KINGSTON GRAMMAR SCHOOL

FOUNDED 1561

ONLINE SAFETY POLICY

Introduction

IT and online communications can greatly enhance learning, but also pose risk. The increased use of and recent developments in personal devices, now pose an increased risk of threats and opportunities for misuse.

Technology is used for a wide variety of purposes inside and outside school and is constantly evolving. 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 provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

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.

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.
- Puts measures in place to ensure that users can only access appropriate material.

This policy, supported by the IT Acceptable Use Policies for staff and students and the Bring Your Own Device Policy (BYOD) for students, is implemented in line with our safeguarding obligations and to protect the interests and safety of the whole School community. It has regard to the DfE non-statutory filtering and monitoring standards and aims to provide clear guidance on how to minimise risks 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 and
- Data Protection Policy and Privacy Notices.

Scope of this Policy

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.

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.

Roles & Responsibilities

The **Governors** of the School are 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. 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.

The **Designated Safeguarding Lead (DSL)** has overall responsibility for online safety, supported by the **Deputy Heads,** including filtering and monitoring systems and processes to meet the DfE standards, and will ensure that:

- staff are adequately trained about online safety and
- staff are aware of the School procedures that should be followed in the event of breach or suspected breaches of online safety.

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 community and to help the School keep up-to-date with current online safety issues and guidance issued by the DfE and relevant organisations, including the Independent Schools Inspectorate, Social Services, CEOP (Child Exploitation and Online Protection) and Childnet International.

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.

The DSL and Deputy Heads will monitor the use of the internet and emails, maintain content filters and will act on inappropriate usage.

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.

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.

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 from the First Year upwards 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.

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.

Staff

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

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.

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

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.

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).

Online safety in the curriculum

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.

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 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.

At age-appropriate levels, and usually in lessons, students are taught about how to look after their own online safety, about recognising online sexual exploitation, stalking and grooming, radicalisation and of their duty to report any such instances they or their peers come across. 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.

At age-appropriate levels, students are also taught about the existence of online scams, particularly those that may involve blackmail or fraud.

At age-appropriate levels, students are also taught about relevant laws applicable to using the internet, such as data protection and intellectual property. All students are taught about respecting other people's information and images.

Students are taught about the impact of cyber-bullying and how to seek help if they are affected by it. Students should approach any member of staff for advice or help if they experience problems.

Staff 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 images on the internet (e.g. on social networking sites).

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

The School seeks to work closely with parents in promoting a culture of online safety. The School will always contact parents if it has any concerns about students' behaviour in this area and encourages parents to share any concerns with the School.

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

School email accounts

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.

Email communications through the School network, WiFi and staff email accounts are monitored.

Use of the internet and social media

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

Staff and students should ensure their online communications do not:

a. place a child or young person at risk of or cause harm
b. breach confidentiality
c. breach copyright or data protection legislation
d. discriminate against, threaten, bully or harass any individual or
e. express radical views.

Filtering and monitoring are both important aspects of safeguarding students and staff from potentially harmful and inappropriate online material.

Certain websites are automatically blocked by the School's filtering system. 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 school work / research purposes, they should contact their form tutor for assistance. Students should report to their Form Tutor if they accidentally access materials of a violent or sexual nature whilst using School equipment.

All internet usage via the School's systems and its WiFi network is monitored. Any deliberate attempt to access inappropriate material may lead to disciplinary action.

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.