MAIDSTONE GRAMMAR SCHOOL
FOUNDED 1549

Online Safety Policy

Designated Safeguarding Lead: Miss R Johnson, Deputy Headteacher

School Bursar (providing ICT and online support to the DSL): Mrs H Cook

ICT Network Manager: Mr S Moores

School Governor with responsibility for Online Safety: Mrs C Norey

February 2023

Maidstone Grammar School recognises that ICT and the Internet are fantastic tools for learning and communication that 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 practise good online behaviour. 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.

Online safety covers the Internet, but it also covers mobile phones and other electronic communication 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 and educating all members of the School community on the risks and responsibilities of online safety falls under this duty.

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 that members of the School community can use as a reference for their conduct online outside of School hours. Online safety is a whole-School issue and responsibility.

This policy should be read in conjunction with the following policies for further clarity:

- Safeguarding and Child Protection
- Anti-Bullying
- Behaviour
- Staff Code of Conduct and Acceptable Use Policy
- Student Code of Conduct and Acceptable Use Policy
- Bring Your Own Device (BYOD)
- ICT
- Data Protection/GDPR

1. Roles and Responsibilities

Staff

The School has appointed Miss R Johnson, Deputy Headteacher, as the Designated Safeguarding Lead. She has lead responsibility for safeguarding and child protection, including online safety. In overseeing online safety within the School the DSL is supported by the School Bursar and ICT Manager/technical staff. Other members of staff with appropriate skills and expertise regarding online safety are encouraged to help support the DSL and any deputy DSL as appropriate.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports. Online safety falls within the remit of the governor responsible for Safeguarding. The role of the online safety governor will include:

- ensure an online safety policy is in place, reviewed every year and/or in response to an incident and is available to all stakeholders
- ensure that there are key staff who have been trained to a higher level of knowledge which is relevant to the School, up to date and progressive
- ensure that procedures for the safe use of ICT and the Internet are in place and adhered to
- hold the headmaster and staff accountable for online safety.

The designated member of the governing body responsible for online safety is Mrs C Norey.

Headmaster and SLT

The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the School community. Overall responsibility for online safety is held by the DSL, supported by the School Bursar, ICT and other relevant staff. The Bursar line manages the Network Manager and day-to-day responsibility for online safety will be delegated to her. Any concern or complaint about staff misuse / misconduct must be referred to the Headmaster in the first place who may then delegate the matter to the DSL and / or Bursar and / or other member of the leadership team or refer to the LADO service if relevant.

The Headmaster and SLT will:

- Ensure access to induction and training in online safety practices for all users.
- Ensure all staff receive regular, up to date training.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures are supervised by a named member of SLT. This is the School Bursar.
- Ensure that student or staff personal data recorded within School management systems is sent over the Internet securely.
- Work in partnership with the DfE, the Internet Service Provider and School ICT Manager to ensure systems to protect students are-appropriate and managed correctly.
- Ensure the School ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.
- The Senior Leadership Team will receive monitoring reports from the Network Manager via the Bursar.

The Designated Safeguarding Lead (DSL):

- Leads online safety meetings.
- Liaises and is in close contact with the Bursar and Network Manager/ICT technicians on matters to do with on-line safety.
- Communicates with the On-Line Safety Governor and other staff with specific technical expertise as appropriate in matters to do with online safety
- Ensure referrals are made to relevant external partner agencies as appropriate
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole School approach is implemented
- Access regular and appropriate training and support to ensure DSL/DDSLs recognise the additional risks that students with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate
- Work with the E-Safety group (DSL, Bursar, E-Learning Manager, Network Manager, Assistant Head overseeing school website and social media and On-line Safety Governor) to coordinate strategy plans to include participation in national and local events to promote positive online behaviour and Safer Internet Day and promotion of online safety to parents, carers and the wider community
- Maintain records of online safety concerns, as well as actions taken, as part of the School's safeguarding recording mechanisms
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and the School's policies and procedures;
- Report online safety incidents, as appropriate, to the School leadership team and Governing Body. The

Bursar will support with this too.

