ICT & E-Safety Policy
Senior School

Contents

Introduction
The School recognises the importance and relevance of new technologies in the lives of our pupils. The internet and other digital and information technologies are powerful tools, which can open up new and exciting opportunities for learning. However, the use of these new technologies can put young people at risk within and outside the School. Some of the online dangers pupils may face include:

(i) Threatening behaviour
(ii) Trolling – seeking to provoke outrage by posting insults, defamatory or negative comments and abuse online
(iii) Blackmail – including 'revenge porn'
(iv) Cyberbullying – writing messages with the intent to cause distress or anxiety in a public place (e.g. Twitter, Instagram)
(v) Grooming online – causing or encouraging a child under the age of 18 to engage in sexual activity online or meeting them in person after online contact. This also relates to contact with extremists.
(vi) Fake profiles
(vii) Hacked accounts / compromised security
(viii) Exposure to extremist materials – including terrorist propaganda
(ix) Youth produced sexual imagery (often referred to as sexting)

Aims of the ICT & E-Safety Policy
The School aims to provide a supportive, friendly and safe environment for all pupils and staff, where bullying is not tolerated, so that staff can teach and pupils can learn in a secure and relaxed atmosphere and achieve their full academic potential. This policy outlines how this is achieved within

Reviewed and updated by the Deputy Head (Teaching and Learning) June 2021
Appendix D reviewed and updated by the Head Mistress with advice from Ellis Whittam September 2021
Substantive changes from KCSIE23 added by the DSL September 2023. Minor update October 2023.

the context of ICT and E-Safety and outlines the roles and responsibilities of all members of the School community.

Legislation and Guidance

This policy is based on information from the following:

- Independent Schools Standards Regulations 2014
- ISI Commentary on the Regulatory Requirements September 2017
- 'Keeping Children Safe in Education 2023
- The use of social media for online radicalisation (www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation)
- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- Meeting digital and technology standards in schools and colleges (March 2023)

The policy should be read in conjunction with the following MHSG policies and documents:

1. The Child Protection and Safeguarding Policy
2. The Behaviour and Discipline Policy
3. The Anti-Bullying Policy
4. The Staff Code of Conduct
5. The Equality Policy
6. The Data Protection Policy
7. Policy for ICT Use by Pupils (Appendix A)
8. MHSG E-Safety Charter (Appendix B)
9. The Use of Mobile phones at MHSG (Appendix C)
10. ICT Code of Conduct and Acceptable Use Guidance for Staff (Appendix D)
11. Guidance for Staff on the Use of Photographs (Appendix E)

Definitions

The term 'E-Safety' relates to the safe use of all information and electronic systems and the means by which pupils are protected from associated dangers. The term 'ICT' refers to the Information Communications Technology used in school.

Filtering – Effective filtering systems block students from harmful content, denying access to any harmful content. Smoothwall provides Schools with industry-leading filtering systems and restricting access to certain websites, applications, and other sources that could pose a threat to student safety and/or privacy.

Monitoring – Monitoring systems monitor the on-screen activity of students. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. See UK Safter Internet Centre Guide for education settings and filtering providers.

The Use of Technology in the Classroom and Beyond

Technology is used extensively by pupils, staff and visitors in MHSG. It is considered a crucial part of effective teaching and learning.

Guidance on the use of technology in the classroom and beyond, including by staff and pupils can be found in the Policy for ICT Use by Pupils (Appendix A) and the ICT Code of Conduct and Acceptable Use Guidance for Staff (Appendix D).

In addition, visitors to school are able to access the School wifi with their own devices in school. However, when accepting the connection to our system, all visitors agree to a terms and conditions

statement relating to their use of devices. Upon arrival at the School, visitors are also provided with the instruction that they:

(i) should not use any form of electronic device within the School without the express permission of the member of staff responsible for, or co-ordinating the visit. This includes the use of mobile phones
(ii) should not use photography or video equipment on the school site unless agreed prior to the visit by the Director of Digital Solutions / Estates Manager / Development Director in conjunction with the DSL (Designated Safeguarding Lead) if necessary
(iii) may connect to the School wifi but that this is provided at the discretion of the Director of Digital Solutions via the authorised channels only

Breaches to any of these instructions may lead to the visitor being asked to leave School premises and, if appropriate, external agencies consulted.

If pupils abuse the Policy for ICT Use by Pupils, the Deputy Head (Pastoral) will decide upon appropriate sanctions. Depending on the results of any associated investigation, the sanctions can range from a lunchtime detention to expulsion.

Specific advice provided to the pupils in relation to their use of mobile phones is published and pinned on all form notice boards. This can be found in Appendix D of this policy.

The School's Technical Provision and Associated Safeguards

A firewall and internet traffic monitoring systems are in place to provide the appropriate hardware and support services to ensure the School has a robust web-filtering and appropriate reporting capability to meet the demands of our safeguarding duties. As part of this, the Smoothwall system allows us to monitor in real-time and report on web usage of pupils, staff and visitors. As a way of implementing Filtering and Monitoring mechanisms, considering AI, we are investigating the implementation of key logging software (October 2023)

The School Governing body have overall strategic responsibility for filtering and monitoring. A member of the Senior Leadership Team and a Governor will work to ensure standards are met. These people are the DSL and the Safeguarding Governor.

A member of staff is responsible for the day-to-day management of filtering and monitoring systems. This person is the Director of Digital Solutions as they have specialist knowledge of both safeguarding and I to be the effective lead in this area.

In order to meet the technical standards required the DSL and Director of Digital Solutions are responsible for:

- procuring the filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why.
- reviewing the effectiveness of the provision.
- overseeing reports
- procuring a system which identifies risk
- ensuring that all staff: understand their role - are appropriately trained - follow policies, processes, and procedure - act on reports and concerns.

In addition to the above the DSL will take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems.

The Director of Digital Solutions will have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems.

Clear daily reports of 'suspicious activity' are provided for the Deputy Head (Pastoral) who is the Designated Safeguarding Lead (DSL) so that she can monitor web searches in line with safeguarding and 'Prevent' recommendations.

Building Resilience

It is an important part of the School's pastoral care programme to ensure that pupils are provided with the education and resilience needed to protect themselves and their peers from online dangers. This is facilitated through the following:

(i) E-Safety education is built in to the School's Well Being programme. E-Safety sessions are delivered by the DSL, members of the Computing Department and the Director of Digital Solutions. The focus of the sessions is not only on educating the pupils on information relating to the benefits and dangers of online use but also in encouraging them to develop those characteristics which enable them to be responsible online, resilient if something goes wrong and the courage to report and gain support when further help may be needed. For example, the 'Zip it, Block it, Flag it' message is used with pupils in Years 7 – 9 to summarise key issues relating to online safety.

(ii) The pupils themselves are encouraged to provide input into the advice provided to all pupils about the manner in which members of the School community should interact online. In this way, the DSL summarised the advice of the pupils into the 'MHSG E-Safety Charter' which is published in the pupil planner for pupils to read. This can be found in Appendix B of this policy.

(iii) Assemblies are used as a vehicle for teaching about responsible online use and strategies pupils can use to avoid associated dangers.

(iv) The DSL uses the School's 'Thought of the Week', on occasion, to remind pupils of the importance of resilience when facing online challenges. This is used in response to issues taking place within School or responding to situations in the news which may be relevant to online safety.

(v) The DSL uses 'Theme Weeks' such as 'Perseverance Week' to encourage pupils to reflect on the importance of resilience in their interactions with those around them.

