



ONLINE SAFETY POLICY

This policy should be read in conjunction with the following linked policies:

- Electronic Information and Communications Systems
- Social Media
- Staff Acceptable Use of ICT
- Data Protection
- Use of Student Images
- Anti-bullying
- Search and Confiscation Policy
- Child Protection and Guidance for adults working with children
- Academic Honesty
- Privacy Notice
- Staff Code of Conduct
- Mobile Phone Charter
- Live Communications & remote education protocols
- Remote Learning Charter

Introduction

Online safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

We are aware that students and staff cannot be completely prevented from being exposed to risks both on and offline. Students should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns.

All members of staff need to be aware of the importance of good online safety practice in the classroom in order to educate and protect the children in their care; this includes actively protecting students from the risks of child sexual exploitation and radicalisation. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role. For further guidance see Staff Code of Conduct.

Online safety education

An online safety training programme is established across the School to raise the awareness and importance of safe and responsible use of the Internet and social media. This is delivered in discrete training sessions in assemblies (such as Safer Internet Week), as part of the HSEE programme and in subjects across the curriculum. The School provides parents with information in letters home, on our website and through information evenings. Up-to-date and

Online Safety

Approved: October 2022

Review: every two years

Review date: November 2024

Review level: Head Teacher

appropriate staff training in safe and responsible Internet use, both professionally and personally, is provided for all members of staff.

Acceptable Use Policies

To protect all members of our school community (including students, staff and visitors) the School implements Acceptable Use Policies. Staff, students and visitors are required to read and sign the relevant Acceptable Use Policy before using any school ICT resources. All users are made aware that Internet and network traffic can be monitored and traced to individuals.

Risk assessments

The School takes all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The School does not accept liability for the material accessed, or any consequences resulting from Internet use. Emerging technologies are examined for educational benefit and a risk assessment carried out before use in school is allowed.

The Internet

The Internet is an integral part of the School's administration, management and curriculum: it is a necessary tool for learning that enhances and extends education. Students are taught how to:

- use the Internet responsibly, including the importance of acknowledging information sources and respecting copyright when using material from the Internet in their own work.
- research effectively, including the skills of knowledge location, retrieval and evaluation and be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Staff should guide students to online activities that will support the learning outcomes planned for their age and ability using age-appropriate tools to research Internet content. *For further guidance see Academic Honesty Policy.*

Filtering

The School's Internet filters are provided by a specialist educational supplier and designed to suit the age and curriculum requirements of the students in school. The filtering system blocks all sites on the Internet Watch Foundation (IWF) list. Changes to the School filtering policy are risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Strategy Group.

If staff or students discover unsuitable sites, the URL should be reported to the Designated Safeguarding Lead with responsibility for online safeguarding who will then record the incident and escalate the concern as appropriate. Any material that the School believes is illegal will be reported to appropriate agencies.

Email

Students may only use approved email accounts for school purposes and must immediately tell a member of staff if they receive messages that they find alarming, distressing or harassing. Students must not reveal personal details of themselves or others in email

Online Safety

Approved: October 2022

Review: every two years

Review date: November 2024

Review level: Head Teacher

communication or arrange to meet anyone without specific permission from a parent or carer. Staff must only use official school provided email accounts to communicate with students and parents/carers. *For further guidance see Electronic Information and Communications Systems Policy and Staff Code of Conduct.*

Published content

The contact details on the website are the School's address, email and telephone number. Staff and students' personal information is not published.

The Head Teacher takes overall editorial responsibility for online content published by the School to ensure that content published is accurate and appropriate. The School's website complies with the School's guidelines for publications including respect for intellectual property rights, privacy policies and copyright. *For further guidance see Academic Honesty Policy.*

Student images / work

The School respects the permissions granted by students, parents and carers when publishing images or videos that include students. Parental or carer permission is sought when students join the School. Students' full names are not used anywhere online or in public electronic communications (such as the school email bulletin), particularly in association with photographs. The School seeks support from parents and carers at school events to refrain from taking photographs or filming where it may distract performers, infringe copyright permission or present safeguarding risks for individuals. *For further guidance see Use of Student Images Policy and Student Privacy Notice.*

Social networking, social media and personal publishing

The School controls and restricts access to social media and social networking sites on the IT network. All members of the school community are advised to communicate in a manner that is "kind, necessary and helpful".

Staff personal use, including safe and professional conduct, of social media and personal publishing sites are discussed as part of staff induction. *For further guidance see Social Media Policy and Acceptable Use Policy and Staff Code of Conduct.*

Online Learning Platforms

Online learning platforms include shared storage drives, Office 365 as well as websites that provide learning content and activities that track student progress. The School may monitor the use of communication tools and publishing facilities for safeguarding and management purposes.

Only current students and members of staff have access to the School's online learning platforms. All users are mindful of copyright issues and must only upload appropriate content onto the School's learning platforms. When staff or students leave the School their account and access to learning platforms are disabled. A visitor, for example a partner school, may be invited onto the School's learning platforms with the consent of the Deputy Head (Curriculum) where there is an agreed focus within a limited time frame and no licencing conflicts. *For further guidance see Acceptable Use Policy and Academic Honesty Policy.*

Live communications

Online Safety

Approved: October 2022

Review: every two years

Review date: November 2024

Review level: Head Teacher

The School uses Microsoft Teams for live communication. There are defined protocols for the use of video and audio in live communication within the school community. Where staff wish to use live communications with external guest users, permission should be sought from the Strategy Group Line Manager and a full risk assessment carried out. *For further information see Remote Learning Charter and live communications and remote education protocols.*

Responding to incidents of concern

All members of the School community are informed about the procedure for reporting online safety concerns (such as cyberbullying, breaches of filtering, illegal content).

The Designated Safeguarding Lead must be informed of any online safety incidents involving child protection concerns who will coordinate a response in consultation with the School's Designated Safeguarding Leads for online safeguarding, which will then be escalated appropriately.

Investigation into incidents may include the review of school IT systems and searching students' electronic devices. We seek students' and parents' support in working with the School when responding to incidents.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will contact the Kent Education Safeguarding Team and may escalate the concern to the Police. Student Managers record all reported incidents and actions taken in the School online safety incident log and other in any relevant areas.

After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes required. *For further guidance see Anti-Bullying Policy, Behaviour Policy, Search and Confiscation Policy and Child Protection Policy.*

Use of personal devices

Students are expected to follow the Mobile Phone Charter and seek their teacher's permission if they wish to use their mobile phone for learning in lessons.

Staff and visitors are not permitted to use their personal phones or devices to photograph, record or contact students, young people and their families within or outside of the School setting in a professional capacity. Staff are issued with a camera or school phone where contact with students or parents/carers is required. Staff should not allow students to use devices belonging to staff.

All staff are issued with a school laptop for their work at the School. The School does not have a BYOD (Bring Your Own Device) scheme for teaching – only school managed devices may be used for teaching be it in the classroom or for remote education. *For further guidance see Staff Acceptable Use Policy.*

Online Safety

Approved: October 2022

Review: every two years

Review date: November 2024

Review level: Head Teacher