- Share updates or reviews of online safety policies with the Senior Leadership Team;

The School Bursar will:

- Work in partnership with the DFE and the Internet Service Provider, School ICT Manager and E-learning Manager to ensure systems to protect students are reviewed and improved.
- Ensures the School ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly. Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate
- Report any serious abuse of the network to the Headmaster
- Ensure, with the DSL, that all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training
- Work with the E-Safety group (DSL, Bursar, E-Learning Manager, Network Manager and On-line Safety Governor) to coordinate strategy plans to include participation in national and local events to promote positive online behaviour and Safer Internet Day and promotion of online safety to parents, carers and the wider community
- Report, with the DSL, online safety incidents, as appropriate, to the School leadership team and Governing Body.
- Share updates or reviews of online safety policies with the Senior Leadership Team;
- Meet regularly with the E-safety Group including the lead governors responsible for online safety;
- Meet regularly with the Network Manager to ensure that the School's filtering and monitoring systems are working and up-to-date
- Meet regularly with the E-learning Manager and Network Manager on keeping the School's network safe and secure and devise ways in which this can be accomplished;

ICT Manager / Technical Staff:

The ICT Manager is responsible for ensuring:

- That the School's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the School meets required online safety technical requirements and any relevant body online 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 online safety technical information to effectively carry out their online 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 to Headmaster for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in School policies.

2. Communicating School Policy

This policy is available on the website for parents, staff, and students to access when and as they wish. Rules relating to the School Code of Conduct when online, and online safety messages, are displayed around the School and shared at a whole school level through assemblies and tutor time. The School Code of Conduct makes clear rules regarding use of mobile phones on the school site. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used and during PSHCE lessons which specifically address online safety issues in an age appropriate way.

3. Making use of ICT and the Internet in School

The Internet is used in School to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need to enable them to progress confidently into a professional working environment when they leave School.

Some of the benefits of using ICT and the Internet in Schools are

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

For parents:

- Parentmail for information by text or letters from the School
- Maidstone Grammar School website for key information about the school
- Talaxy for access to their child's reports, attendance information etc
- SchoolCloud for booking interview evenings
- Email staff on their work email where this has been provided or via school@mgs.kent.sch.uk

Parents / third parties are not permitted to use student Teams accounts, student email, the VLE or any other platforms etc intended for student use– these are for student use only by the designated student who has the correct password / access arrangements. School staff also have access to and use of these platforms etc.

4. 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.

Online safety is taught at various stages in a student's academic career in an age appropriate way. Online Safety is taught in discrete Computing lessons in Key Stage 3 for all students, using age related examples and activities – how to safely access information, how to keep students safe on-line, how to questions information on-line. There is also a spiral PSHCE curriculum continually reinforcing safety - in KS3 all students take the Online Safety Alliance Certificate of Online Safety in Year 7 as part of their PSHE programme. At Key Stage

4, Online Safety is included in the PSHCE programme and all students take the KS4 OSA Certificate of Online Safety in Year 11 (for 14-16 year olds). In addition, Online Safety is approached by the School as part of digital literacy across all subjects in the curriculum and online safety issues are regularly highlighted through whole school assemblies, the tutor time programme and annually for Safer Internet Day in February,

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
- Identify online risks and make informed decisions about how they act
- Understand safe ways in which to report a concern / seek support if they are concerned or upset by something they have seen 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 work in an exam or a piece of coursework, they may be prohibited from completing that exam.

The School's filtering and monitoring systems are very robust. **Filtering is provided by Kent Public Service Network using Smoothwall filtering; Monitoring is provided via SENSO.cloud.**

Monitoring alerts are sent to the Network Manager and also checked by members of the Designated Safeguarding Team in SENSO. These flag up any concerns over online safety or misuse of the internet by either a member of staff or a student when connected to the school network or externally if using school issued IT equipment. Alerts are manually checked and appropriate action taken.

