

Online Safety Policy

Designated Safeguarding Lead: Miss R Johnson, Deputy Headteacher
School Business Manager (providing ICT and online support to the DSL): Mrs J Rees
ICT Network Manager: Mr Steel
Head of Digital Teaching and Learning: Mr Martin

School Governor with responsibility for Online Safety/ Safeguarding: Mrs C Norey
Ratified by Governors July 2026 (subject to ratification by Full Governors)
For Review by Governors July 2027

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Ensure that everyone knows that Online Safety is a whole school issue and everyone is responsible.

2. The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Legislation, Guidance and School Policies

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards <https://www.gov.uk/government/publications/preventing-and-tackling-bullying>
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

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

- MGS Safeguarding and Child Protection Policy
- MGS Behaviour and Anti-bullying Policy
- MGS Staff Code of Conduct
- MGS Staff Acceptable Use Policy
- MGS Student Acceptable Use Policy
 - MGS Data Protection/GDPR Policy

The policy meets the requirements of Keeping Children Safe in Education.

4. Roles and Responsibilities

The Governor

The Governors have overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governors will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Governors will also make sure all staff receive regular online safety updates (via email, staff meetings. Relevant training etc), as required to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Governors will meet with appropriate staff to discuss online safety and requirements for training, and monitor online safety practices in the school.

The Governors will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The Governors will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.

They will review the DfE's filtering and monitoring standards, and discuss / review what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

Mrs Ceri Norey is the Governor overseeing online safety.

The Headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

Mr Tomkins is the Headteacher

The Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher and Governors to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Ensuring that there are appropriate and robust filtering and monitoring systems and processes in place on school devices and school networks and that these are annually reviewed
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the Business Manager, ICT Manager and other key colleagues to make sure the appropriate systems and processes are in place
- Working with the Headteacher, Business Manager, ICT manager and other key staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring, supported by other relevant staff / DDSLs
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy. Online Safety Incidents are recorded in the Student Services restricted access and confidential Incident log and identified as "Online Safety" to enable identification, tracking and monitoring of incidents. Incident reports are linked by reference number to the log entries and contain detailed reports of incidents investigated.

- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Ensuring that there is regular and appropriate staff training in relation to online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

Miss Johnson is the Designated Safeguarding Lead

The School Business Manager

The School Business Manager:

- Ensures the School ICT systems and all devices are reviewed regularly with regard to security and safety so that they are in line with DfE expectations.
- Report any serious abuse of the network or online safety issues to the Headteacher / DSL
- Work with the DSL, ICT Network Manager and other relevant colleagues to ensure that all filtering and monitoring systems are in place and reviewed at least annually; Ensure that virus protection is installed and updated regularly.
- Meet regularly with the E-safety Group to ensure that the school is meeting all DfE requirements in relation to the school network and online safety.

•

Mrs Rees is the School Business Manager

The ICT Network Manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- With the DSL, making sure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are referred to the DSL so they can be dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Mr Steel is the ICT Manager

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms of the Staff Acceptable Use Policy on acceptable use of the school's ICT systems and the internet and making sure, as far as reasonably possible, that pupils follow the Student Acceptable Use Policy. Ensuring that staff online conduct outside the school is in line with the Staff Code of Conduct and does not bring the school into disrepute or create a safeguarding concern.

- Knowing that the DSL has overall responsibility for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by alerting the Designated Safeguarding Team / DSL
 - Following the correct procedures by communicating with the IT Network Manager and / or DSL if they need to bypass the filtering and monitoring systems for justified educational purposes
 - Referring any online safety concerns immediately to the DSL to make sure that any online safety incidents are reported and logged and dealt with appropriately in line with this policy.
 - Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy by reporting to the Designated Safeguarding Team/DSL if a concern is identified.
 - Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'. All concerns should be immediately referred to the Designated Safeguarding Team / DSL
- This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff, DSL or the Headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms of the Student Acceptable Use Policy for the school's ICT systems and internet and also the MGS issued 1:1 device Acceptable Use Policy, if relevant

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum

All secondary schools have to educate pupils about the following areas:

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images

- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
 - What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
 - About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
 - That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
 - That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
 - How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
 - That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
 - How information and data is generated, collected, shared and used online
 - That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
 - That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
 - That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk
- The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6. Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

7. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website.

