RGS ESTD 1562
HIGH WYCOMBE
SCHOLA REGIA GRAMMATICA

E-Safety Policy

Date Agreed by the Governing Body	
Date to be reviewed	June 2027
Date of last review	June 2026
Governors Committee accountable for review	Education
Senior Leadership Team member accountable for review	ISW

RESPECT **INTEGRITY** **ASPIRATION**

1.Aims, legislation and guidance

1.1. The aim of this Policy is to safeguard members of our School community online in accordance with best practice and statutory guidance outlined in Keeping Children Safe in Education (KSCIE) and DfE publication: 'Teaching Online Safety in Schools' and guidance on filtering and monitoring. We feel that the term E-safety is more appropriate as it is all encompassing. Our approach to E-safety aims to address the following categories of risk:

1.1.1. Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

1.1.2. Contact – being subjected to harmful online interaction with other users, such as child-to- child pressure, commercial advertising and adults posing as children with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

1.1.3. Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, sharing other explicit images and online bullying.

1.1.4. Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2.Roles and Responsibilities

2.1. The Governing Body are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness. This review will be carried out annually by the Safeguarding Governor who is responsible for reporting significant online safety incidents to the Governing Body.

2.2. **The Headmaster** is responsible for ensuring the implementation and day-to-day management of the policy and procedures. The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the School community and fostering a culture of safeguarding.

2.3. **The Designated Safeguarding Lead (DSL)** holds the lead responsibility for online safety, within their safeguarding role as defined in KCSIE. The DSL will:

2.3.1. Promote an awareness of and commitment to online safety education and awareness within the School community.

2.3.2. Be responsible for receiving, handling and recording reports of online safety incidents and deciding whether to make a referral by liaising with relevant agencies, including Prevent

2.3.3. Be responsible for the filtering and monitoring systems and processes in place on School devices and School networks.

2.3.4. Liaise with the Deputy Head and Assistant Head (innovation) to create a whole school approach to online safety

2.4. **The Network Manager** is responsible for:

2.4.1. Implementing an appropriate level of security protection procedures, such as filtering and monitoring systems on School devices and networks, which are reviewed and updated annually to assess their effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online.

2.4.2. Ensuring that the School's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

2.4.3. Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

2.5. **The Deputy Head and Associate Assistant Head (Digital Learning)** will: Liaise with the DSL to create and implement a whole school approach to online safety.

3.Content

3.1. The School manages access to content across online systems for all users on all School devices using filtering software that meets the standards defined in the DfE Filtering Standards for Schools and Colleges.

3.2. Illegal content is filtered using a firewall that complies with Internet Watch Foundation URL list. Filtered content lists are regularly updated.

3.3. There are established processes for users to report inappropriate content, recognising that no system can be 100% effective. The content accessed by users is monitored by the DSL, Deputy Head and Heads of Year using monitoring software. Inappropriate use is reported to the DSL and acted upon following the procedures outlined in the Behaviour and Safeguarding policies.

3.4. If staff or students come across unsuitable online materials, the site must be reported to the Network Manager.

3.5. The School will seek to ensure that the use of online materials by staff and students complies with copyright law.

3.6. Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3.7. Artificial Intelligence (AI)

3.7.1. Artificial Intelligence (AI) tools are now integrated into the fabric of teaching and learning at RGS. While the school recognises their potential to enhance creativity, reduce workload, and strengthen inclusion, we maintain a "human-first" approach that prioritises character development and original thought.

3.7.1.1. The School operates on a "Learn Mode by Default" principle. Access to AI tools is restricted unless a teacher explicitly authorises their use for a specific task. This ensures students develop foundational skills and critical thinking before utilising algorithmic assistance.

3.7.1.2. AI use must align with our core values:

3.7.1.2.1. **Integrity:** Passing off AI-generated content as original work is classified as academic misconduct.

3.7.1.2.2. **Aspiration:** AI should be used as a collaborative "co-pilot" to explore complex concepts or optimise workflows (e.g., organising notes), not as a shortcut to bypass cognitive challenges.