The School also take steps to filter 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 Network Manager/technicians working in the ICT department. In the case of serious sites / unsuitable sites this will be reported to the Network Manager and then the School Bursar. Any material found by members of the School community that is believed to be unlawful will be reported to the appropriate agencies by the DSL and/or the School Bursar. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

5.Remote and Blended Learning

Remote and blended learning has become a daily feature of school life since the advent of the COVID pandemic. This has included all students accessing all lessons remotely during national lockdown periods and groups and individuals accessing learning remotely when they have tested positive or a required to self isolate as contacts while other students remain in school (blended learning)

In relation to online and blended learning:

- All staff will continue to look out for any signs that indicate a child may be at risk online and will report and respond to concerns in line with the Child Protection Policy addendum.
  - Where necessary, referrals will be made to LADO, children's social care and as required, the police.
- Learners are encouraged to report concerns to a member of staff or a trusted adult at home. Where this is not possible, additional support can be accessed online via:
  - Childline: www.childline.org.uk
  - UK Safer Internet Centre's 'Report Harmful Content': https://reportharmfulcontent.com
  - National Crime Agency Child Exploitation and Online Protection Command (NCA-CEOP): www.ceop.police.uk/safety-centre

- Parents/carers are encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented.
- All communication with learners and parents/carers should be for professional purposes only and will only take place using school provided or approved communication channels; for example, school provided email accounts, the School's Virtual Learning Environment (VLE) and the school's Microsoft Teams facility. Ideally, this should be on school issued/owned equipment as staff are NOT permitted to keep any personal data of students on privately owned devices (this includes lists of students). Where this is not possible, the situation must be discussed with the IT Manager & Bursar beforehand.
    - In addition, any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.

- Maidstone Grammar School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

- All the safeguarding principles and procedures underpinning practice when the school is fully operational continue to apply during the school closure / online learning period. These include that:
    - All staff have a duty of care to all students.
    - The welfare of the child / young person is always paramount.
    - "Recognise"- Staff should remain vigilant regarding any possible safeguarding concerns and always maintain an attitude of "it could happen here".
    - "Refer"- Staff must never promise confidentiality - they have a duty to share any concerns with appropriate staff and particularly the DSL/ DDSLs at the earliest opportunity.
    - Staff must also ensure compliance with data protection and GDPR procedures with regard to personal data.

- Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our Maidstone Grammar School Student Code of Conduct and Behaviour for Learning Policy, Maidstone Grammar School Staff Code of Conduct and the School's Online Safety Policy and Acceptable Use Policy.

- When delivering remote learning, staff will:
    - Only use online tools that have been evaluated and agreed by leadership.
    - Ensure remote learning activities are planned in accordance with our curriculum policies, taking learner needs and technology access into account.
    - Where possible, pre-record content.

- Where 'live' streamed webcam videos or 'live' audio conversations (rather than in recorded form) via chat facilities are deemed appropriate and beneficial to learning and lesson delivery:
    - These must always take place via the School's Microsoft Teams facility with a **minimum of three students participating at any one time.**
    - If there is any circumstance where this cannot be complied with then this will be discussed in advance with the DSL.
    - Staff and learners will ensure that a professional environment is maintained throughout.
    - Staff will agree online behaviour expectations with learners at the start of lessons. Staff will revisit our Acceptable Use Policy for staff / Acceptable Use Policy for students / Online Safety Policy with learners as necessary.
    - All participants will wear suitable dress, use professional language, and ensure backgrounds of videos (live or pre-recorded) are appropriate (e.g. a neutral, blank, blurred or pre-set background in

teams). Staff and learners should ensure personal information and/or, inappropriate or unsuitable personal items are not visible.

- Where possible, other household members should not be in the background or shot; if this is unavoidable, they should follow appropriate language, appropriate dress and appropriate behaviour expectations.
- If Live streaming, staff will mute and/or disable learners' videos and microphones, as required.

- There may be occasions where it is appropriate for staff to have a 1:1 communication with a student for a legitimate professional reason (e.g regarding an individual academic issue or pastoral reason). If this is required:
  - All 1:1 communication should take place via TEAMs Chat using the **text messaging facility** not via the live streamed video or audio facility.
  - If there is any circumstance where this cannot be complied with then this will be discussed in advance with the DSL and / or DDSLs so that appropriate arrangements are put in place.