Professional Development for Staff

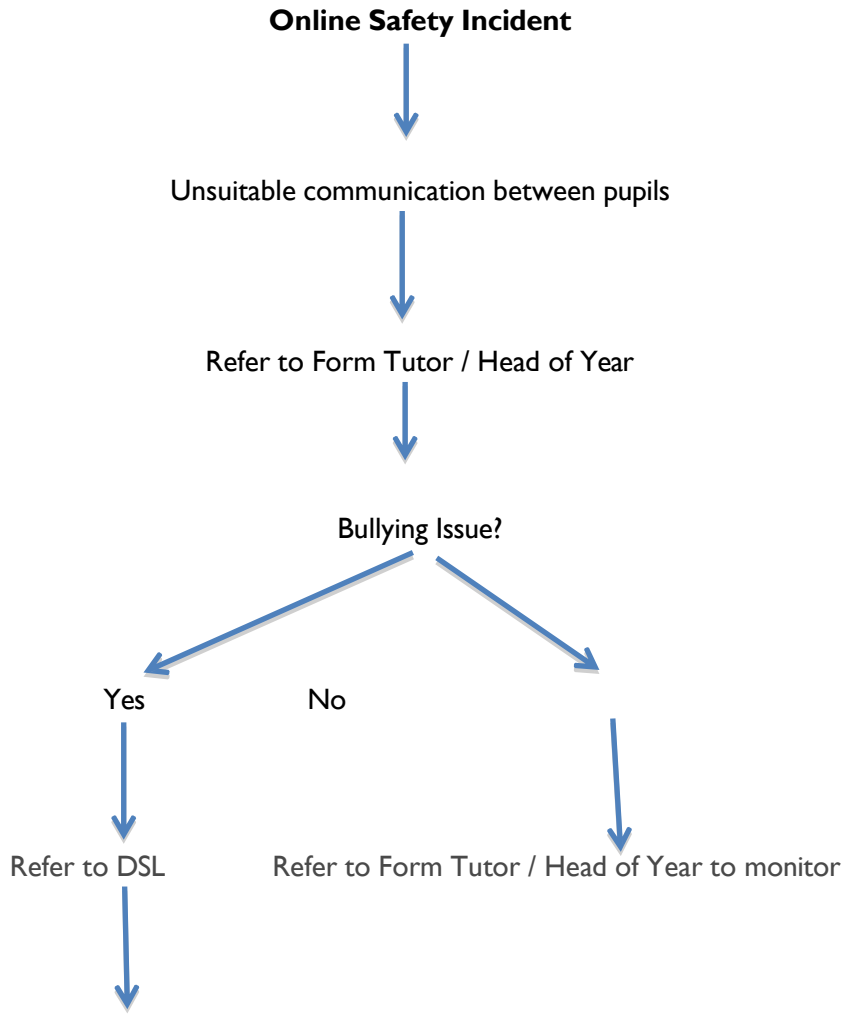
E-Safety is considered part of the wider school strategy in relation to safeguarding. As such, staff receive information relating to online dangers in staff meetings as well as when receiving their safeguarding update training. External training relating to E-Safety is provided as necessary and is available through Educare for all staff to ensure that they are informed of the most up to date guidance.

Reporting and Responding to Concerns

The DSL receives daily updates of suspicious internet searches, as recorded by the Smoothwall systems. Based on these records, the DSL uses a table in the format shown on the following page to record concerns and how these may be followed u

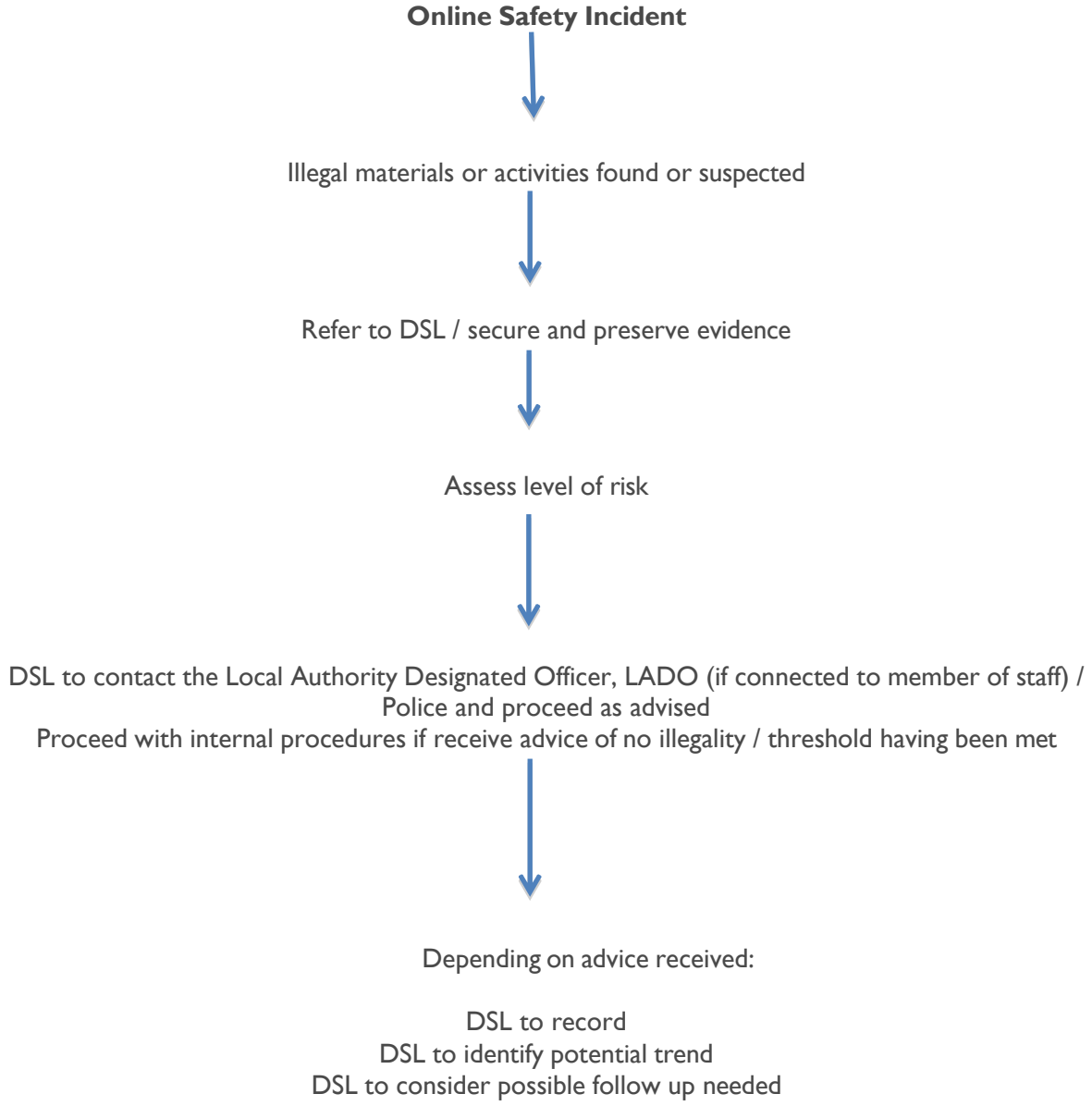
Reporting log						
Date	Time	Incident	Action Taken		Link with potential trend/indirect follow up advised	Signature
			What?	By whom?		

The following flow-charts summarise the procedures used in school to report issues and concerns relating to online safety:



- DSL to investigate DSL to liaise with parents
- DSL to sanction as appropriate (in conjunction with Head Mistress if sufficiently serious to warrant suspension / expulsion)
- DSL to contact Police if any evidence of criminality DSL to record in bullying log
- DSL to identify potential trend

- DSL to advise regarding follow up (Well Being provision / assembly)



If appropriate, the DSL will liaise with the Director of Digital Solutions to review changes to systems and procedures.