3.7.1.2.3. **Respect:** Users must respect data privacy and never input personally identifiable information or sensitive school data into public AI tools.14

3.7.1.3. **Academic Standards**

3.7.1.3.1. Any permitted AI use must be fully attributed, documenting the tool, version, and the exact prompts used.

3.7.1.3.2. Students must be able to confidently explain their entire assignment without AI assistance. A failure to pass this test indicates that learning has been inappropriately outsourced.

3.7.1.3.3. AI use must only be in line with the terms of service fo the platform. **S**tudents in Year 7 and 8 are not permitted to use Generative AI (such as Google Gemini) on school accounts.

3.7.1.4. **Prohibited Technologies & Safeguarding**

3.7.1.4.1. **Wearable AI:** Wearable AI devices (e.g., AI-enabled glasses, pins, or clips) are strictly prohibited on site and in lessons unless expressly authorised for specific accessibility purposes.

3.7.1.4.2. **Risk Mitigation:** The School remains vigilant regarding AI-related risks, including deepfakes, impersonation, and "hallucinations" (factual errors). Any AI-related safeguarding concerns must be reported immediately to the Designated Safeguarding Lead (DSL).

3.7.2. Strategic oversight of these protocols is maintained by the AI Strategy Group to ensure our approach remains responsive to this rapidly evolving landscape.

4.Contact

4.1. Electronic Communication

4.1.1. Students must immediately inform a member of staff if they receive an offensive electronic communication.

4.1.2. Students must not reveal personal details of themselves or others in electronic communication or arrange to meet anyone without specific permission.

4.1.3. Student to staff electronic communication must only take place via a School email address or Google Classroom and will be monitored.

4.1.4. Incoming email must be treated as suspicious (with the following in mind: Spear Phishing, Whaling, Smishing, Vishing) and attachments not opened unless the author is known.

4.1.5. Students must seek authorisation for any email sent to external bodies when representing the School.

4.2. Published content and the School website

4.2.1. The Headmaster takes overall editorial responsibility to ensure that content is accurate and appropriate.

4.2.2. Photographs that include students will be selected carefully and checked with the consent register. The School will only use a student's first name with a digital image and will always ensure students are appropriately dressed.

4.2.3. Permission is sought on image-taking, storage and publishing.

4.2.4. Students are encouraged to tell the School if they are worried about any photographs and/or videos that are taken of them.

4.3. Social networking and learning platform

4.3.1. Students and parents will be advised that the use of social network spaces outside School brings a range of dangers for students.

4.3.2. Students will be advised never to give out personal details of any kind which may identify them or their location. They are advised to use nicknames and avatars when using social networking sites.

4.3.3. Students must not place personal photos or videos on the network without permission.

5.Mobile Phones

5.1. Mobile phones must not be used during lessons without specific permission from the teacher in charge.

5.2. The use of the camera functionality in any such device during the School day is forbidden unless with staff permission.

5.3. Appropriate and the policy surrounding inappropriate use of mobile phones can be seen in the appendix of the Behaviour Policy

6.Remote Learning

6.1. The School may use live-streaming or video-conferencing services in line with national safeguarding guidance.

6.2. Remote learning lessons must only take place via Google Meets using an @rgshw.com account.

6.3. Staff will understand and know how to set up and apply controls relating to student interactions, including microphones and cameras.

6.4. Attendance of Google Meets are automatically logged

6.5. Staff, students and parents will have a clear understanding of expectations around behaviour and participation.

7.Conduct

7.1. Acceptable use of the School network

7.1.1. Staff must read the Staff Handbook before using any School network.

7.1.2. Users of the School network must comply with the IT - Acceptable Use Policy which is signed annually by staff and students

7.1.3. RGS Student ICT Acceptable Use Agreement 2026/27

7.2. Introducing the Online Safety Policy to Students

7.2.1. A whole School approach to online safety is led by the Digital Strategy Lead.

7.2.2. Appropriate elements of the Online Safety Policy are shared with students.

7.2.3. Students will be informed that network and internet use will be monitored.

7.2.4. Opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for students as part of the School's annual Online Safety Awareness Week.

7.2.5. The whole School approach to online safety is based upon; culture, ethos, environment and partnerships with parents.

7.3. Culture

7.3.1. The risks posed by content, conduct, contact and commerce are embedded into the School Curriculum. Recommendations from the DfE Teaching Online Safety in Schools can be found in the PSHE, IT, Computer Science and Personal Development and Sixth Form Lecture Series curricula.