This policy will also be shared with parents/carers annually and is available on the school website. If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff, the DSL or the Headteacher.

8. Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

Bullying can be defined as “behaviour by an individual or a group, repeated over time that intentionally hurts another individual either physically or emotionally”. (DfE “Preventing and Tackling Bullying”, July 2017)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. For example, this may take place through PSHCE, assemblies or discussions with individual students.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

Where considered appropriate by the school, the DSL/DDSLs will report the incident and provide the relevant material to the police as soon as is reasonably practicable, including if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

9. Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher / DSL
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the authorized staff member / DSL / Headteacher / Senior Leader to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behaviour and Antibullying Policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

10. Filtering and Monitoring

In addition, as required in KCSIE, the school proactively works to take all reasonable steps to ensure that there is appropriate filtering and monitoring across the school network and all school issued devices including MGS 1:1 laptops issued to students, in relation to AI and in line with guidance from the DfE.

Internet connectivity is provided through resilient dual-fibre connections protected by Sophos next-generation firewalls. Web filtering is enforced through the Sophos firewall platform and applies to all internet traffic routed through the school's network.

In addition, all staff and student devices are equipped with Senso.cloud, which provides device-level filtering and monitoring capabilities both on-site and when devices are used off-site.

FastVue reporting is used to provide enhanced visibility, analysis and reporting of internet usage and filtering activity, supporting safeguarding, monitoring and investigative processes.

Monitoring alerts are sent to the Safeguarding Team and Network Manager in SENSO. These alerts flag up any concerns over online safety or misuse of the internet, school devices (in and out of school) and Teams 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. Safeguarding assemblies and staff training ensures that staff and students are aware of these monitoring practices and expectations for appropriate use.

The school also takes 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 ICT department. In the case of serious sites / unsuitable sites this will be reported to the Network Manager and then the School Business Manager and / or DSL. 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 Business Manager. Regular software and broadband

checks will take place to ensure that filtering services are working effectively. This information has been shared with staff, including through staff safeguarding training.

11. Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Maidstone Grammar School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Maidstone Grammar School will treat any use of AI to bully pupils seriously, in line with our Behaviour and Anti bullying Policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of AI should be carried out in accordance with the school's 'Use of Artificial Intelligence (AI) Policy'.

12. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role, if a member of staff or a student.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements.

13. Pupils using mobile devices in school

Information on the use of mobile / personal devices is found in the MGS Behaviour and Anti-Bullying Policy available on the website at: [Our Policies & Documents - Maidstone Grammar School](#)

Information on the use of MGS issued 1:1 laptop devices is found in the 1:1 Device Acceptable Use Policy.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Not sharing the device among family or friends
- Keeping operating systems, protection software up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of the Staff Acceptable Use Policy or the Staff Code of Conduct.

MGS issued devices should be used solely for MGS work related activities.

If staff have any concerns over the security of their device, they must seek advice immediately from the IT Network Manager.

14. Remote and Blended Learning

Remote and blended learning became a daily feature of school life after the advent of the COVID pandemic. There may also be other times when remote learning is required such as Snow Days or unexpected and unavoidable closure of the school.

In relation to online and blended learning if required in the future:

- **This should only take place if specifically authorised in advance by the senior leadership team**
- All staff will 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 MGS Safeguarding and Child Protection Policy.
 - 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. 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 & Business Manager 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 and its staff 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, 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 school 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 unless this has been agreed in advance with the DSL.
 - 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:

- 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 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.

15. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour and Antibullying Policy and other relevant policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the MGS Allegations and Low Level Concerns Policy and / or other relevant school policies and procedures as applicable. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

16. Training for staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

17. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the DSL, School Business Manager, IT

Network Manager and head of Digital teaching and Learning. At every review, the policy will be shared with the Governors.

18. Links with Other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour and Antibullying Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable Use Policies
- AI Policy