Communication with Parents

The School considers the parents / guardians as having a vital role in the education of pupils on E-Safety. The School uses the following main strategies for working in partnership with parents in ensuring the ongoing safety of the pupils:

(i) Twilight information sessions and Information Evenings at the start of the academic year are used to educate pupils and parents on E-Safety related issues and the importance of responsible online use

(ii) The DSL uses the weekly bulletin to provide information relating to topical E-Safety issues for parents, encouraging school and parents to work in partnership to ensure the safety of all pupils

Personal Data

Information relating to the management of personal data can be found in Appendices A and D to this policy as well as in the School's Data Protection Policy.

Roles and Responsibilities

The safety of pupils online forms part of the School's wider safeguarding responsibilities. Key roles and responsibilities are set out as follows:

The Deputy Head (Pastoral):

The Deputy Head (Pastoral) leads on E-safety within the School and is the School's E-Safety Coordinator in addition to being the DSL. She has the following roles and responsibilities:

- To be trained in E-Safety issues and be aware of the potential for serious child protection issues resulting from online behaviour
- Establish and review the School ICT and E-Safety policy in line with her wider safeguarding responsibilities
- Provide training and advice for staff
- Liaise with the Director of Digital Solutions to ensure the ongoing safety of ICT systems within school
- Liaise with the Head of Well Being to oversee the provision of E-Safety education to the pupils through Well Being lessons
- Liaise with the Head Mistress, Heads of Sections and Heads of Year to oversee the provision of E-Safety education through school assemblies
- Communicate concerns relating to E-safety with parents
- Provide information and education sessions for parents through Information Evenings and Twilight Information sessions
- Receive a daily log of suspicious searching activity to monitor individual risks and to inform future developments
- Administer sanctions, as appropriate, to those pupils who maliciously misuse ICT systems
- Investigate any issues which relate to cyberbullying and administer sanctions as appropriate
- Identify any trends which can be detected in relation to misuse of systems by pupils and identify ways of following up such concerns

The Director of Digital Solutions works with the ICT support staff to:

- Ensure that the School's ICT infrastructure is secure and is not open to misuse or malicious attack
- Provide all users who may access the School's network with a properly enforced password protection policy
- Update and apply the School's filtering and monitoring systems on a regular basis
- Update and implement the School's monitoring software and systems on a regular basis
- Keep up to date with E-Safety technical information in order to inform and update the DSL as relevant
- Ensure that the DSL receives a daily log of suspicious searching activity
- Liaise with staff who report any suspected misuse of ICT systems

- Report any misuse of ICT systems to the DSL

Teachers / Heads of Section / Heads of Year / Support Staff:

- Have an up to date awareness of E-Safety matters and the School's ICT and E-Safety policy
- Read, understand and uphold the Staff Acceptable Use Policy and the Staff Code of Conduct
- Report any suspected misuse of ICT systems to the Director of Digital Solutions
- Report any E-Safety concerns to the form tutor / Head of Year / / Head of Section / DSL as appropriate
- Report any inappropriate mobile phone use to the Form Tutor / Head of Year via the SIMS Behaviour Management System
- Deliver relevant E-Safety Well Being lessons to forms as directed by the Well Being Coordinator
- Ensure that pupils within forms understand the pupil acceptable use policy and how to interact positively online
- Ensure that pupils within forms understand the School procedures in relation to the use of mobile phones, cameras and hand-held devices and report any associated concerns as appropriate
- Display the mobile phone procedures notice on form notice boards
- Guide pupils to sites checked as suitable for their use in lessons

Pupils:

- Sign the Policy for ICT Use by Pupils so that they understand their responsibilities in using the School ICT systems
- Understand the need to report abuse, misuse or access to inappropriate materials
- Read and understand relevant sections of the School planner which relate to appropriate behaviour online

Head Mistress:

- Monitors and evaluates the implementation of the School policy in relation to ICT and E-Safety

Governors:

- The Safeguarding Governor meets each term with the DSL who updates them on E-Safety strategy in line with wider safeguarding duties
- Monitor and evaluate the implementation of the School policy in line with their duties

Reviewed and updated by the Deputy Head (Teaching and Learning) June 2021
Appendix D reviewed and updated by the Head Mistress with advice from Ellis Whittam September 2021
Substantive changes from KCSIE23 added by the DSL September 2023. Minor update October 2023.

Appendix A

POLICY FOR ICT USE BY PUPILS

ICT USE IN SCHOOL

We believe that the use and availability of ICT can bring great benefits to learning. The School ensures that pupils have access to a range of ICT facilities and resources that will enhance their learning activities. Our ICT Support team works to maintain these facilities, assist users and protect the School and individuals from the misuse of ICT. However, it is the responsibility of all individual pupils to guard against misuse of our facilities through their actions.

This policy applies to the use of all hardware, software and services provided by MHSG. This includes (but is not restricted to) all internet, electronic mail and other communication facilities, multi-user computers, personal workstations, micro-computers, and any networks connecting them provided by MHSG. Many elements of this policy also apply to the use of personal devices both on the school site and off site (in relation to accessing remote resources or working at home).

Pupil Access to ICT Facilities

There are many ICT suites, laptops and other computing devices available to Senior School pupils. Pupils have specific Computer Studies lessons and many other subject areas use the ICT suites as part of their programmes of study.

Pupils are allowed to use ICT Room E18 at break and lunchtimes. They may not use the computer rooms after 3.45pm unless a member of staff has agreed to supervise. The Library suite normally has supervised access after school hours from Monday to Thursday.

Pupils must observe the following guidelines:

- Read, understand and agree to the School's ICT Use Policy
- Report technical faults to the member of staff supervising and/or the ICT technician

Printing

The School employs print management software to monitor and account for pupil printing. All pupils have the ability to print, however there are restrictions on the volume and type of printing placed on their accounts. The primary aim of the print management software is to reduce waste of paper by encouraging responsible use.

- Pupils should be environmentally aware and avoid excessive printing.
- Large documents may be intercepted by the print management software and pupils will need to request their release
- Colour printing may require additional authorisation
- Pupils should report any printing problems to the nearest teacher or ICT technician as soon as possible.

Other computers in the School

Each teaching classroom has a computer installed for use by the teacher. Pupils **may not use** any of these machines without the specific permission of a member of staff. Computers located in offices are not for pupil use.

Internet Access

MHSG pupils have access to the internet via their ICT Network account. In addition to access via school computers, pupils are permitted to connect their personal devices (phones, tablets, laptops etc.) to the Pupil wifi which will enable them filtered access to the internet. Further details on the use of personal devices is given below. All ICT use is managed by monitoring systems that:

- Maintain records of internet sites visited, web-searches, electronic communications, network activity. This includes via personal devices connected to the school wifi.
- Block access to materials or commercial activities that are considered inappropriate for school-aged pupils, that might pose a risk to the security of the school network or an individual using that network or are considered disruptive to effective teaching and learning.

Examples of inappropriate and unacceptable use are:

- releasing School information to unauthorised individuals
- sending, forwarding, browsing, exporting from or importing into the School any material that is pornographic, obscene, profane, offensive, libellous, defamatory, illegal or of a criminal or subversive nature
- sending or forwarding commercial or advertising material
- violating other people's privacy, including uploading text referring to staff or pupils or uploading images representing staff or pupils
- using chat lines or similar services
- damaging other pupils' work in any way
- committing the School to buy or acquire services or goods
- downloading unauthorised software and files, including sound and video files
- playing games
- using the network for sending SMS messages
- any use that could bring the School's name into disrepute or that could be damaging to the School
- any attempt to by-pass the School's security and content-filtering system

Note should be taken of the following three legal points:

1. The use of personal data in any public display is subject to the Data Protection Act.
2. Using the internet to access any School or third party facility for which the user does not have authority is an offence under the Computer Misuse Act.
3. Using the internet to download or otherwise copy copyrighted software, information or other material without adhering to its licensing conditions is an offence under the Design, Copyright and Patents Act.