7.3.2. As part of these curricula, students are informed of the specific processes required to report concerns and seek support in School.

7.4. Ethos

7.4.1. The School promotes a positive online ethos through assemblies, tutor group discussions, staff training and the Student Council.

7.4.2. Students can actively contribute to the development of the School's E-Safety approach through the Student Council.

7.4.3. Staff receive regular training on E-Safety in line with the latest Keeping Children Safe in Education updates.

7.5. Environment

7.5.1. The School's online environment is closely monitored and filtered according to the principles set out in the DfE Filtering and Monitoring standards recommendations.

7.5.2. Students are informed of how their network usage is monitored during IT lessons and during the induction sessions in Sixth Form.

7.6. Partnerships with parents

7.6.1. The School seeks to proactively engage parents in School activities that promote the agreed principles of E-safety.

7.6.2. Information is shared with parents where new threats/changes have been identified.

7.6.3. Information is shared with parents whose children are moving into Sixth Form to inform them of the BYOD policy as well as at the Year 12 Parent Information at the beginning of the year.

7.7. Enlisting Parents' Support

7.7.1. Parents' attention will be signposted to this policy on the Parent Portal.

7.7.2. Parents will be provided information on online safety as part of the annual Online Safety Awareness Week. Specific elements of E-safety are covered in relevant parent information evenings.

7.7.3. Parents are required to sign the Home-School Agreement when they register their child with the School. Sixth Form students are required to sign the Sixth Form Agreement.

7.8. **Cyberbullying (Updated with Online Safety Act 2023)**

7.8.1. Cyberbullying is the use of technology to bully an individual or group. It differs from traditional bullying due to its potential for anonymity, rapid and wide-reaching nature, and the difficulty of

containing circulated content. It can occur on or off school premises, and the School is empowered by law to regulate pupil conduct in both environments.

7.8.2. It is a criminal offence to send messages that are grossly offensive, indecent, or menacing under the Malicious Communications Act 1988 and the Communications Act 2003. Furthermore, the Online Safety Act 2023 places a significant duty of care on technology companies and underscores the severity of harmful online communication.

7.8.3. Typical examples of cyberbullying include, but are not limited to:

7.8.3.1. **Threats and Intimidation:** Use of mobile devices, social media, gaming platforms, or message boards to threaten or intimidate.

7.8.3.2. **Harassment and Cyber-stalking:** Repeated, prolonged, unwanted contact or the monitoring of a person's online activity.

7.8.3.3. **Vilification and Defamation:** Posting upsetting, derogatory, or defamatory remarks, or name-calling via digital channels.

7.8.3.4. **Exclusion:** Using social media or messaging groups to deliberately ostracise or incite hatred against an individual.

7.8.3.5. **Identity Theft and Impersonation:** Unauthorised access to accounts (which is illegal under the Computer Misuse Act 1990), or creating fake profiles to impersonate others.

7.8.3.6. **Creation and Distribution of Harmful Imagery:** Sharing private, humiliating, or explicit images/videos, including manipulated content or "deepfakes." Creating, possessing, or distributing indecent images of children under 18 is illegal under the Protection of Children Act 1978.

7.8.3.7. **Manipulation:** Putting pressure on an individual to reveal personal information.

7.8.4. The School remains vigilant in addressing these evolving risks and treats all reports of cyberbullying with the utmost seriousness. Students are encouraged to report any concerns immediately through our established safeguarding channels.

8.Commerce

8.1. Risks associated with commerce and E-safety are covered throughout the RSE curriculum (details of which can be found in the curriculum map in the RSE policy). Access to services where risks exist are mitigated via the filtering and monitoring systems used by the school. Risks include but are not limited to:

8.1.1. online gambling

8.1.2. inappropriate advertising

8.1.3. phishing and/or financial scams

9.Boarding Specific

It is expected that the boarders and boarding staff at RGS follow the RGS E safety policy and the additional guidance that they are given in the following documents.;

Device Management for Boarders (updated June 2026)

FYH Additional Guidance on Mobile phones and Tablets 2025-26 (updated June 2026)