In addition, the following arrangements must be adhered to when delivering remote lessons via blended learning (for example in circumstances where a student or a teacher is required to stay at home because they test positive for COVID:

a) When the teacher is present in the class in school and broadcasting live to students who are remote learning at home: in this case the students at home may activate their camera so that the teacher ONLY can see them on the laptop screen. The teacher MUST NOT broadcast other students in the class during the lesson to students accessing remotely from home or vice versa. This is to protect the students and the teacher from third parties who may be viewing the lesson.

b) When the teacher is delivering the lesson remotely from outside school to the class in school: In this case if all the students are present in the classroom in school the teacher may activate the camera and also audio so that they can view and interact with the class. A cover teacher or other allocated member of staff will also always be present in the classroom with students in these lessons. However, if ANY student from the class is requiring to access the lesson remotely at the same time as the teacher is delivering the lesson from outside school then the camera will need to be disabled. This is to protect the students and the teacher from third parties who may be viewing the lesson.

6. Managing Information Systems

The School is responsible for reviewing and managing the security of the computers and Internet networks 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/IT Technicians will review the security of the School information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the School takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software/apps are not downloaded to any School devices. Alerts will be set up to warn users of this.
- **Anti-Virus software monitors any file accessed in real time.**
- 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 a member of the senior leadership team once they have satisfied themselves that the data will be safe and secure.

For more information on data protection in School please refer to our **GDPR and Data Protection Policy** which can be found on the School's website.

7. Emails

The School uses email internally for staff and students, and externally for contacting parents and other individuals and organisations outside the School community, and it is an essential part of School communication. It is also used to enhance the curriculum by:

- Initiating contact with other bodies about possible or on-going projects in the School
- Being able to access trusts and funds for educational purposes
- Being able to contact outside Agencies such as the DfE, MoD, examination boards, Police and Social Services, travel agencies for educational and extra-curricular purposes
- 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 but will only do so if it feels there is reason to.

School Email Accounts and Appropriate Use

MGS only allows email accounts in School that have been managed and approved by the School.

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 always representing the School 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.
- Where possible it is advised to use BCC when sending email to multiple recipients.

Students should be aware of the following when using email in School, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- In School, students should only use School-approved email accounts
- Excessive social emailing is not considered appropriate
- 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 curriculum, PSHCE lessons, assemblies, notices and posters, including to identify spam, phishing and virus emails and attachments that could cause harm to the School network or their personal account or wellbeing.

The School uses Parentmail to contact parents, generally in the form of an email but more urgent matters will be sent by a text in addition to Parentmail.

Parents can email a member of staff on their work email address where this has been provided if there are concerns about their child's academic development or welfare. Alternatively they can email the school: school@mgs.kent.sch.uk requesting contact in relation to their child or marking the email for the Attention of the member of the relevant staff (if known).

The students can access resources through Teams or through the Virtual Learning Environment.

8. Published Content including the School Website and School Social Media sites

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 students will be published, and details for contacting the School will be for the School office and House Teams only. **For information on the School policy on children's photographs on the School website please refer to section 9 of this policy.**

Our Assistant Head KS3 is responsible for publishing and maintaining the content on the School website. He is supported by a member of the IT Network Team. They are responsible for ensuring that the content is relevant and appropriate.

Maidstone Grammar School's official social media channels are Twitter (@MGS1549), Facebook (@MGS1549), Instagram (@mgs_1549), YouTube (@MaidstoneGrammarSchool1549) and LinkedIn (https://www.linkedin.com/school/maidstone-grammar-school/).

- The official use of social media sites by Maidstone Grammar School only takes place with clear educational or community engagement objectives and with specific intended outcomes and once the use has been formally risk assessed and approved by the Headmaster and school's social media manager prior to use.
- Official social media sites are suitably protected and, where possible, run and linked to our website.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
- Staff use setting provided email addresses to register for and manage official social media channels.
- Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Parents/carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Any official social media activity involving students will be moderated if possible and written parental consent will be obtained as required.

- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.
- If members of staff are managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Read and understand our Acceptable Use Policy.
    - Where they are running official accounts, sign our social media Acceptable Use Policy.
    - Be aware they are an ambassador for the school.
    - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Follow our image use policy at all times, for example ensuring that appropriate consent has been given before sharing images.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any private or direct messaging with current or past students or their family members.
    - Inform their line manager, the DSL, the Headmaster and/or the school's social media manager of any concerns, such as criticism, inappropriate content or contact from students.