The School reserves the right to retrieve and look at all emails at any time, without the permission of the person and without notice. Users should have no expectation that any electronic information will remain private.

E-Safety

The School recognises that the internet and other digital technologies have the potential to be used in both positive and negative ways and works with pupils and parents to promote e-safety and the responsible use of ICT. E-Safety principles and practice are taught in both the Well Being Programme and in Computer Studies lessons. Pupils need to be aware that their own actions may increase their personal risk of becoming a victim of inappropriate attention online. Parents have a key role to play in supporting the School's work in promoting e-safety and the responsible use of ICT and are asked to talk with their daughter about the risks she might encounter and help her to develop safe and responsible behaviour when using technologies.

The School also employs a range of measures to protect pupils from incidents of cyber-bullying, inappropriate communications via social networking, exposure to inappropriate internet content, illegal activities and content liable to be offensive to members of our School community. These measures include the blocking of certain websites and monitoring an individual's internet use.

The correct use of ICT accounts and passwords

All pupils are issued with their own user account to access the ICT Network, MSOffice 365 services and Moodle. Several academic departments also subscribe to online resources to support learning in their subject area. Each user account on the network is protected by a personal login - a user account name and a password set by the pupil.

- Any pupil who forgets their password should request it to be reset, through their Form Tutor or directly to the Director of Digital Solutions.
- Pupil users should not tell anyone their personal login details under any circumstances.
- Pupils will be held responsible for all network activity that occurs using their user account.

Microsoft Office 365

All pupils are issued with a Microsoft Office 365 account. This service provides each pupil with an email address, online file storage and access to the Microsoft Office suite of programmes, including Teams. Pupils are able to use both the online versions of office and to download the software to their home computers, tablets and phones. The email address given to pupils as part of this package is stored on our administrative systems and is the one used by the School to communicate electronically or provide access to additional learning services. Any email communication to pupils from members of staff will be sent to this address and pupils are expected to check their school email messages at least every two working days.

Moodle

MHSG uses a Moodle Learning Platform to support learning. In the Senior School, each pupil has their own Moodle account which they can use in school and at home to gain access to subject resources. Parents also have their own Moodle account. Parents of new Year 7 pupils will receive details in the documentation that is sent home after the Taster Day in June. It is important that the contact details in this account are kept up-to-date.

SIMS Student

Senior School pupils are provided with access to the SIMS Student service which allows for direct communication between school and pupil, access to their timetable and other calendared events as well as access to reports.

ICT security and data storage

User data, personal files and documents are stored on the server, making use of individual user accounts. All data stored is backed up regularly by the School and held securely.

- Hardware, software and data should be treated as a valuable resource and with respect.
- The use of USB memory devices and external hard drives is strictly forbidden on the School network. (This includes pen drives, memory sticks and media players.)
- Pupils wishing to bring files into school from their home computers may do so using Foldr (foldr.mhsg.manchester.sch.uk), by emailing it to themselves or by using facilities made available in their MSOffice 365 account.
- Particular care must be taken when accessing email attachments or downloading documents from the internet. If a pupil has any concern about such a file, it must be reported immediately.

Malicious software protection

Major disruption and damage can be caused by computer viruses, particularly on computer networks. All computers on the School network are protected by Anti-Virus software and any alerts must be

immediately reported to the supervising member of staff, ICT Support or the Director of Digital Solutions.

Copyright

- Pupils must respect software copyright by keeping to licence agreement terms.
- The unauthorised copying of software is unethical and illegal.
- Software must not be copied (other than as back-up to the original) and software acquired for use on one machine must not be loaded to a second machine.

The use of "outside" software

- Pupils must not attempt to install their own software onto any machine.
- The School will avoid the use of software supplied from any unauthorised or unknown outside sources for the following reasons:
    - breach of copyright
    - danger of computer viruses
    - dangers of corruption of existing systems and/or data

MHSG wifi access and the use of personal laptops or other mobile devices

Wifi is available across the entire site to support the use of laptops and other mobile computing devices such as phones and tablets. Pupils are allowed to connect their own devices to the appropriate wifi channel (MHSG Pupil BYOD) to allow them access to the internet. This connection allows access to the internet and web-based resources only, it does not allow direct access to network resources and is monitored and managed in the same way as all pupil access to the internet.

Pupils will be informed of the Wireless Access Key at the start of the academic year, and can subsequently login with their network details to the MHSG Pupil BYOD wifi.

- Pupils should not attempt to connect any personal laptop or mobile device to the school network (MHSG domain).
- All connections to the pupil wifi should be for learning and research purposes and pupils should be aware of restrictions on locations and times for wifi use.
- Pupils must be aware that any personal device brought into school should be covered by their own / family's insurance arrangement – it will not be covered by the School's insurance.
- Pupils must take appropriate actions to ensure their personal safety while carrying a high value device – especially in public areas adjacent to the School, on the buses and while travelling between home and school.

The use of digital cameras, mobile phone cameras and other recording devices

- Digital cameras, mobile phone cameras, and other recording devices must only be used in lessons as directed by a teacher or with permission from the Deputy Head (Pastoral).
- If permission is not obtained in advance, the use of such devices will be regarded as a serious disciplinary matter and will be dealt with severely.
- Images must not be taken of school staff, pupils in uniform or areas of the school building.
- Images of School staff, pupils or areas of the School building must not be placed on the internet.

Appendix B

MHSG E-Safety Charter

As a member of the Manchester High School for Girls community, I value the following rights and responsibilities relating to internet use:

I have the right:

- To use the internet without fear of bullying
- To report comments that I find unacceptable
- To tell someone if I feel uncomfortable about something I see online
- To say 'no' if someone asks me to do something I do not want to do
- To know who I am talking to online
- To access websites that are appropriate for my age
- To use the internet to communicate with my friends and to learn
- To have control of images, videos or work that belong to me
- To keep my accounts private
- To be trusted

I have the responsibility:

- To access reliable and trustworthy websites
- To not plagiarise information I read on the internet
- To treat others online as I would want to be treated
- To be aware of my own personal safety online and not swap personal information with people I do not know
- To keep my accounts secure
- To report bullying or abuse
- To post information responsibly. After all, everything I post can stay online forever
- To only talk, online, to people I know
- To respect the privacy of others
- To think before I click

Appendix C

The Use of Mobile phones at MHSG

Mobile phones are a fantastic resource not only for communicating with our friends but also for learning. However, they must be used responsibly. The following rules apply to the use of mobile phones at MHSG:

1. You must not use mobile phones in corridors or in the dining room. You can use your phones in your form rooms, in the locker areas and on the lawn during break and lunchtime.
2. Ensure that your mobile phone is switched off or put to 'flight mode' during lessons **and** form time.
3. You must not use your phone to contact parents if you are feeling unwell. One of the School Nurses will make the decision as to whether you are well enough to stay in school and will make contact with your parents if necessary.
4. You must not use your phone to take photographs or film of your friends in school or when they are wearing school uniform, unless you have specifically been given permission by a teacher.
5. Use your phone responsibly. Do not use it to send unpleasant messages or to engage in malicious gossip. Such behaviour will be regarded as bullying and treated very seriously.

The following sanctions will apply if you do not use your phones appropriately over the course of one academic year:

First Offence:

1. Lunchtime detention and letter sent home to parents.

Second Offence:

2. After–school detention of 30 minutes and letter home to parents.

Third Offence:

3. After-school detention of 1 hour and letter home to parents.

Fourth Offence:

4. Mobile phone handed in to reception every morning and collected at the end of the school day. This sanction will apply for the remainder of the school year.

