Manchester Grammar School
E-Safety Policy

Introduction

It is the duty of The Manchester Grammar School (MGS) to ensure that every pupil in its care is safe, and this applies equally as regards the digital world and the real world. IT and online communications can provide valuable opportunities for learning, but can also pose significant risks to young people. Our pupils are therefore taught about the risks they face online and how to limit them; these risks include, but are not limited to, fraud, malicious software, the risk of identity theft, bullying, grooming, stalking, abusive behaviours (e.g. trolling) and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include websites, email and instant messaging, blogs, social networking sites, chat rooms, music/video downloads, gaming sites, text messaging and picture messaging, video calls and conferencing, podcasting, online communities via games consoles, IoT devices (e.g. Amazon Echo) and personal devices (e.g. smart phones and tablets).

This policy, supported by the Acceptable Use Policy, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies: Safeguarding and Child Protection, Code of Conduct for Staff, Health and Safety, Behaviour, Rewards and Sanctions, Anti-Bullying, Acceptable Use, Data Protection, Use of Personal Devices by Pupils, Use of Personal Devices by Staff and Visitors and PSHE scheme of work.

Whilst recognising the potential benefits of the above innovations, it is important to remember that these internet technologies are not consistently policed. All users therefore need to be aware of the range of risks associated with them.

At MGS, we understand our responsibility to educate our pupils on E-Safety issues. We aim to equip pupils with the strategies and critical thinking skills needed to enable them to remain safe and within the law when using the internet and related technologies. We also understand the importance of involving pupils in discussions about E-Safety and listening to their fears and anxieties, as well as their thoughts and ideas.

Scope of this Policy

This policy applies to all members of the School community who have access to the School’s IT systems, including staff, pupils, volunteers, parents and visitors. In this policy ‘staff’ includes teaching and non-teaching staff, governors, and regular volunteers. ‘Parents’ includes pupils’ carers. ‘Visitors’ includes anyone else who comes to the School, including occasional volunteers.

Both this policy and the Acceptable Use Policy cover both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment etc.), as well as any personal devices brought onto school premises.
Roles and responsibilities

1. The Governing Body

The governing body of the School is responsible for the approval of this policy and for reviewing its effectiveness. It will review this policy at least every three years.

The nominated governor for safeguarding takes responsibility for ensuring that the E-Safety Policy is implemented.

2. The High Master and the Senior Leadership Team

The High Master is responsible for the safety of the members of the School community, and this includes responsibility for E-Safety. The High Master has delegated day-to-day responsibility to the Assistant Head (Safeguarding) who acts as the School’s E-Safety Coordinator.

In particular, the role of the High Master and the Senior Leadership team is to ensure that:

- staff, in particular the E-Safety Coordinator, are adequately trained about E-Safety; and
- staff are aware of the School procedures and policies that should be followed in the event of the abuse or suspected breach of E-Safety in connection to the School.

3. E-Safety Coordinator

The School’s E-Safety Coordinator is responsible to the High Master for the day-to-day issues relating to E-Safety. The E-Safety Coordinator has responsibility for ensuring this policy is upheld by all members of the School community, and works with IT staff to achieve this. The post-holder will keep up to date on current E-Safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

4. Computer Services staff

The School’s technical staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School’s hardware system and its data. They provide appropriate access to, and monitor the use of, the internet and emails; they maintain content filters and report inappropriate usage to the E-Safety Coordinator.

5. Staff and volunteers

Anyone accessing the School's IT infrastructure is required to abide by the Acceptable Use Policy.

All staff working with pupils are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any E-Safety issues which may arise on a daily basis.

Staff have a responsibility to record and report any incidents or concerns relating to E-Safety using a Safeguarding Note of Concern, which they should pass on as soon as possible to the School's Designated Safeguarding Lead (DSL).
6. Pupils

Pupils are required to abide by the Acceptable Use Policy when accessing the School’s IT infrastructure, and must let staff know if they see IT systems being misused.

7. Parents and carers

Parents and carers are responsible for endorsing the School’s Acceptable Use Policy, and for promoting E-Safety, both in and outside of school.

Education and training

1. Staff: awareness and training

New staff receive information on MGS’s E-Safety and Acceptable Use Policies as part of their induction.

Staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety. They also receive, as and when appropriate, additional guidance and training on E-Safety issues in briefings and CPD sessions.

2. Pupils: E-Safety in the curriculum

IT and online resources are used across the curriculum. New pupil induction includes guidance in Computing lessons regarding the Acceptable Use Policy and E-Safety. Aspects of E-Safety are also covered in PSHE lessons and assemblies, and also informally, when opportunities arise. We review and modify our provision in the light of changing needs.

At age-appropriate levels, pupils are taught about their E-Safety responsibilities, and to look after their own online safety. From Year 7, pupils are formally/informally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL or any other member of staff at the School.

From Year 7, pupils are also taught about relevant laws applicable to using the internet, such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc) through discussion and classroom activities.

Pupils are made aware of the impact of cyber-bullying and how to seek help if they are affected by these issues. (The School's Anti-bullying Policy describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying). Pupils should approach any member of staff, as well as parents and their peers, for advice or help if they experience problems when using the internet and related technologies.

3. Parents/carers

The School seeks to work closely with parents and carers in promoting a culture of E-Safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area, and likewise it hopes that parents will feel able to share any concerns with the School.

