# MAIDSTONE GRAMMAR SCHOOL

# ONLINE SAFETY POLICY
# January 2020

**Designated Safeguarding Lead: Miss R Johnson, Deputy Head**

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

**ICT Network Manager: Mr S Moores**

**School Governor with responsibility for Online Safety: Mrs C Norey**

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 practice good online behaviour and conduct. 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 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 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. In line with the principles laid out in the DfE '*Teaching Online Safety in School*' guidance 2019, the school also recognises that the online world develops and changes at speed. New opportunities, challenges and risks are appearing all the time. It is therefore important to focus on the underpinning knowledge and behaviours that can help students to navigate the online world safely and confidently regardless of device, platform or app.

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. The school will undertake its best endeavours to provide a safe online environment for all users while also recognising that the nature of the online world this cannot always be fully guaranteed. Online safety is a whole-school issue and responsibility.

This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2019, 'Working Together to Safeguard Children' 2018 and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.

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

- Maidstone Grammar School Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour for Learning Policy
- Staff Code of Conduct
- Staff Acceptable Use Policy
- Student Acceptable Use Policy
- Sex and Relationships Policy
- Data Protection/GDPR Policy

## 1. Roles and Responsibilities

The School has appointed Miss R Johnson, Deputy Headmaster, as the Designated Safeguarding Lead. The Designated Safeguarding Lead has lead responsibility for safeguarding and child protection, including online safety. In overseeing online safety within the school the Designated Safeguarding Lead is supported by the School Bursar and the 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.

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

### Governors

Governors are responsible for the approval of the online safety policy. 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 the Designated Safeguarding Lead, Bursar and ICT Network Manager 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.

### 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 Designated Safeguarding Lead, supported by the School Bursar, ICT Manager and other relevant staff. Any complaint about staff misuse must be referred to the DSL and the Bursar, at the school or, in the case of a serious complaint, to the Headmaster.

The Headmaster must:

- 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 be supervised by a named member of SLT. This is the School Bursar.
- Ensure that student or staff personal data as recorded within the school management system which is sent over the Internet is secure.
- 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 / DSL / Deputy Designated Safeguarding Leads will receive monitoring reports from ICT Manager / Technicians, as appropriate.

**The Designated Safeguarding Lead (DSL) will:**

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with and be closely supported by other members of staff, in particular the Bursar, ICT Network Manager, ICT Technicians, Online Safety Governor and other staff with specific technical expertise as appropriate on matters of online safety.
- Ensure appropriate 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 understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep students safe online.
- 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 staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the setting'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 concerns, as appropriate, to the school management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually).
- Meet regularly with the E Safety Steering Groups and the governor with a lead responsibility for online safety.

**The School Bursar:**

- Works in partnership with the DFE and the Internet Service Provider, the DSL and school ICT 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.
- Receives reports of online safety incidents and uses these to inform future online safety developments.
- Reports to Senior Leadership Team.
- Provide an annual report to the Governors on ICT, including online safety.
- Leads E Safety steering group meetings

**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 the Headmaster, DSL and Bursar for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.

**All Staff Must:**

- Complete appropriate safeguarding training to carry out their roles.
- Have read, understood and signed for the latest version of Keeping Children Safe in Education (KCSIE) together with the Staff Acceptable Use Policy and Staff Code of Conduct.
- Follow and uphold the School's Online Safety Policy (this document) and Child Protection and Safeguarding Policy.

## 2. Communicating School Policy

This policy is available on the School website for parents, staff, and students to access when and as they wish. Information about conduct when online, and online safety guidelines, are displayed around the school. Staff and Students must sign an Acceptable Use Policy. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, during PSHE lessons where personal safety, responsibility and/or development are being discussed. Assemblies also focus on safeguarding and online safety including during e-safety week.

## 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, to communicate with parents 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 and safely 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.
- Contact with schools in other countries resulting in cultural exchanges between students all over the world.
- 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, training 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, reporting to parents and assignment tracking.

**For parents:**

- Parentmail for information by text or letters from the school
- Website including online safety information and links.
- Insight for access to their child's reports, booking interview evenings
- Email staff on their work email

## 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. This is approached by the school as part of digital literacy across subjects in the curriculum, through the ICT curriculum, PSHCE lessons, assemblies, notices and posters. Students will be taught to:

- Evaluate what they see online and be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Recognise techniques used for persuasion including techniques that are often used to persuade or manipulate others.
- Understand what acceptable and unacceptable online behaviour look like, including the importance of respect for others.
- Identify online risks and make informed decisions about how to act.
- Understand safe ways in which to seek support if they are concerned or upset by something they have seen online.
- 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 students. If staff or students discover unsuitable sites, then the URL will be reported to the Network Manager or technician working in the ICT department.

The discovery of serious unsuitable sites must 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. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

## 5. 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 internal and external security threats. The Network Manager, along with his 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.
- 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
- Staff must ensure that data removed from school must be encrypted prior to leaving the site, including student exam submissions.
-

For more information on data protection in school please refer to our **data protection policy which can be found on the School's website**. More information on protecting personal data can be found in **section 11** of this policy.

## 6. 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 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
- 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 for educational and extra-curricular purposes

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.

### 6.1 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.

**Students should be aware of the following when using email in school**, and will be taught to follow these guidelines through the curriculum, PSHCE lessons, assemblies, notices and posters and in any instance where email is being used:

- 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 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 text also through Parentmail.