Appendix D

ICT Code of Conduct and Acceptable Use Guidance for Staff

Introduction

Information and Communication Technologies (ICT) have become an essential resource in supporting learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. The school has invested in multiple electronic systems and developed processes for effective management of data relating to pupil performance, pastoral information, contact and financial management. Many of the interactions we have on a professional and personal level have become intrinsically linked with both fixed and mobile technologies to the extent that the competent use of ICT is a de-facto requirement. Pupils, parents and the wider community also have an increasing expectation that information, services and communications will be via electronic methods.

The use of ICT is therefore critical to the efficient and effective daily business of the school and its future development. It is crucial that all users are aware of fundamental operating procedures which are designed to ensure that:

- the ICT network and other ICT resources are used responsibly to maintain their availability and effectiveness.
- colleagues are alerted to the potential risks of using electronic communication and the internet.
- the ICT network is not disabled by viral infections or that its held data is not compromised through security breaches.
- colleagues guard against access to unlawful, offensive or contextually inappropriate material, accidentally or otherwise.
- colleagues are aware of their professional responsibilities in their institutional and personal use of ICT.
- in accordance with the 'Prevent Strategy', all staff have a duty to protect students from radicalisation and report to the) Designated Safeguarding Lead any use of ICT to access materials that may encourage radicalisation, support or promote terrorism or compromise counter terrorism measures.
- colleagues are aware of the statutory and precautionary measures taken by MHSG for the safeguarding of pupils, data and the reputation of the institution.

Legislation

There are numerous pieces of legislation which affect the way our systems are managed, the use of the facilities made available to staff and the nature of materials downloaded, uploaded or communicated. The most relevant ones are:

- **Computer Misuse Act 1990:** This covers three basic offences: unauthorised access to computer files or software; unauthorised access with intent to commit further offence; unauthorised modification of a computer or software to impair its operation.
- **The Data Protection Act 2018:** This Act relates to personal data held on computer. All colleagues must maintain the confidentiality of any such personal data and ensure that it is only used for the purpose for which it was intended.
- **The Copyright, Designs and Patent Act 1988:** This Act forbids the making of unauthorised copies of computer programs or software, text, music, films and images. It is also an offence to use, distribute or permit the use of such unauthorised copies.

- **Communications Act 2003 / Malicious Communications Act 1998:** These cover the sending by, means of the Internet or email, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety.
- **Public Order Act 1986 / Racial and Religious Hatred Act 2006:** These cover criminal offences related to the possession or publication of material designed to threaten racial or religious hatred or likely to stir up such hatred.
- **Obscene Publication Act 1959 and 1964:** This covers the publishing of "obscene" materials.
- **Child Protection Act 1978:** This covers the creation (including permitting creation), possession, display, distribution or advertising of indecent images of children under 18 years of age.
- **Sexual Offences Act 2003:** This covers the grooming of a child; creating, possessing, viewing or distributing sexual images of children. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.

Code of Conduct

This Code of Conduct applies to the use of all hardware, software and services provided by MHSG. This includes (but is not restricted to) all internet, electronic mail and other communication facilities, multi-user computers, personal workstations, micro-computers, and any networks connecting them provided by MHSG. Many elements of the Code of Conduct also apply to the use of personal devices both on the school site and off site (in relation to accessing remote resources or working at home).

The MHSG Network and ICT Hardware

MHSG provides many ICT facilities for use in connection with the duties for which you are employed and the purposes of education. Limited use of our facilities for personal purposes is permitted; MHSG acknowledges that personal use may occur from time to time. Colleagues should be mindful that resources are shared and that personal use should be restricted to a minimum during break, lunch and free periods and that other staff requiring access for work needs take priority.

- Colleagues must keep their personal password confidential and follow the MHSG password protocol.
- Colleagues must not disclose any system, computer or services password to unauthorised users. This includes the sharing of WiFi access codes beyond their intended usergroup.
- When leaving the PC unattended, colleagues must lock their workstation or log off the system to prevent unauthorised users using the PC in their absence.
- Personal data, SIMS data, PASS data, the content of emails or other sensitive information should not be shared with pupils or parents other than when it is specific to them. Staff should be mindful in their use of data projectors/screens to ensure such data is not inadvertently displayed.
- Colleagues should not open other colleagues' files without their permission although ICT personnel may need to access both colleagues' and students' files. Colleagues must not corrupt, interfere with or delete any other user's information.
- The general use of USB connected storage devices (eg. Memory Sticks, USB Pen Drives, External Harddrives etc) is strictly forbidden on equipment connected to an MHSG domain. Exception will only be granted by the Director of Digital Solutions or ICT Systems Manager and will require ICT Support intervention.
- Any damage to ICT equipment must be reported promptly to one of the ICT team.
- Colleagues must not reproduce copyright material without first getting permission from the owner. All resources should clearly acknowledge the source used.
- The viewing of Internet sites which contain inappropriate humour, explicit language, racism, sexism, offensive images, religious extremism or incitement to terrorism is forbidden.
- Colleagues must not use the ICT network to play computer games.

- The MHSG Staff BYOD WiFi network is provided to allow staff to utilise their own devices while on the school site, this network provides appropriate separation between personal devices and the school network.
- Colleagues should not connect their own devices directly to an MHSG Domain (either wirelessly or via a cable) without the permission of the Director of Digital Solutions. Guests requiring WiFi access should obtain a Guest Pass from the Director of Digital Solutions.
- Teaching staff should avoid personal use of email or the internet when they are teaching a lesson and support staff should confine their personal use to breaks or lunchtime.
- Printing should be kept to a minimum. Bulk printing requirements should be submitted to the Reprographics team or directed through the high volume photocopiers.
- Colleagues should be mindful of where printed materials will emerge and ensure that sensitive information is not left unattended. Secure printing facilities are available through the photocopiers.
- The use of any mobile device, camera or recording equipment (school owned **or** personal) within the EYFS setting is statutorily restricted. Colleagues must not take their own devices to that area of the school and gain specific agreement from the Head of Prep or the EYFS staff before using any school owned device in that area or with EYFS pupils.

Confidentiality of Information

MHSG holds significant volumes of personal and confidential information and as such is bound by the Data Protection Act (2018). Many of the security and operating procedures in place are designed to maintain our compliance with this Act. All employees are required to act in such a manner that data is securely maintained, used for intended purposes only and not inappropriately shared. This applies equally to users working on the site and remotely.

- Colleagues must not share any personal information held by the school with any unauthorised person or organisation. Colleagues should seek advice (and where necessary authorisation) from the Director of Digital Solutions or Senior Leadership on any request to share data.
- Any data shared with an outside organisation for support, research or training purposes should be appropriately anonymised.
- SIMS or PASS screens should not generally be shared with pupils or parents (except in the course of one-to-one or direct discussion on pupil performance)
- School data should not be copied, transferred or downloaded to personal computing or storage devices without the express permission of the ICT Development Director or Senior Leader. Authorised data transfers over the Internet should be via a secure connection and stored data on external devices should be encrypted.
- Colleagues are encouraged to use Remote Access (which is secure) rather than transferring data out of our systems.
- Colleagues using personal devices (home computers, tablets or other mobile devices), both on site and remotely, are required to maintain appropriate security and protection procedures. All personal devices should be password protected, be maintained with appropriate anti-virus protection and be protected from unauthorised access. We recommend that security updates are regularly applied and Operating Systems updated as appropriate.
- If a colleague loses a device that has been linked to our school systems (email, Remote Access, VPN) they should immediately change their network password and/or request that their network account is secured to prevent unauthorised access.

