that artificial intelligence (AI) and generative AI technologies are now widely available and can offer valuable educational opportunities. However, these technologies also create new safeguarding, privacy and online safety risks which must be carefully managed.

In accordance with Keeping Children Safe in Education 2026 and the DfE Filtering and Monitoring Standards, the school will consider AI-related risks as part of its safeguarding, filtering and monitoring arrangements.

Potential AI-related risks include:

- AI-generated misinformation and disinformation.
- Deepfake images, audio and video.
- AI-generated bullying, harassment or abuse.
- Creation of manipulated or sexually explicit imagery.
- Privacy and data protection concerns.
- Over-reliance on AI-generated content for schoolwork.
- Exposure to harmful or inappropriate content through AI platforms.
- Any use of AI to harass, bully, intimidate, exploit or harm another person will be treated as a safeguarding and behaviour matter and dealt with in accordance with the Behaviour Policy and Child Protection and Safeguarding Policy.

The school will:

- Educate pupils on the safe, responsible and ethical use of AI technologies.
- Teach pupils how to critically evaluate AI-generated content.
- Raise awareness of deepfakes and manipulated media.
- Ensure staff understand AI-related safeguarding risks.
- Undertake risk assessments before introducing new AI systems or platforms.
- Consider AI services within filtering, monitoring and safeguarding reviews.
- Monitor emerging national guidance and adapt practice accordingly.
- Staff using AI tools must comply with the school's Data Protection Policy, Acceptable Use Policy, Staff Code of Conduct and any specific AI guidance issued by the school. Personal, confidential or safeguarding-sensitive information must not be entered into AI systems unless formally approved and compliant with data protection requirements.

The school reserves the right to restrict or prohibit the use of specific AI tools where safeguarding, educational or data protection concerns have been identified.

7. Acceptable Use of Technology and the Internet

The school recognises that access to technology and the internet is an essential part of teaching, learning, communication and school administration. All use of technology within the school must support the school's educational aims, safeguarding responsibilities and values.

All pupils, parents/carers, staff, volunteers, governors/trustees, contractors and visitors who use school technology systems will be required to read, understand and agree to the relevant Acceptable Use Agreement (AUA) before accessing school devices, networks or online services.

In line with Keeping Children Safe in Education 2026 and the DfE Filtering and Monitoring Standards, users are expected to use technology safely, responsibly, respectfully and lawfully. The school reserves the right to monitor, filter and review the use of its ICT systems where necessary to fulfil its safeguarding, legal and operational responsibilities.

Use of the school's internet, devices, systems and online platforms must be:

- For educational, professional or authorised school purposes only.
- Consistent with safeguarding, data protection and professional standards.
- Respectful of the rights, privacy and wellbeing of others.
- Compliant with the school's safeguarding, behaviour, staff conduct and data protection policies.

The school will maintain appropriate filtering and monitoring systems to:

- Protect users from accessing illegal, harmful, extremist or inappropriate content.
- Identify potential safeguarding concerns.
- Support the prevention of cyberbullying, online abuse and exploitation.

- Meet statutory safeguarding requirements.

Users must not:

- Access, create, store or share inappropriate, offensive, discriminatory, extremist or illegal content.
- Attempt to bypass the school's filtering or monitoring systems.
- Access another user's account without permission.
- Use school systems for personal commercial activities.
- Engage in behaviour that could bring the school into disrepute.
- Misuse artificial intelligence (AI) tools or technologies in a way that compromises safeguarding, privacy, academic integrity or professional standards.

Further details are contained within the Acceptable Use Agreements contained in the appendices.

Any misuse of school technology may result in disciplinary action, withdrawal of access privileges, safeguarding intervention and/or referral to external agencies where appropriate.

8. Pupils Using Mobile Phones and Smart Devices

HKKGS is committed to promoting a safe, focused and disruption-free learning environment.

Pupils are not permitted to use personal mobile phones, smart watches or other internet-enabled personal devices during the school day unless specifically authorised by a member of staff for educational, medical or safeguarding reasons.

All mobile phones and smart devices must be handed into the school office upon arrival and collected at the end of the school day. Devices remain the responsibility of the owner, and whilst reasonable care will be taken, the school cannot accept liability for loss, theft or damage.

The school reserves the right to confiscate any unauthorised device used in breach of this policy.

Where a device is confiscated, the school will act in accordance with:

- Keeping Children Safe in Education 2026
- Searching, Screening and Confiscation Guidance
- The school's Behaviour Policy
- The school's Safeguarding and Child Protection Policy.