Parents can email a member of staff on their work email address if there are concerns about their child's academic development or welfare. Students must not email staff but speak to them in person, unless agreed by the member of staff. Parents can also access information about their child's report or book appointments for interviews through the Parents' Portal known as Insight.

The students can access learning resources through the Virtual Learning Environment.

## 7. 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.

**For information on the school policy on children's photographs on the school website please refer to section 7.1 of this policy.**

The Media/ICT technician, overseen by the Network Manager, is responsible for updating the website and liaising with the necessary staff to ensure the content on the website is relevant and appropriate.

**7.1 Policy and Guidance of Safe Use of Children's Photographs and Work**
Colour photographs and students work bring our school to life, showcase our student's 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 year, 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. This consent form will outline the school's policy on the use of photographs of children, including:

- How and when the photographs will be used
- How long parents are consenting the use of the images for
- School policy on the storage and deletion of photographs.

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 any 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 (unless parental consent has been given) or put them at risk of being identified. 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 attending school events can take photographs and videos of those events for personal and private use. 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.
  Whenever a student begins their attendance at the School the parent, or student where appropriate and aged 13 or over, will be asked to complete a consent form in relation to the use of images and videos of that student. 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

For more information on please refer to our **data protection policy on the School's website.**

### 7.2 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 school's **child protection and safeguarding** policy and **behaviour policy.**

Our students increasingly use electronic equipment daily to access the internet and share content and images via social networking sites such as Facebook, twitter, MSN, Tumblr, snapchat and Instagram.

Unfortunately, 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 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.

Misuse of photographs or videos in any form will be dealt with in accordance with the school Behaviour Policy according to the incident type.

### 7.3 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 allowed 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 PSHE, Assemblies, 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). They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Ensure that official school online content created by staff and students/year
- groups/school clubs or as part of the school curriculum will be password-protected 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 students to remember that they are always representing the school and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

## 8. Mobile Phones and Personal Device

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 use of personal devices, including mobile phones, is not permitted on the school site for years 7 – 11. Sixth formers can use their devices discreetly. There are sanctions imposed on students who disobey the rules about mobile phone use. 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 and / or 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.
- For students in Years 7-11 mobile phones must be switched off and out of sight from 8.30 until 3.30. In addition, they must not be used in any other formal school activity. Year 12 and 13 students may use their phones during the school day with the exception of tutor times. Year 12 and 13 students must use their phones discreetly. Staff will exercise their professional judgement when determining whether use of phones is appropriate and discreet and may confiscate or apply sanctions where this is not the case.
- Whilst the use of personal devises, including mobile phones, is not permitted on the school site for Years 7-11, the School recognises that a student may bring their mobile device to school. However, the school is not responsible for the safety of these devices which are brought in at the owner's own risk. 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 must not allow a student to use their mobile devices as part of a learning project. This rule will be periodically reviewed.

### 8.1 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, including smart watches, into examination rooms with them. If a student is found with a mobile phone or any device 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 or their result being voided.

**Staff**

- Staff should not use their own personal email to contact students or parents either in or out of school time. Use of personal mobile phones is not allowed except in exceptional circumstances and with approval from SLT.
- Staff are not permitted to take photos or videos of students using 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 and must be used at any time during lessons.
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the Staff Code of Conduct.

## 9. Responding to Online Safety Incidents

- All members of the community are made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer abuse, including 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, regular 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 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.
- 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.

**9.1 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.
- Maidstone Grammar School recognises that whilst risks can be posed by unknown individuals or adults online, students can also abuse their peers; all online peer on peer 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.

**9.2 Concerns about staff online behaviour and/or welfare**

- Any complaint about staff misuse will be referred to the Headmaster, in accordance with our allegations against staff policy.
- 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.

**9.3 Concerns about parent/carer online behaviour and/or welfare**

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

**10. Procedures for Responding to Specific Online Concerns**

**10.1 Online sexual violence and sexual harassment between children**

- The DSL and other appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2019.
    - Full details of our response to peer on peer 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 our 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 compromised.
    - review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- Maidstone Grammar school recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- 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, information briefings for students and parents, PSHE lessons, assemblies, notices and posters.

**10.2 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.

**10.3 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 ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to students and other members of our community.
- 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.

**10.4 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 (ISP) 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 and / or DSL 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.

**10.5 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 for Learning Policy and 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
- 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 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 provide may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

Sanctions will be imposed in line with the school behaviour policy.

**10.6 Online hate**

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Maidstone Grammar School and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

**10.7 Online radicalisation and extremism**

As listed in this policy, we will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site.

- If we are concerned that student may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection and safeguarding policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Headmaster will be informed immediately, and action will be taken in line with the child protection and complaints policies.

**11. Vulnerable Students**

- Maidstone Grammar School recognises that anyone can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some students, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.

- Maidstone Grammar School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable students as appropriate to their individual need.
- Members of staff are made aware through regular staff training that children with SEN and disabilities and looked after children can be disproportionately vulnerable to and impacted by online safeguarding concerns.

**12. Managing Emerging Technologies**

Technology is progressing rapidly, and new technologies are emerging all the time. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments where required.

**13. Protecting Personal Data**

MGS follows statutory General Data Protection Regulations in 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 Regulations 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 data protection policy which can be found on the School's website.**

This policy will be reviewed annually.