Use of Email

Email is the cornerstone of most of our communication between each other and with pupil and parents. The use of email has allowed us to be much more responsive and frequent in our dialogue while at the same time enabling us to maintain effective records of dialogue we have had. Staff should be aware of some key principles of email and the school policy and procedures in using it.

Drafting of emails

- Email is an insecure communication method; contents can be easily read, copied, forwarded and archived.
- Colleagues are advised to take the utmost care when sending emails which contain confidential information and must ensure that such information is not disclosed to third parties. Colleagues must not release personal details including phone numbers, fax numbers or personal email addresses of any colleagues or student over the internet other than for official returns.
- All users have a responsibility to draft emails carefully in accordance with the standards of any other form of written communication. Colleagues must not send any message which is likely to cause annoyance, inconvenience or needless anxiety or use language which is offensive, abusive, obscene, menacing or any that may incite hatred against any ethnic, religious or other minority. Colleagues must check contents with respect to discrimination, harassment, defamation or causing any damage to the reputation of MHSG. The law of libel applies to email; both the author and MHSG can be held responsible for the contents if it contains unlawful damage to the reputation of the recipient or a third party, whether a person or corporate body.
- The size of email attachments should be kept to a minimum as large attachments result in slow transmission times.
- Colleagues must not send any unsolicited promotional or advertising material or chain letters or pyramid selling schemes.
- All outgoing emails are scanned for inappropriate content (including attachments). If an email is blocked, the sender will be informed and may request release. (Release is at the discretion of the ICT System Manager who may decline such a request if the email is believed to be in breach of school policies).
- A disclaimer is automatically attached to all outgoing MHSG email; however, this does not remove the personal responsibility of the originator to ensure that emails conform to the law and MHSG protocol.

Received Emails

- Colleagues must be aware that in-bound emails may contain explicit or offensive material that is beyond their control or that of MHSG and should be aware of their situation when opening.
- All incoming emails to the school system (including attachments) are scanned for viruses, inappropriate language or material.
- Emails which are deemed to be either a risk to our system or containing inappropriate material may be blocked from delivery. Users will receive notification of blocked emails and be given the option to request its release. (Release is at the discretion of the ICT System Manager who may regard the risk too great and decline a request)
- Colleagues are required to report email content which breaches standards of decency or contains inappropriate material to the Director of Digital Solutions, Designated Safeguarding Person or Headmistress.
- Colleagues are responsible for verifying the validity of any attachments received before opening them on the MHSG network. If an email is not expected, or comes from an unfamiliar source, or from overseas please consult the ICT Systems Manager for guidance. If colleagues have any doubt, the attachment must be deleted without opening.
- Colleagues should also take caution on acting on the contents of emails that are requesting personal information or asking for you to log into services (phishing). Again, if in any doubt about the validity of an email, seek advice from ICT Support.
- Where a response is required, colleagues should to respond to emails from pupils or parents within 2 working days. That response may be an acknowledgement while further clarification or information is sought. Colleagues are requested to respond to internal emails within a timescale reasonable to the request.

Monitoring of Email

- Automated email monitoring and blocking systems are in use used MHSG.
- Incoming and outgoing email content may be read at any time by monitoring staff.

- MHSG reserves the right to retrieve the contents of email and other files when a colleague is absent, for the purpose of determining whether use is legitimate, to find lost messages or retrieve messages following computer failure, to assist in the investigations of wrongful acts, or to comply with any legal obligation.
- Colleagues cannot expect the content of any email message composed, received or sent via the MHSG network to be private, regardless of the use of the personal passwords.

Use of the Internet

Use of the internet and web based resources within the classroom for learning, teaching and in the preparation or sharing of resources is common and its benefits are well established. As such, MHSG make access to the Internet and the World Wide Web available to students, teachers and support staff and colleagues are encouraged to utilize the Web to enrich our students' experiences.

- All internet traffic into and out from the school is monitored for the purposes of security, safety and decency.
- The school utilizes a Firewall policy to protect its Network and data from unauthorized access. Staff should not attempt to circumvent the Firewall: if a change in the school's Firewall policy is required for the deployment of a specific resource or development, a request must be made to the ICT System Manager.
- The school enforces Web Filtering policies suitable for the nature of the establishment. Staff must not attempt to circumvent the Web Filtering applied without authorization from the Director of Digital Solutions or ICT Systems Manager. Attempts to bypass filtering and monitoring policies (either by the use of Proxy websites or by changed connections settings) will be considered a disciplinary issue.
- Staff may request that specific websites either be blocked or unblocked if current access arrangements are an impediment to learning or teaching. Such requests will be considered on a case by case basis and may be refused. Teachers should not expect a site to be unblocked immediately on request.
- If a course being delivered may require yourself or students to access materials that you know may be in breach of general guidelines (eg. information relating to the growth of extremist views, terror related activity etc.), this should be discussed with the Deputy Head responsible for Safeguarding in advance of any request to the Director of Digital Solutions.
- Web Filtering as a method of limiting access to inappropriate material is an inexact science, it cannot be 100% guaranteed that our system will block all inappropriate material or that will not unexpectedly block seemingly innocuous websites.
- Teachers should check the appropriateness and availability websites before they use them in a lesson and also be aware that students have a different filtering policy applied to them that may affect the activities assigned.

Downloading Information

- Information should only be downloaded, ie, copied from an Internet site, and saved onto MHSG equipment if the user is certain of the integrity of the Internet site from which the information is to be obtained. When obtaining information in this manner the above rules apply in the same way. If the user is in any doubt regarding whether or not to access a particular web site or download information from one, advice should be sought from the ICT Systems Manager.
- Colleagues should be aware of relevant copyright when downloading and subsequently using downloaded text, images or media. While much material sourced from the internet may be used in classrooms for the purpose of teaching, ownership of the material is retained by the creator or publisher of the material and appropriate permissions should be sought for any use beyond timetabled lessons.
- Colleagues must not use the schools facilities to download (or attempt to download) pirated or copyright material or access peer-2-peer sharing networks (BitTorrent).
- All sites visited leave evidence on the computer being used and leaves a log in our management software. Colleagues must not attempt to visit internet sites with pornographic, racist, violent, extremist, terror related, illegal or illicit content. Viewing of pornography or obscene material

(whether an attempt is made to download material or not) will be considered as an act of gross-misconduct and is likely to result in summary dismissal and the police or other authorities may be involved to investigate such activity.

Streamed Media

- Access to streamed media is managed within the school's Web filtering policy.
- Teachers should note that the filtering policy cannot always determine the content of video/audio and as such they should review any media before use in the classroom. Teachers should also note that media may be blocked to students based on their applied filtering policy.
- Most media sharing systems have extensive comments/social media supporting them. Colleagues are cautioned to ensure surrounding information is appropriate to the audience.
- Teaching staff have several school based media systems available to them (eStream, Clipbank, Espresso) which are fully available as a teaching a learning resource.