9. Policy and Guidance on Safe Use of Children's Photographs and Work

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 General Data Protection Regulation 2018 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 to prevent repeatedly asking parents for consent over the School years, which is time-consuming for both parents and the School. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period rather than a one-off incident does not affect what you are consenting to. A copy of the consent form can be found at the end of the policy.

Parents will be required to give consent upon admission of their child into the School. This will be in place for the duration of their time at MGS unless it is removed by the parent/carer or a child, if over the age of 13. Anyone wishing to make changes to consent should do so in writing to the School.

Using photographs of individual children

It is important that published images do not identify students or put them at risk of being identified (unless parental consent has been given). 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.

- ***Parents and others at School events can take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a School performance involving their child. The School does not prohibit this as a matter of policy.***

- ***The School does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the School to prevent.***

- ***The School asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.***

- ***As a School we want to celebrate the achievements of our students and therefore may want to use images and videos of our students within promotional materials, or for publication in the media such as local, or even national, newspapers covering School events or achievements. Whenever a student begins their attendance at the School they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that student. We will not use images or videos of students for any purpose where we do not have consent.***

For more information on please refer to our **GDPR and Data Protection Policy on the School's website.**

10. Concerns and 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 by the school. Please refer to our C**omplaints Policy** on the School website for more information on the steps to take when making a complaint.

It is also the case that photographs and videos may be misused by young people or adults. Many young people and adults use electronic equipment to access the internet and share content and images via social networking sites such as Facebook, Twitter, Tumblr, Snapchat, Discord, LinkedIn, TikTok and Instagram. Unfortunately, some adults and young people will use these technologies to harm children, including through Child on Child abuse by children and young people. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings. Students may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity.

Any concerns regarding the misuse of photographs or videos by students of the school should be reported immediately to the school for the attention of the Designated Safeguarding Team
Misuse of photographs or videos in any form by students will be dealt with in accordance with the School Behaviour Policy according to the incident type and may involve external agencies such as the Police and Social Services.

Any concern regarding the misuse of photographs or videos by adults, including staff or other adults outside the school should be reported immediately to the Headmaster.

11. Social Networking, Social Media and Personal Publishing
Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are potentially more vulnerable to content, contact and conduct behavioural issues. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. Students are not permitted to access social media sites in School.

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 PSHCE, Assemblies, tutor time, notices and posters 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 will:

- Ensure that students are educated on the dangers of social networking sites and how to use them in safe and productive ways (out of school only). Students are regularly reminded of the School's Code of Conduct in relation to use of mobile phones and IT (including via the student Acceptable Use Policy)
- That any sites that are to be used in class should be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Ensure that any official School blogs created by 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. This member of staff is Mr J Hanratty.
- 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 students to remember that they are always representing the School and must act appropriately.
- Include safe and professional behaviour of staff online at staff induction.

12. Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace today, 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 are used responsibly in School. Some of these are outlined below as stated in the MGS Student Code of Conduct and Behaviour Policy:

- *Years 7-11: Ensure all mobile devices / ear phones of any type are turned off and out of sight during the school day except when a member of staff has specifically permitted use in a lesson for an educational purpose.*
- *Sixth Form: discreet use of phones only; No phones /ear phones in tutor time unless specifically related to the activity and permitted by staff. No phones / ear phones visible in corridors or when moving around the school site.*
- The use of mobile phones is not permitted in tutor time unless expressly required by the teacher.
- 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 subject to the School behaviour policy. **School Behaviour Policy available on the school website.**
- A member of staff can confiscate mobile phones, and a member of the senior leadership team and/or the Designated Safeguarding Lead and Deputies can search the device 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 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.

- Staff may wish students to use their mobile phones in class as part of a learning project but they must not allow students to use their phones without permission.