Any misuse of a personal device, including:

- Cyberbullying;
- Recording or photographing individuals without consent;
- Sharing inappropriate content;
- Accessing harmful content;
- Creating or sharing AI-generated harmful material;

- Circumventing the school's safeguarding systems;

may result in behavioural sanctions, confiscation, suspension, safeguarding intervention and/or referral to external agencies where necessary.

The school recognises that technology-related safeguarding concerns may arise outside school hours. Incidents occurring off-site may still be investigated and addressed where they impact upon the welfare of pupils, school staff or the wider school community.

9. Staff Use of School Devices and Technology Outside School

Staff are expected to maintain the highest standards of professional conduct when using school devices, networks, systems and online platforms both inside and outside school.

In accordance with the Data Protection Act 2018, UK GDPR, Keeping Children Safe in Education 2026 and the school's Staff Code of Conduct, staff must take all reasonable steps to protect confidential information and maintain cyber security.

All staff will:

- Keep devices password protected using strong passwords and multi-factor authentication (MFA) where available.
- Ensure devices automatically lock when unattended.
- Use only authorised school systems for storing and sharing school information.
- Keep operating systems, software and security updates current.
- Ensure anti-virus and endpoint protection software remain active and updated.
- Report suspected cyber security incidents immediately.
- Store sensitive information securely and in accordance with data protection requirements.
- Take reasonable precautions when accessing school systems remotely.
- Protect school data when working from home or external locations.

Staff must not:

- Share school devices with family members or friends.
- Download unauthorised software or applications.
- Store confidential school information on personal devices unless authorised and securely protected.
- Use personal email accounts to transmit confidential school information.
- Access inappropriate, harmful or unlawful content using school equipment.
- Input confidential, safeguarding-sensitive or personally identifiable information into artificial intelligence platforms unless expressly authorised and compliant with school data protection procedures.

The school recognises that cyber security forms part of its safeguarding responsibilities. In accordance with the DfE Filtering and Monitoring Standards, staff play an active role in protecting school systems and reporting concerns promptly.

Any member of staff with concerns regarding the security of a device, suspected cyber incident, potential data breach or online safety concern must report the matter immediately to the designated safeguarding lead, line manager or IT support provider in accordance with the school's incident reporting procedures.

Failure to comply with this policy may result in disciplinary action and, where appropriate, referral to external agencies or professional bodies

10. How the School Will Respond to Misuse of Technology

The school takes all incidents involving the misuse of technology seriously and will respond proportionately, consistently and in accordance with safeguarding, behaviour and disciplinary procedures.

Where a pupil misuses the school's ICT systems, internet services, devices or online platforms, the school will follow the procedures outlined in the Behaviour Policy and Child Protection and Safeguarding Policy. The response will take account of:

- The age, understanding and vulnerability of the pupil.
- The nature and severity of the incident.
- Any safeguarding concerns identified.
- Whether the behaviour was deliberate, reckless or accidental.
- Any previous incidents or patterns of behaviour.
- The impact on others and the wider school community.

Responses may include:

- Educational interventions and restorative approaches.
- Temporary or permanent restriction of ICT access.
- Behaviour sanctions.
- Safeguarding support and intervention.
- Parent/carer involvement.
- Referral to external agencies where appropriate.

Where a member of staff, volunteer, governor/trustee or visitor misuses school technology systems, online platforms or personal devices in a manner that may constitute misconduct, the matter will be addressed in accordance with the Staff Code of Conduct, Disciplinary Policy and safeguarding procedures.

The school will consider referral to external agencies, including the police, children's social care, the Local Authority Designated Officer (LADO), the Information Commissioner's Office (ICO) or other appropriate bodies where incidents involve:

- Criminal activity.
- Illegal content.
- Child sexual abuse material.
- Child-on-child abuse.
- Online exploitation.
- Serious cyberbullying.
- Extremism or radicalisation concerns.
- Significant breaches of data protection legislation.
- Serious safeguarding concerns.

The school will ensure that appropriate records are maintained for all significant online safety incidents and that lessons learned inform future practice and safeguarding arrangements.

11. Training

The school recognises that effective online safety depends upon all members of the school community having appropriate knowledge, skills and confidence.

In accordance with Keeping Children Safe in Education 2026, all staff will receive safeguarding and child protection training, including online safety training, as part of their induction and at regular intervals thereafter.

Staff Training

All new staff members and volunteers will receive induction training which includes:

- Online safety responsibilities.
- Acceptable use requirements.
- Cyberbullying.
- Child-on-child abuse.
- Harmful sexual behaviour.
- Online exploitation and grooming.
- Radicalisation and extremism.
- Filtering and monitoring arrangements.
- The safe use of technology and social media.

