KINGSTON GRAMMAR SCHOOL

FOUNDED 1561

ONLINE SAFETY POLICY

1. Introduction

1.1. KGS ("the School") is committed to ensuring that all our students are safe, and the same principles apply to the digital world as they do in the real world. Online communications and technology can greatly enhance opportunities for learning, but they also pose risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks.

1.2. Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with these internet technologies. Current and emerging technologies used inside, and outside school include:

- Websites
- Email and instant messaging
- Blogs, forums and chat rooms
- Mobile internet devices such as smart phones and tablets
- Social networking sites
- Music/video downloads
- Gaming sites and online communities formed via games consoles
- Instant messaging technology via SMS or social media sites
- Video calls
- Podcasting and mobile applications
- Virtual and augmented reality technology
- Artificial Intelligence AI).

1.3. We understand the responsibility to educate our students on online safety issues, to teach them the appropriate behaviours and critical-thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving students in discussions about online safety.

1.4. The School:

- Regularly reviews the methods used to identify, assess and minimise online risk.
- Examines emerging technologies for educational benefit and considers potential risks and appropriate mitigations before use in school is permitted.
- Ensures that appropriate filtering and monitoring is in place and takes all reasonable precautions to ensure that the DfE non-statutory filtering and monitoring standards are met.

1.5. This policy, supported by the IT Acceptable Use Policies for staff and students and the Student Device Policy for students, is implemented in line with our safeguarding obligations and to protectthe interests and safety of the whole School community. It has regard to the DfE non-statutory filtering and monitoring standards and aims to provide clearguidance on how to minimise risks, how to deal with infringements and ensure the standards are met. It is also linked to other School policies including:

- Safeguarding & Child Protection Policy and Procedures
- Staff Code of Conduct
- Behaviour Policy
- Student Code of Conduct
- Anti-Bullying Policy
- Data Protection Policy and Privacy Notices
- Taking, Using and Storing Images of Children
- Artificial Intelligence (AI) Policy (to be issued)

2. Scope of this Policy

2.1. This policy applies to all members of the School community including staff, students, parents and visitors who have access to and are users of the School IT systems. In this policy 'staff' includes teaching and support staff, governors, and volunteers. “Parents” includes students’ carers. “Visitors” includes anyone else who comes to the School.

2.2. This policy covers both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.) as well as all devices owned by students, staff or visitors and brought onto School premises (personal laptops, tablets, smart phones and watches, etc) where connected to the internet via the school Wi-Fi.

2.3. In designing this policy, the School has considered the “4Cs” outlined in Keeping Children Safe In Education (KCSIE) – content, contact, conduct and commerce – as the key areas of risk. However, the School recognises that many students will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some students may use mobile technology to facilitate child on child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by students in or out of school, will be dealt with under the School’s Behaviour Policy, Anti-Bullying Policy and/or Safeguarding and Child Protection Policy & Procedures as is appropriate in the circumstances.

3. Roles & Responsibilities

3.1. All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make referrals. The following roles and responsibilities must be read in line with the School’s Safeguarding and Child Protection Policy & Procedures.

The Governing Body

3.2. The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy & Procedures.

3.3. The Governing Body is responsible for the approval of this policy and for periodically reviewing its effectiveness which includes ensuring that appropriate filtering and monitoring systems are in place and meet the DfE standards.

3.4. The Governors have appointed two Safeguarding Governors whose duties include oversight of the School's online safeguarding procedures and ensuring that appropriate filtering and monitoring systems and processes are in place.

3.5. The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, including in relation to online safety.

The Head and Senior Leadership

3.6. The Head is responsible for the safety of the members of the school community, and this includes responsibility for online safety.

3.7. Together with other senior leadership, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

The Designated Safeguarding Lead (DSL)

3.8. The DSL takes lead responsibility for Safeguarding and Child Protection at the School.

3.9. Supported by the Deputy Heads, this includes a responsibility for online safety including filtering and monitoring systems and processes to meet the DfE standards.

3.10. The DSL will ensure that:

- staff are adequately trained about online safety
- staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise and escalate concerns when identified
- staff are aware of the School procedures that should be followed in the event of abuse or suspected breach of online safety in connection to the School.