13. Mobile Phone or Personal Device Misuse

Students

- Where a student misuses their phone/device/earphones in a lesson / tutor time by using it in any way that the teacher has not specifically permitted or uses it (Years 7-11) at any time in unstructured time, then it will be usual practice for the staff member to confiscate the phone/device. The same principles will apply to earphones / ear pods etc. On the first confiscation the student receives a verbal warning and the phone/device will remain at Reception until 3.20pm when the student may collect it. On the second confiscation the student receives a verbal warning, parents are notified and the phone/device will remain at Reception until 3.20 when the student may collect it. On the third confiscation, the phone will be retained by the School until the parent/carer can collect it in person from Reception. Where students persistently misuse phones the school may ban the student from having the phone in school. In addition, where the School considers that a student has misused a device the School may make use of the school's sanction system.
- In addition, where the School considers that a student has misused a device the School may make use of the school's sanction system. Sanctions (which include Lunchtime Detentions, After School Detentions, Extended Detentions and in more serious cases, Suspensions) are applied depending on the seriousness and/or frequency of the behaviour concern(s). Sanctions may be applied using a staged approach OR applied at any level, depending on the nature of the concern.
- Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. Watches are also not permitted as many are now internet enabled. If a student is found with a mobile phone or other personal device / watch 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 devices to contact students or parents either in or out of School time.
- Staff are not permitted to take photos or videos of students on 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. More information on this can be found in the **Child protection and Safeguarding Policy**, or in the staff Code of Conduct and contract of employment.

14. Responding to Online Safety Incidents

- All members of the community are made aware of the reporting procedure for any safeguarding concerns in the start of year safeguarding training and assemblies for staff and students. This includes reporting online safety concerns, including breaches of filtering, child on child abuse, cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content. Awareness is raised through regular staff training, updates and briefings for students, parents and governors.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns. The complaints procedure and whistleblowing policy are available on the school website.
- We require staff, parents, carers and students to work in partnership with us to resolve online safety issues.

- After any investigations into serious concerns are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- If we are unsure how to proceed with an incident or concern, the DSL or Deputy DSL will seek advice from the Education Safeguarding Service or LADO.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101 or 999 if there is immediate danger or risk of harm as appropriate.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL or Deputies may judge it appropriate to speak with the police and/or the Education Safeguarding Service first, to seek advice and ensure that potential criminal or child protection investigations are not compromised.

Concerns about student online behaviour and/or welfare

- The DSL or deputy will be informed of all online safety concerns involving safeguarding or child protection risks in line with our Safeguarding and Child Protection Policy.
- All concerns about students will be recorded in line with our Safeguarding and Child Protection Policy, including on CURA- our school safeguarding software.
- Maidstone Grammar School recognises that whilst risks can be posed by unknown individuals or adults online, students can also abuse their peers; all online child on child abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL or deputy will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to students as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Concerns about staff online behaviour and/or welfare

- Any concern or complaint about staff misuse will be referred to the Headmaster.
- Matters to do with Child Protection/safeguarding will be referred to the Headmaster and DSL
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff Code of Conduct Policy.
- Welfare support will be offered to staff as appropriate.

Concerns about parent/carer online behaviour and/or welfare

- Concerns or complaints regarding parents/carers behaviour and/or welfare online will be reported to the Headmaster. The Headmaster will respond to concerns in line with existing policies, including but not limited to safeguarding and child protection, anti-bullying, complaints, allegations and low level concerns against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.

15 Procedures for Responding to Specific Online Concerns

Online sexual violence and sexual harassment between children

- The DSL and other appropriate members of staff have accessed and understood the DfE 'Keeping Children Safe in Education 2022" which includes Part 5 Child on Child Sexual Violence and Harassment. Details of the School's response to child on child abuse, including sexual violence and harassment can be found in our safeguarding and child protection policy.
- Maidstone Grammar School recognises that sexual violence and sexual harassment between children can take place online. Examples may include:

  Non-consensual sharing of sexual images and videos

  Sexualised online bullying

Online coercion and threats
'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence.
Unwanted sexual comments and messages on social media
Online sexual exploitation

- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL or deputy and act in accordance with out child protection and anti-bullying policies.
    - If content is contained on students' personal devices, they will be managed in accordance with the DfE 'searching, screening and confiscation' advice.
    - Provide the necessary safeguards and support for all students involved, such as implementing a risk assessment/safety plans, offering advice on blocking/reporting/removing online content, and providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make referrals to partner agencies, such as Children's Social Work service and/or the police.
    - If the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community. If a criminal offence has been committed, the DSL or deputy will discuss this with the police first to ensure that investigations are not compromises.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- Maidstone Grammar School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Maidstone Grammar School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of inappropriate online behaviours including sexual violence and sexual harassment including through regular staff training, assembly information briefings for students and parents, PSHCE lessons.

