INFORMATION ON E-SAFETY AND ACCEPTABLE USE (Students)

Maiden Erlegh Chiltern Edge recognises that IT and the internet are powerful tools for learning, teaching and communication. It can help students work independently, support personalised learning and enhance creativity. In addition, using IT interactively and to share ideas has many benefits for all members of our community.

It is important that the use of ICT and especially the internet is appropriate and responsible. E-safety is a whole-school responsibility and all users must, therefore, understand and practise good and safe e-conduct, whether on the school's network, on the internet or in private. This protocol clarifies our expectations for IT activity in school, and what is appropriate online conduct outside of school hours. It covers the use of school hardware, personal mobile phones and any other electronic communication technology.

Cyber-bullying and harassment by students will be treated as seriously as any other type of bullying and will be managed in line with our Anti-Bullying, Safeguarding and Behaviour Policies.

The school's E-Safety and Child Protection Lead Officer is Mrs N Benham, Assistant Headteacher. The designated Trustee responsible for Safeguarding is Miss Lindsey Bowden.

Education and information

This protocol and the Rules for Acceptable Use of Digital Technology and the Internet at Maiden Erlegh Chiltern Edge are available to all students and parents on the website or from the school office.

Rules relating to the Code of Conduct when online, and e-safety guidelines, are displayed around the school.

E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used and during the pastoral programme.

Learning to evaluate internet content

It is important that students learn how to evaluate internet content for accuracy and intent. This is covered as part of digital literacy in ICT lessons and across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter and monitor internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL will be reported to the school's internet provider and be blocked. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively. The school is able to monitor internet use by students.

IT Information

Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. For more information on data protection in school please refer to our Data Protection Policy available on the school's website.

Emails

The school uses email internally for staff and students, and externally for contacting parents, and is an essential part of school communication. Students' email addresses do not state their full name in order to protect their identity.

School email accounts should only be used for school-related matters and the school monitors emails and their contents.

Students are reminded not to divulge personal information over email, or to arrange to meet up with third parties. They are also told to tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

Students will be educated through the ICT curriculum to identify spam, phishing, virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Published content and the school website

The school website is a useful means of communication for the school and a valuable resource for parents, students, and staff. It is in the public domain, and can be viewed by anybody online. Any information published on the website is carefully considered by a member of the school's Senior Leadership Team in terms of safety, copyrights and privacy policies. No personal information on staff or students is published without their consent.

Policy and guidance on safe use of students' images (still or in video format) and work

Images of students and examples of their work bring our school to life and showcase our students' talents and their contribution to the community. Under the Data Protection Act 1998 images of students and staff will not be displayed in public, either in print or online, without consent.

Only images created by or for the school in line with our Acceptable Use Protocol will be used in the public domain and students may not be approached or photographed by third parties while in school or doing school activities without the school's permission.

Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable.

At present, the school blocks access to most social networking sites to students via the school network, though it cannot block access via 3G/4G enabled devices, or networks run by third parties.

Where staff require students to use a particular social networking site for a lesson, then they can request the site to be unblocked for that period. The request will be risk assessed by the school's Strategic and Classroom ICT advisor the **day before** the lesson and any requests will be logged.

Students are educated on the dangers of social networking sites and how to use them in safe and productive ways through the ICT and the pastoral programme. Key messages are that they should:

- Not give out personal details or post images of themselves or others which may enable third parties to identify them or where they are. This may put them or others in danger.
- Pay due care when uploading images of themselves or others. Once images or words are posted online, it is extremely difficult to remove them.
- Set and maintain profiles to maximum privacy and deny access to unknown individuals.
- Be aware that they can never be certain who is communicating virtually with them.
- Be wary about publishing specific and detailed private thoughts.
- Never publish any material, chat or comment which might be construed as bullying, harassment, prejudicial or criminal.
- Never publish any material of a sexual nature (image, word etc).
- Never publish material which brings the reputation of an individual or the school into disrepute.
- Report any incidents of bullying or harassment to the school and, where necessary, to the companies running the sites and/or the police.

Mobile phones, smart and other personal device

Students may bring their mobile phones to school but they must not be switched on or visible at any time during the school day or during school-organised activities unless they have the express permission from a member of staff. To do so will result in them being confiscated and potentially searched by a member of the senior leadership team if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.

Any student who brings a mobile phone or other personal device into school is automatically agreeing that they are responsible for its safety and that they will abide by the school's Acceptable Use Agreement and Code of Conduct. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.

Cyber-bullying

The school will not tolerate cyber-bullying and harassment of either students or staff (and indeed any member of our wider community). Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the Anti-bullying Policy.