IT Department and others

3.11. The School's Director of IT, Head of STEAM and Head of Wellbeing all work with the DSL and Deputy Heads to ensure that this policy is understood and upheld by all members of the School communityand to help the School keep up-to-date with current online safety

issues and guidance issued by the DfE (including KCSIE) and relevant organisations, including the Independent Schools Inspectorate, Social Services, CEOP (Child Exploitation and Online Protection) and Childnet International.

3.12. The IT Department has a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with technical developments. They are responsible for the security of the School's hardware system, its data and for training the School's teaching and administrative staff in the use of IT.

Staff

3.13. All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the School's online safety procedures.

3.14. All staff are required to have read and accepted the Staff IT Acceptable Use Policy before accessing the School's systems (usually via the induction process).

3.15. Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise.

Duty to Report online safety breaches and safeguarding concerns:

3.16. Staff should promptly inform the Director of IT or Deputy Heads if they suspect or become aware of an online safety breach, except where the case involves safeguarding concerns, in which case the matter should be reported to the DSL.

3.17. Staff must promptly inform the DSL, Deputy Heads, or other member of the Safeguarding Team if they have any safeguarding concerns about a student related to online activity (including sexting, cyberbullying and inappropriate or illegal content). Where appropriate, safeguarding concerns will be reported to relevant agencies (which may include social services, the police and CEOP).

3.18. If the School believes that a child or young person is at risk as a consequence of online activity, it may seek assistance from CEOP (Child Exploitation and Online Protection).

Students

3.19. All students are responsible for using the School's digital systems in accordance with the Student IT Acceptable Use Policy, and for letting staff know if they see those systems being misused.

Parents

3.20. It is essential for parents to be fully involved in the promotion of online safety, both

in and outside of school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks relating to internet usage.

4. Filtering and Monitoring

In general

4.1. The School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are both important aspects of safeguarding students and staff from potentially harmful and inappropriate online material.

4.2. It is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

4.3. Staff, students, parents and visitors should be aware that the School's filtering and monitoring systems apply to all users, all school owned devices and any device connected via the school's Wi-Fi.

4.4. Deliberate access, or attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Student Behaviour Policy as appropriate.

Checks and reviews

4.5. Checks will be carried out once per term that the filtering and monitoring systems are operating effectively. These checks will be recorded along with any appropriate action.

4.6. The Deputy Heads, DSL and Director of IT will (with the involvement of a Safeguarding Governor as appropriate) conduct an annual review of the school's approach to online safety and filtering and monitoring provision, supported by an annual risk assessment that considers and reflects the risks its students face. The results of the review will be recorded and reported to the Governors.

4.7. Further reviews should be undertaken if there is a major safeguarding incident, a change in working practices or if new technology is introduced.

Filtering

4.8. The School's filtering system blocks internet access to harmful sites and inappropriate content.

4.9. However, this is not intended to unreasonably impact on teaching and learning or school administration or restrict students from learning how to assess and manage risks themselves. If a student wishes to access a blocked site for schoolwork / research purposes, they should contact an appropriate member of staff for assistance.

Monitoring

4.10. The School will monitor the activity of all users across all of the School's devices or any device connected to the school's internet server allowing individuals to be identified. The DSL in conjunction with other senior staff will monitor the logs daily and will act upon inappropriate usage.

4.11. Teaching staff should notify the DSL if they are teaching material which might generate unusual internet traffic activity.

Staff

4.12. If any member of staff has concerns about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content.

4.13. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

Students

4.14. Students should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

4.15. Students must report any accidental access to inappropriate materials to their Form Tutor.

4.16. Deliberate access to any inappropriate materials by a student will be dealt with under the School's Behaviour Policy.

5. Education and Training

Staff: awareness and training

5.1. New staff receive information as part of their induction on the School's approach to online safety including this Policy and an understanding of the expectations, and applicable roles and responsibilities in relation to filtering and monitoring.

5.2. All staff receive regular information and training on online safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety, including an understanding of the filtering and monitoring systems and processes in place

at the school.

Students: Online safety in the curriculum

5.3. IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to students on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our students' understanding of it.

5.4. Students throughout the School are taught about online safety matters, with particular regard paid to students with SEND or other issues that may make them more vulnerable to exploitation. Teaching is delivered through the IT and PSHE curriculums. In addition, the School provides opportunities to teach about online safety within a range of other curriculum areas. Educating students on the dangers of technologies that may be encountered outside school will also be carried out in lessons, by presentations in assemblies, as well as informally when opportunities arise.