The School recognises that not all parents and carers may feel equipped to protect their son(s) when they use electronic equipment at home. The School therefore from time to time arranges discussion evenings.
for parents to provide advice on E-Safety and the practical steps parents can take to minimise the potential dangers to their son(s).

For further guidance and access to E-Safety resources, visit www.childnet.com.

Policy Statements

1. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. (For further details of password security, see below.) When the device is not being used it should be locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are permitted to use their own personal devices. Usage must be in accordance with the Code of Conduct for Staff and policy on Use of Personal Devices by Staff and Visitors.

Pupils

The School permits pupils to bring into school personal devices as a teaching and learning tool, but these remain their responsibility, and they are brought to school entirely at their own risk. The School does not accept any responsibility for loss or damage.

Pupils must abide by the School’s Acceptable Use Policy and policy on Use of Personal Devices by Pupils when using personal devices for school work. Pupils are prohibited from using personal devices for non-school related activities during lessons.

The School recognises that personal devices are sometimes used by pupils as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a personal device for such purposes, this will be discussed by the SEND department with the pupil’s parents or carers. Once agreement is reached, the SEND Department will then inform the pupil’s teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must at all times act in accordance with guidance provided in the Code of Conduct for Staff.

All digital communication between staff and pupils must take place using school accounts. Staff are expressly forbidden from having contact with pupils via private email or social media accounts.

The School has taken all reasonable steps to ensure that the School network is safe and secure. Staff should be aware that all activity on the School’s network, including email communication via staff email addresses, is monitored.

Communication between staff and pupils or parents/carers must be professional in tone and content.
When using school systems, staff should immediately report to the E-Safety Coordinator or DSL the any online material or email communication which makes them feel uncomfortable, or is offensive, discriminatory, threatening or bullying in nature. They must not respond to any such communication.

Staff must remain alert to the risk of fraudulent emails. They should report emails they suspect to be fraudulent to the E-Safety Coordinator, DSL or the Head of the Computer Services Department.

**Pupils**

All pupils are issued with their own personal school email addresses and usernames for use on our network and by remote access (including Home Access Plus and MGScentral). Access is via a personal login, which is password protected. This official service may be regarded as safe and secure, and must be used when submitting schoolwork electronically. Pupils should be aware that email communications through the School network and school email addresses are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork/research purposes, pupils should contact their Form Tutor, who will log a request for assistance via FreshService.

Pupils must only use their school accounts to email staff; they must not seek to contact staff via private email or social media accounts.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, and should immediately report such a communication to a member of staff.

The School expects pupils to think carefully before they post any information online, or re-post or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to their Form Tutor or Head of Year/Head of College. The deliberate accessing of inappropriate material by a pupil will lead to the incident being recorded on their file and will be dealt with under the School's Behaviour, Rewards and Sanctions Policy. Pupils should be aware that all internet usage via the School's systems, including its Wi-Fi network, is monitored.

Certain websites are automatically blocked by the School's filtering system. If this causes problems for school work/research purposes, pupils should contact the Head of Computing for assistance.

4. **Password security**

Pupils and staff have individual school network logins, email addresses and personal storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All staff and pupils should:
- use a strong, unique password consisting of at least 12 characters. This should include a mixture of capital and lower case letters, numerals and special characters. It must not include a group of three characters from the username. As a matter of good practice it should be changed every 6 months.
- **never share their passwords.**
Security (password protection or finger scan, but not a finger swipe, facial recognition or voice trust system) should be enabled on any personal device which is used to access school data.

5. **Safe use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with their creation, use, sharing, publication and distribution. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents/carers are permitted to take videos and digital images of their own children at school events for their own personal use, provided that they have the permission of the member of staff responsible for the event. To respect everyone's privacy and, in some cases, protection, these images must not be published (e.g. on blogs or social networking sites) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow the School's policy on Taking Photographs in School and on School Trips concerning the sharing, distribution and publication of those images.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

Pupils must not take, use, share, publish or distribute images of others, except when in connection with a clear educational purpose and/or authorised to do so by staff.

Photographs published on the School website, or displayed elsewhere, which include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. When photographs are to be published accompanied by the full names of pupils, permission from parents/carers will be obtained. (See the Parent Contract and Acceptable Use Policy for more information.)

6. **Misuse**

MGS will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the Manchester Safeguarding Children Board. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Centre.

Incidents of misuse or suspected misuse will be dealt with by staff in accordance with the School’s policies and procedures (in particular the Safeguarding and Child Protection Policy and the Behaviour, Rewards and Sanctions Policy).
In accordance with its Anti-Bullying Policy, the School will impose one of a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil.

**Complaints**

As with all issues of safety at MGS, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to E-Safety, prompt action will be taken to deal with it. Complaints should be addressed to the Pastoral Deputy Head (who is also the School’s DSL). Please see the Complaints Policy for further information.

**Monitoring and evaluation**

The monitoring and evaluation of the effectiveness of this policy and its implementation will be carried out by the Pastoral Deputy Head and Assistant Head (Safeguarding), taking account of information provided by the Heads of Section and Proctors. The Senior Management Team will meet annually to review the effectiveness of the policy.

SMT lead: Pastoral Deputy Head

Governing Body lead: Joy Kingsley

Date last reviewed by the Governing Body: 22 June 2017

Next Governing Body review: when there is a significant change in the policy.