Social Media and Online Presence

- Colleagues are cautioned in their use of Social Media (Facebook, LinkedIn, Instagram, Twitter etc.) to ensure that their use does not compromise their professional responsibilities or the reputation of Manchester High School for Girls
- Colleagues must not share opinions or images (personal, political, religious or racial) that are likely to cause offence, compromise the impartial nature of a teacher's role, cause embarrassment or discomfort to others, reflect poorly on their own character or bring the school into disrepute.
- Colleagues should be aware that some social media sites may be hosting material that would be in breach of the school's Filtering Policies and are cautioned to be vigilant.
- Colleagues should ensure that their online profiles are appropriately secure against: hacking; the sharing of inappropriate personal information; and the distribution of images, opinions, comments or connections that may compromise their position.
- Colleagues should also be mindful of how their friends/followers portray them within Social Media environments.
- Staff **should not** request, or accept a request, to "friend" (or equivalent) current pupils. Staff are cautioned in their friendship links to past pupils, especially if those individuals still have active family or personal relations within the school.
- All staff have responsibilities in maintaining the principles of eSafety relating to current and past pupils:
    - images of pupils should never be shared online without the permission of the parents and the Headmistress;
    - images and full names of pupils should never be linked in an online environment;
    - the use of any image should be appropriate to the age of the pupil, the activity being demonstrated and not be of a condition that could inappropriately manipulated;
    - the movement of pupils or other personal information should never be shared online; information on the health and welfare of pupils should never be shared online;
    - information that would allow an unauthorized individual to make direct contact with a pupil should never be shared;
- Where a colleague regularly contributes to an online publication (blog, online magazine etc.) or regularly comments on online forums, they should be mindful of the need not to bring the school or their position into disrepute, not to share personal information and, where appropriate, anonymize anecdotal or evidenced information. Articles that make specific reference to the school, its policies or procedures should be approved by the Headmistress before publication.
- Colleagues should be aware that their use of Social Media, forums, blogs etc. leaves a "digital footprint" which overtime can build a significant public profile on their character, interests and opinions.
- Colleagues must immediately report to the Head Mistress any instance of their email account (either school or personal), or any social media account, being used without authorisation by another person to impersonate them, misrepresent them or to portray them inaccurately.

Storage, sharing and copying of files

MHSG provides all users with personal storage space and access to shared storage spaces. While we do not put a figure on the volume of storage, users are requested to manage their retention of files on the school servers. Where files become obsolete (either by age, subsequent revision or duplication) they should be deleted or archived. This will enable us to maintain a more efficient and resilient network. Staff may request ICT support in the transfer of files to an archive.

- Filing / deletion of emails/files is to be managed by each colleague bearing in mind the limitations of data storage, archival records, contractual evidence and legal discovery issues.
- Departments should make use of shared areas to make files available to colleagues rather than emailing documents. (Emailing documents is likely to create multiple copies of the same file)
- Heads of Departments or equivalent should regularly review the shared areas they are responsible for to remove or archive obsolete files.
- Email and other files should only be copied to relevant parties and this should be kept to a minimum in order to conserve resource space. If a paper copy would not have been distributed, do not send an email copy. When copying or forwarding emails to other relevant parties please ensure that any attachments are absolutely necessary before they are sent, otherwise the attachment is continually duplicated across the network and this quickly leads to data storage and overall system performance problems.
- If an email contains information that relates to a colleague or student, a copy should either be copied into CPOMS or be printed and filed in the relevant file as with any other written communication.
- If you have saved attachments from an email, please delete the email (or Remove the attachment from the email) to save space on the email server and in your email account.
- Where possible, colleagues should use the Grangethorpe Portal or the VPN to access and transfer files from home (rather that emailing documents)

Guidance on the use of personal devices within school and for school related activities
Within this section, a personal device may be considered to include home computers, personally owned laptops, tablets, mobile phones, cameras or any other device capable of capturing, storing or transmitting forms of data.
Staff are permitted to use personal devices to connect to a range of ICT services both on and off the school site for the purposes of convenience or in the absence of an appropriate supplied alternative. However, staff must take note of specified restrictions, conduct principles and appropriate use guidance given below. Clarification on the use of such devices can be sought from the Director of Digital Solutions should any query arise.

- **Use of any personal device within the EYFS setting is strictly forbidden.**
- Any device brought onto the school site should be appropriately secured against unauthorized access: Tablets and phones should use password/passcodes to unlock; laptops should require user authentication.
- Home computers used to access restricted school resources should be username/password protected on startup and should lock when left unattended.
- Any personal device used to access school resources should be appropriately protected against viruses and from unauthorized access. We recommend that security updates are regularly applied and Operating Systems updated as appropriate.
- Staff should not use their personal phones to contact pupils or parents; staff should not use their personal email accounts to contact pupils or parents.
- Staff should not allow any pupil to use a staff-owned personal device, (unless in a genuine emergency situation in which it is in the best interests of the pupil's welfare).
- Staff are permitted to connect WiFi enabled devices to the MHSG Staff BYOD Network while on the school site. The WiFi Access Codes should not be shared with any non-staff member.
- WiFi enabled devices should not be allowed to create their own "WiFi Hotspots" or allow other devices or users to connect through them or access any of the personal devices' shared resources.
- Bluetooth, AirPlay or similar ad-hoc relationships should not be created between your device and school owned or pupil owned devices without the express permission of the Director of Digital Solutions.
- Colleagues must ensure that there is no inappropriate material on any device that they bring onto the site or into proximity with students. This can be defined as any material that would be considered inappropriate to view, download or store on school facilities.
- Staff should not use their personal devices to capture or store video or still images of pupils.
- Staff are permitted to use their own devices:
    - to access MHSG Exchange based email and calendars
    - to establish a VPN connection to personal and shared resources
    - to access Remote and Web-Based applications made available by ICT Support
    - to contribute (where authorized) to school websites, blogs and social media
    - in the preparation of pupil reports, reports for colleagues or reports for other authorities
    - in the preparation of learning and teaching materials
    - in the presentation of learning and teaching materials (where a suitable alternative is not available or convenient)
    - in cases of emergency where a school owned alternative is not available
- The following advice is issued to staff on the storage and processing of school information on personal devices:
    - The preparation, storage and transfer of learning and teaching materials on personal devices and home computers is perfectly acceptable
    - Colleagues are encouraged to use the VPN or Grangethorpe Portal to access and transfer personal and shared files rather than via email. Bulk transfer of such materials should be via One Drive or similar.

- Colleagues are encouraged to use Remote Access to SIMS to access school data rather than transfer data out.
- When personal, pupil performance or other sensitive data is required to be transferred to a home computer or personal laptop it must not be used for any other purpose that immediately intended; it should be retained only for the period of time necessary for intended processing; it should be deleted once its intended use has been completed.
- Staff should seek agreement from the Headmistress if any data is required to be retained for the purposes of research, training, academic study or statutory requirement. Where appropriate, school data should be anonymized and/or encrypted when stored off site.

- ICT Support Staff will, where possible, give assistance on the setting up and use of personal devices but are not in a position to offer extended technical support

Monitoring of ICT usage

- Staff should be aware that their use of ICT is monitored and logged by numerous automated and manual systems.
- The Headmistress, or other authorized authority, can request access to these logs which can record: *[NB: this is not an exhaustive list of logs and is under constant review]*
  - times and location of user logon to the network (both internally and through remote systems)
  - activity on an specified computer
  - access to and activity within SIMS and PASS and other data management systems
  - access to file and media storage
  - internet histories
  - email transactions
  - print histories
  - support requests
  - computer room requests

- Colleagues should not expect their use of ICT to be private, regardless of the use of personal passwords.

MHSG Staff ICT Acceptable Use Summary

Information and Communication Technologies (ICT) have become an essential resource in supporting learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. The school has invested in multiple electronic systems and developed processes for effective management of data relating to pupil performance, pastoral information, contact and financial management. The use of ICT is therefore critical to the efficient and effective daily business of the school and its future development.

The ICT Code of Conduct and Appropriate Use Guidance is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are required to read the guidance and adhere to its contents. Any concerns or clarification should be discussed with the Director of Digital Solutions, Deputy Heads or the Headmistress.

