Maidstone Grammar School

E-SAFETY POLICY

SEPTEMBER 2016

MAIDSTONE GRAMMAR SCHOOL
E-SAFETY POLICY

Maidstone Grammar School recognises that ICT and the Internet are great tools for learning and communication and can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

E-safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children to educate all members of the school community on the risks and responsibilities of e-safety. This falls under this duty of care. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use so that members of the school community can use this as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through the school's anti-bullying procedures which are outlined in the School's Behaviour Policy.

1. Roles and Responsibilities

The School's e-safety Coordinator is the School Bursar She is supported in this role by the E-Learning Manager and Network Manager.

The designated member of the Governing Body responsible for e-safety is Mr John Hoadly.

1.1 Governors

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of it by reviewing e-safety incidents and monitoring reports.

The role of the E-Safety Governor will include:

- Ensure an E-safety Policy is in place, reviewed every **two** years and is available to all stakeholders.
- Ensure that the E-safety Coordinators have received appropriate CEOP training.
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to.
- Ensure that the Headmaster and staff are accountable for E-safety

1.2 Headmaster and SLT

The Headmaster has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-safety Co-ordinator. Any complaint about staff misuse must be referred to the Staff E-safety Coordinator at the school or, in the case of a serious complaint, to the Headmaster. Student misuse must be referred to the Deputy Head Staff and Student Development.

The Bursar supported by the E-Learning Manager and Network Manager will ensure:

- that there is access to induction and training in E-safety practices for all users.
- that appropriate action is taken in all cases of misuse.
- that Internet filtering methods are appropriate, effective and reasonable.
- that staff or external providers who operate monitoring procedures in the school are supervised.
- that student or staff personal data as recorded within the school information management system is secure.
- that systems to protect students are reviewed and improved where necessary.
- that the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- that the Headmaster and Governors receive monitoring reports from the E-safety Co-ordinators.

E-Safety Coordinator with the support of the E Learning Manager and Network Manager:

- Have regular E-safety meetings.
- Work in partnership with the DfE, KCC and Internet Service Provider to ensure systems to protect staff and students are reviewed and improved where necessary.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of e-safety incidents involving staff and creates a log of incidents to inform future e-safety developments,
- Ensures that the Deputy Head Staff and Student Development receives reports of e-safety incidents involving students.
- Liaises with the E Safety Governor & Headmaster to provide an annual report on e-safety.

Network Manager / Technical Staff:

The ICT Manager is responsible for ensuring:

- That the schools technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements and any relevant body E-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with e-safety technical information in order to effectively carry

out their e-safety role and to inform and update others as relevant.
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported

For parents:

- **On line communications such as Insight for reports**
- **Attendance data**
- **Paying for trips and visits**

2. Learning to Evaluate Internet Content

With so much information available online it is important that students learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy in Computing and PSHE lessons. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online
- 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 Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the *school e-safety coordinator for staff related offences and the Deputy Head Staff and Student Services for pupil related offences.* 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.

3. 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. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The Network Manager supported by his technicians will review the security of the school information systems and users regularly and virus protection software will also be updated regularly.

Some safeguards that the school takes to secure our computer systems are:

- Personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced

- Portable media containing school data or programmes will not be taken off-site without specific permission from **Headmaster or a member of the SLT**.

For more information on data protection in school please refer to our **data protection policy**. More information on protecting personal data can be found in **section 11** of this policy. The Data Protection Policy can be found in S/Common/policies/approved policies or on the School's website.

4. Emails

The school uses email internally for staff and students, and externally for contacting parents. It is an essential part of school communication. It is also used to enhance the curriculum by:

- Initiating contact and projects with other schools nationally and internationally
- Providing immediate feedback on work, and requests for support where it is needed.

Staff and students should be aware that school email accounts should only be used for school-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents.

4.1 School Email Accounts and Appropriate Use

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team 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.
- The forwarding of chain messages is not permitted in school.

Students should be aware of the following when using email in school:

- In school, students should only use school-approved email accounts
- Excessive social emailing will be restricted
- Students should 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 must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

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

5. Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only.

6 Policy and Guidance of Safe Use of Children's Photographs and Work

Colour photographs and students' work bring our school to life, showcase our students' talents and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of students and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year which is time-consuming for both parents and the school.

6.1 Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children: Parental consent must be obtained. Consent will cover the use of images in:

- all school publications
- on the school website
- in newspapers as sanctioned by the school
- in videos made by the school or in class for school projects.

In addition:

- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of

activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (ie a student in a swimming pool, rather than standing by the side in a swimsuit).

- For public documents, including newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.

6.2 Complaints of Misuse of Photographs or Video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **complaints policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools **child protection and safeguarding** policy and **behaviour policy.**

6.3 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 pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Students are not allowed to access social media sites in school. There are various restrictions on the use of these sites in school that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the computing curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by the Headmaster, staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.

- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction and training.

7. Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make students and staff more vulnerable to cyberbullying
- Can be used to access inappropriate internet material
- Can be a distraction in the classroom
- Are valuable items that could be stolen, damaged, or lost
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones/personal devices are used responsibly in school. Some of these are outlined below.

- The school will not tolerate cyber bullying against either students or staff. 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 **school behaviour policy.**
- A member of staff can confiscate mobile phones, and a member of the senior leadership team, Student Services or Network Manager can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Mobile devices for years 7 – 10 must be switched off during the school day unless they are required in lessons when a teacher is following the BYOD initiative. Years 11 – 13 students can use their mobile devices discreetly outside lessons but can only use their mobile devices if a teacher agrees that it is appropriate for them to be used during their lessons.
- Any student who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Images or files should not be sent between mobile phones in school.
- If staff wish to use these own personal devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

7.1 Mobile Phone or Personal Device Misuse

Students

- Students who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.
- Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the student being prohibited from taking that exam.

Staff

- Under no circumstances should staff use their own personal accounts (including personal mobile phone for SMS, personal email and personal social media) to contact pupils or parents either in or out of school time.
- Are not permitted to take photos or videos of pupils on their own personal devices. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff.

Cyberbullying

The school, as with any other form of bullying, takes cyberbullying very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the **behaviour policy.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the perpetrator
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content

that has been published and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

Repeated bullying may result in fixed-term exclusion.

8. Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

9. Protecting Personal Data

Maidstone Grammar school believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary. The school will keep parents fully informed of how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, the local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection **read the school's data protection policy.**

Signed by

_____	**Chair of governors**	**Date: .....**
_____	**Headteacher**	**Date: .....**

This policy will be reviewed every two years.