All staff will receive safeguarding and online safety updates at least annually and more frequently where emerging risks are identified.

Training will ensure that staff understand:

- Technology is a significant feature in many safeguarding and wellbeing concerns.
- Children can experience abuse, exploitation and harm online.
- Abuse may occur both online and offline and frequently overlaps.
- Online activity can be an indicator of wider safeguarding concerns.

- Cyber security forms an important part of safeguarding responsibilities.
- Staff will be made aware that children can abuse other children online through:
- Abusive, threatening, discriminatory or misogynistic messages.
- Online harassment and coercive behaviour.
- Sharing nude and semi-nude images without consent.
- The use of social media, messaging applications and online gaming platforms to target others.
- Sharing sexualised, violent or harmful content.
- AI-generated content, manipulated images and deepfake material created to humiliate, deceive or abuse others.

Training will support staff to:

- Identify signs of online abuse and exploitation.
- Understand emerging technologies and associated risks.
- Respond appropriately to online safety concerns.
- Promote safe, responsible and respectful online behaviours.
- Help pupils develop resilience and critical thinking skills.
- Recognise misinformation, disinformation and manipulated online content.
- Understand safeguarding implications associated with artificial intelligence and generative AI technologies.

Designated Safeguarding Lead (DSL) Training

The DSL and Deputy DSLs will undertake safeguarding and child protection training, including online safety training, in accordance with statutory requirements and local safeguarding partnership expectations.

The DSL will:

- Update their safeguarding knowledge and skills regularly and at least annually.
- Maintain an up-to-date understanding of emerging online risks.
- Remain informed about developments in filtering and monitoring expectations.
- Understand risks associated with AI technologies, deepfakes and online exploitation.
- Support staff training and awareness programmes.

Trustee Training

Trustees will receive safeguarding training that enables them to:

- Understand their strategic safeguarding responsibilities.
- Understand online safety expectations within Keeping Children Safe in Education 2026.
- Understand filtering and monitoring responsibilities.
- Provide effective challenge and oversight regarding online safeguarding arrangements.
- Understand emerging risks associated with technology and artificial intelligence.

- Further information regarding safeguarding training can be found in the school's Child Protection and Safeguarding Policy.

12. Monitoring, Review and Evaluation

The school continuously monitors the effectiveness of its online safety arrangements.

The DSL will maintain records of:

- Online safety incidents.
- Cyberbullying concerns.
- Safeguarding concerns involving technology.
- Filtering and monitoring alerts.
- Emerging online risks and trends.

In accordance with Keeping Children Safe in Education 2026, the school will undertake regular reviews of filtering and monitoring arrangements, including a formally documented review at least once every academic year. This review will be led by the designated senior leader responsible for filtering and monitoring, with support from the DSL and IT support provider.

The school will also:

- Conduct annual online safety risk assessments.
- Review incident trends and safeguarding data.
- Evaluate the effectiveness of online safety education.
- Consider emerging technologies and associated risks.
- Review the effectiveness of filtering and monitoring systems.
- Seek feedback from pupils, staff, parents and trustees where appropriate.

This policy will be reviewed annually by the Headteacher and DSL, or sooner if:

- There are significant changes to legislation.
- New statutory guidance is issued.
- Serious incidents identify the need for policy revision.
- Emerging technologies create new safeguarding risks.

The Board of Trustees will receive and review the updated policy following each review cycle.

13. Links with Other Policies

This Online Safety Policy should be read alongside the following policies and procedures:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy

- Staff Code of Conduct
- Staff Disciplinary Procedures
- Data Protection Policy
- Privacy Notices
- Filtering and Monitoring Policy
- Mobile Phone and Smart Device Policy
- ICT Acceptable Use Agreements
- Searching, Screening and Confiscation Procedures
- Relationships, Sex and Health Education (RSHE) Policy
- Remote Learning Policy
- Artificial Intelligence (AI) Acceptable Use Guidance (where applicable)
- Whistleblowing Policy
- Complaints Procedure
- Cyber Security and Information Security Procedures

These documents collectively support the school's commitment to safeguarding and promoting the welfare of children in both online and offline environments.

Appendix 2: Acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it • Only use AI as directed by my teachers and only submit work that is mine and referenced, acknowledging the source. **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will hand it in to the office as soon as I arrive to school. • I will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**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 pupils 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 3: Acceptable use agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS	
Name of staff member/trustee/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 pupils without checking with teachers first • Share confidential information about the school, its pupils 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 • Share my online profiles with or accept a social media request from students • Use a mobile phone during lessons and outside break times.	
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 ICT manager know if a pupil 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 pupils in my care do so too.	
Signed (staff member/trustee/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, trustees and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**