The key points of the Code and Guidance are summarised here:

- Do use the school's ICT hardware, software and associated services to support your professional activities, the business of the school and for other uses deemed 'reasonable' by the Head or Governing Body. Where suitable facilities are provided by the school, staff should primarily use these; staff may use their own devices where additional benefit to their roles can be achieved.
- Staff must comply with the ICT security protocols and not disclose personal passwords or those provided by the school or other related authorities. It is the responsibility of all staff to maintain the highest standards of security.
- Staff should ensure that all electronic communications with pupils, parents and staff are compatible with your professional roles and use only the approved e-mail system(s) for any school business.
- Staff must ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data accessed or taken off site must be encrypted and or anonymised.
- Staff must ensure that any images of pupils and/or staff will only be taken, stored and used for purposes in line with school policies and with written consent of the parent, carer or staff member.
- Staff should support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- Staff should ensure that online activity, both in school and outside school, will not bring their own professional role into disrepute, or that of the school.
- Staff should support and promote the school's e-Safety and Data Security policies and help pupils be safe and responsible in their use of ICT and related technologies.
- Staff should be aware of their duty to report incidents where the eSafety of students or colleagues is compromised in regarding to Safeguarding or the Prevent Strategy.
- Staff must not share any passwords that may allow unauthorised access to ICT systems or school held data. Staff should also ensure that they do not leave workstations or other access points unattended and at risk from unauthorised access. Where personal devices or home computers are used to access school based resources, these too should have appropriate security measures applied.
- Staff should not give out their own personal details, such as mobile phone number and personal e-mail address, to pupils.
- Staff must not install any hardware of software without permission of the ICT Development Director or ICT System Manager.

Reviewed and updated by the Deputy Head (Teaching and Learning) June 2021
Appendix D reviewed and updated by the Head Mistress with advice from Ellis Whittam September 2021
Substantive changes from KCSIE23 added by the DSL September 2023. Minor update October 2023.

- Staff must not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. All users should understand that any use of the Internet and other related technologies can be monitored and logged and can be made available on request of the Headmistress or other appropriate authority.
- Staff must ensure that images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headmistress.
- Staff should respect copyright and intellectual property rights.
- Staff must not use their own digital devices in any part of the EYFS setting in the school.

Staff must read, understand and agree to abide by the Code of Conduct and Appropriate Use Guidance to support the safe and secure use of ICT throughout the school. Staff must be aware that any breach of the Code or Guidance may lead to disciplinary procedures which could result in dismissal

Appendix E

Guidance for staff on the use of photographs

Definitions in this guidance document

- ***Photography*** includes digital images, photographic prints and transparencies, video and film
- ***In school*** is whenever and wherever pupils and young people are the responsibility of the School
- ***Child*** refers to any pupil under the age of eighteen.

Relevant laws in relation to images of children

Photography of children in schools is subject to the following legal rights:

- The Data Protection Act 1998, regarding the rights of individuals to have information of a personal nature treated in an appropriate manner
- The Human Rights Act 1998, protecting the privacy of individuals and families

As well as these statutory rights, restrictions on photography arise from the responsibility of every member of the School staff for child protection. Schools have a duty of care for their children; it is their duty to ensure that the safety of every child in their care not compromised.

Risks associated with digital photos

Photos that have been placed online may be altered and distorted. This could range from an image being changed in an unflattering way as a cruel joke (common with online bullies), merged with another image to misrepresent or mislead or even used to create pornography.

Consent for publication of images – a legal requirement

Images of pupils should not be taken if you do not have the consent of the child and if the parent has notified the School in writing that no photographs are to be taken. The Development and Marketing Director keeps a record of pupils whose parents have withdrawn consent. Parents are asked to write to the Head Mistress (Prep) or Development and Marketing Director (Senior School) when their daughter joins the School if they wish to withhold consent. They are also asked to discuss this with their daughter.

Unless the School has obtained consent, images of pupils must not be displayed on websites, in publications such as newspapers, the prospectus or advertisements or in a public place such as areas where visitors to the School have access.

Newspapers tend to want to put the names of pupils in photographs. As long as parental consent is gained and it is made clear that the photograph will be published in a newspaper, this is not a cause for concern.

Website editors should immediately remove all material relating to an individual if requested by the legal guardian of the individual or by the individual themselves.

If images are taken at an event attended by large crowds, this is regarded as a public area and permission is not required of everyone in a public crowd shot.

If the School has not been notified of a court order by the parent, it will be assumed that the parent has made an appropriate decision when completing the written consent form.

Purpose

Staff should take care to ensure that their action in photographing a child cannot be misinterpreted and there should be a clear educational purpose to taking the photo – for example:

- As part of the curriculum or an educational enrichment activity such as a school play, concert, visit or sports competition
- To record evidence of, or assess, achievement of a practical skill
- To celebrate achievement

Appropriateness of the photo

- Only use photographs of children in suitable dress. Children in swimming costumes are not to be photographed unless they are in the swimming pool. Where children are photographed in P.E. kit, the content of the photograph should focus on the activity and avoid full close up body shots.
- Photography should only take place in adequately supervised areas, not backstage in a production or in changing rooms. Staff should avoid taking images of children in one-to-one situations unless in a public area such as Main Reception.
- Staff should be aware of children's safety and challenge and report any inappropriate photography or intrusive photography
- Do not use images likely to cause distress or embarrassment to the pupil or parent.
- Try to represent the diversity of the pupils in the school.

Equipment

The use of personal equipment to take photographs of pupils is not permitted. Staff must use a school issued device when taking photographs or filming pupils.

The use of any mobile device, camera or recording equipment (school owned **or** personal) within the EYFS setting is statutorily restricted. Colleagues must not take their own devices to that area of the school and must gain specific agreement from the Head of Prep or the EYFS staff before using any school owned device in that area or with EYFS pupils.

Use and storage of images

- Photography of activities and trips may be used in the curriculum and displayed to illustrate the work of the school but it is important to plan what will happen to the image when the lesson / activity / display is over.
- Digital images should be deleted after use or stored in a school computer folder, not a home computer or personal mobile telephone.
- Images must be carefully and securely managed, so that there is no possibility that they could be used to stalk or groom a child or be manipulated so that they can be used for pornographic purposes.
- Any paper photographs remaining after use should be offered to the Archivists or the pupil and if declined should be destroyed. This is the responsibility of the member of staff who has taken the photograph
- Members of staff need to be able to justify any images of pupils in their possession.
- Staff should only forward or distribute images to other members of staff for a clear purpose and this must not be done on personal devices.

- Photographs contributing to the history of the School, its pupils, activities or the community can be retained indefinitely in the School Archives, as indicated on the consent form. These are the responsibility of the Archivists.
- Photographs and film used for external publicity will be the responsibility of the Development and Marketing Director. These will be stored in a secure computer folder accessible only to members of the Development and Marketing Team.

Information accompanying the image in publicity material
If a photograph is used for publicity material, avoid using the full name of the pupil. Use the first name only.
Do not include any personal information about the pupil, for example address, email or other contact details.
For video footage identifying information should not be included in the sound.

Parental Photography

Photography in schools traditionally forms a long-lasting part of each family's record of their child's progress and a celebration of success and achievement as well as being an established social practice. Where practical, arrangements should allow photographs to be taken by parents and other guests attending school sports, concerts and similar events. Photography must not, though, be allowed to upset the performance or smooth running of the event or affect the health and safety of pupils and others.

Parental photography must not include any child whose parent has refused consent for any reason. This may mean offering photography opportunities before or after the event to those who wish to be involved. Parental photography is secondary to the main aims and purposes of performances and must not be allowed to interfere with the opportunities for pupil participation.

Commercial copyright in a dramatic performance or musical will normally exclude any audio or video recording by the public (other than the school for internal purposes) and, in that event, parents and their guests must be informed that the infringement of copyright is strictly forbidden.