5.5. At age-appropriate levels, students are taught about:

- How to look after their own online safety, about recognising online sexual exploitation, stalking and grooming, radicalisation and their duty to report any such instances they or their peers come across.
- The existence of online scams, particularly those that may involve blackmail or fraud.
- Relevant laws applicable to using the internet, such as data protection and intellectual property.
- Respecting other people's information and images
- Safe and appropriate use of AI.

5.6. Students are also taught about the impact of cyber-bullying and how to seek help if they are affected by it – see also the School's Anti-Bullying Policy which describes the preventative measures and procedures that will be followed in cases of bullying.

5.7. Students should approach any member of staff for advice or help if they experience problems when using the internet and related technologies.

5.8. Students are encouraged to report concerns via the online reporting system (which can be anonymous) or to any member of staff at the School in accordance with the Safeguarding Policy. Students can also contact Childline for which contact numbers are displayed prominently throughout the School.

5.9. The Director of IT and Head of STEAM monitor Government guidance in this area and update where needed. https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Guidance for Parents

5.10. The School seeks to work closely with parents in promoting a culture of online

safety. The School will contact parents if it has any concerns about students' behaviour in this area and encourages parents to share any concerns with the School.

5.11. The School will provide information and guidance on online safety by a variety of means (including on the Parent Portal, specific online safety guidance at parent forums and other events).

6. Use of school and personal devices

6.1. Further detail about the use of devices is set out:

- For students, in the Student IT Acceptable Use Policy and Student Device Policy
- For staff, in the Staff IT Acceptable Use Policy and Staff Code of Conduct.

7. Online Communications

School email accounts and Teams Messaging

7.1. All communications through the School network are monitored.

7.2. Staff and students should immediately report to the Director of IT (or in the case of students, their Form Tutor) the receipt of any communication that makes them feel uncomfortable or which is offensive, discriminatory, threatening or bullying in nature. They should not respond to any such communication.

7.3. Further detail is set out:

- For students, in the Student IT Acceptable Use Policy and Student Device Policy
- For staff, in the Staff IT Acceptable Use Policy and Staff Code of Conduct.

Use of the internet and social media

7.4. The School expects students and staff to think carefully before they post any information online or repost or endorse content created by other people.

7.5. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to others.

7.6. Staff and students should ensure their online communications do not:

- place a child or young person at risk of or cause harm
- bring the School into disrepute
- breach confidentiality
- breach copyright or data protection legislation
- do anything that could be considered discriminatory against, threaten, bully or harass any individual
- express radical views, or

- otherwise breach the Codes of Conduct for staff or students.

7.7. The School takes misuse of technology very seriously, and incidents will be dealt with appropriately under the Staff Code of Conduct or Student Behaviour Policy.

7.8. Further detail about use of the internet and social media is set out in the Student IT Acceptable Use Policy and Staff IT Acceptable Use Policy. Staff should also refer to the Staff Code of Conduct.

8. Data Protection

8.1. Please refer to the Data Protection Policy and IT Acceptable Use Policies for further details on key responsibilities and obligations that arise when personal data, particularly that of children is being processed by or on behalf of the School.

9. Safe use of digital and video images

9.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. Such images may, however, provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassmentto individuals in the short or longer term.

9.2. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, students need to recognise the risks attached to publishing their own personal images on the internet (e.g. on social networking sites).

9.3. For further detail, see the School's Policy on Taking, Using and Storing Images of Children.

10. Artificial Intelligence

10.1. Any usage by students of generative AI tools such as Copilot or ChatGPT is only permitted in the circumstances outlined in and subject to any conditions imposed by the School's Artificial Intelligence (AI) Policy – to be issued - and Academic Honesty Policy.

10.2. In particular, personal confidential information should not be entered into generative AI tools. This technology stores and learns from data inputted and students should consider that any information entered into such tools is released to the internet.

10.3. It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In

particular, students should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff.

11. Misuse

11.1. The School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the School will report illegal activity to the police and/or the local safeguarding partnerships.

11.2. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the CEOP and/or its professional advisers as appropriate.

11.3. The School may impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Anti-Bullying, Safeguarding and Child Protection and Behaviour policies.