Youth produced sexual imagery ("sexting")

- Maidstone Grammar School recognises youth produced sexual imagery (also known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and the local KSCMP guidance: "Responding to youth produced sexual imagery".
    - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- Maidstone Grammar School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.

- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
        - If it is deemed necessary, the imagery will only be viewed where possible by the DSL (or DDSL), and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - act in accordance with our child protection policies and the relevant local procedures.
    - ensure the DSL (or deputy) responds in line with the UKCIS and KSCMP guidance.
    - Store any devices containing potential youth produced sexual imagery securely
        - If content is contained on students personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - carry out a risk assessment in line with the UKCIS and KSCMP guidance which considers the age and vulnerability of students involved, including the possibility of carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - make a referral to Children's Social Work Service and/or the police, as deemed appropriate in line with the UKCIS and KSCMP guidance.
    - provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
    - implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
    - consider the deletion of images in accordance with the UKCIS guidance.
        - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
    - review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- Maidstone Grammar School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.
- Maidstone Grammar School will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target students, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for students, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.

- We will regularly remind students of the 'Report Abuse' CEOPS button in the online safety section of the school website which can be used to report online child sexual abuse – this is highlighted to all students in the start of term safeguarding assemblies and at other times throughout the year.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant KSCMP procedures.
    - store any devices containing evidence securely.
        - If content is contained on students personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk.
    - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - provide the necessary safeguards and support for students, such as, offering counselling or pastoral support.
    - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible and appropriate, students will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).
- If members of the public or students at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- Maidstone Grammar School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant KSCMP procedures.
    - store any devices involved securely.

    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
    - ensure that any copies that exist of the image, for example in emails, are deleted, as long as this does not compromise an investigation.
    - report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on school or any other devices, we will:
    - ensure that the Headmaster is informed in line with our managing allegations against staff policy.
    - inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
    - quarantine any devices until police advice has been sought.

16.Cyberbullying

The School, as with any other form of bullying, takes Cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the **behaviour policy and the anti-bullying 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 to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim.
- Educate and make it clear to the 'bully' that this behaviour will not be tolerated while also providing appropriate support to them.

Sanctions will be issued in line with the School's behaviour policy and anti-bullying policy. 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.

Bullying may result in suspension.

17.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.

18.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 students, parents, and staff and processes it to support teaching and learning, monitor and report on student 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, and the School will keep parents fully informed of the 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 General Data Protection Regulation 2018 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, our 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 GDPR and Data Protection Policy.**

The School's GDPR and Data Protection Policy can be found on the School's website.

MAIDSTONE GRAMMAR SCHOOL
FOUNDED 1549

Mr M Tomkins BSc NPQH
Headmaster

CONSENT FORM

MGS from time to time like to take photographs and make video/audio recordings of pupils for promotional purposes and to celebrate successes and achievements. These images may appear in our printed publications, on video or on our website and MGS Facebook, Twitter and Instagram feeds. Occasionally, we may take photographs and videos of the pupils in our school.

Also, from time to time, the School may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event. Pupils will often appear in these images, which may be printed in local or national newspapers, or be on televised news programmes.

To comply with the Data Protection Legislation, we need your permission before we can photograph or make any recordings of your child. Please provide your explicit consent below then sign and date the form where shown.

May we use your child's image in still or video format in conjunction with any of the following:

(Please tick to confirm consent)

In printed publications produced by MGS, on our Website, MGS Facebook, Twitter and Instagram feeds and Promotional videos. ☐

*We will not include details of full names (which means first name **and** surname) of any person in an image on our website, on video, or in printed publications without specific parental permission. We may include the full name of a competition winner or when sharing pupil successes e.g. in our termly newsletter.*

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Parent/Guardian signature	Date
Name (in block capitals)	
Pupil's Name (in block capitals)	