MAGDALEN COLLEGE SCHOOL

E SAFETY POLICY

Non-Statutory Policy – Annual Review

GOVERNORS' EDUCATION & WELFARE COMMITTEE

Date next due for review by committee	Reviewed by committee	Any Changes YES/NO	Approved by Full Governors
New	1 July 2014	Yes	9 September 2014
June 2015	26 Jan 2016	Yes	N/a
Jan 2017	24 Jan 2017	Yes	Approved by committee 24 Jan 2017
Jan 2018	16 Jan 2018	Yes	Approved by committee 16 Jan 2018
Jan 2019	19 Mar 2019	Updated in line with Keeping Children Save in Education (2018) & GDPR	Approved by committee 19 March 2019
Jan 2020	17 Mar 2020	Yes	Approved by committee 17 March 2020
Jan 2021	16 March 2021	Minor Update	Approved by committee 16 March 2021
	15 June 2021	Minor Update	Approved by committee 15 June 2021
June 2022	15 March 2022	Updated	Approved by committee 15 March 2022
March 2023			

MAGDALEN COLLEGE SCHOOL

E Safety Policy

Adopted from Northamptonshire County Council Local Safeguarding Children's Board

Policy Statement

ICT and the internet have become integral to teaching and learning within schools; providing children, young people and staff with opportunities to improve understanding, access online resources and communicate with the world all at the touch of a button. At present, the internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Social media
- Mobile Devices
- Online gaming
- Learning Platforms and Virtual Learning Environments
- Video Conferencing
- Blogs, Apps and Wikis
- Email, Instant Messaging and Chat Rooms

Whilst this technology has many benefits for our school community, we recognise that clear procedures for appropriate use and education for staff and students about online behaviours, age restrictions and potential risks is crucial.

All schools have a duty to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children, young people and staff continue to be protected.

Aims

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within, and outside of, the school environment.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To ensure Data Security is understood by all staff and procedures adhered to.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Scope of policy

This policy applies to all staff, students, governors, visitors and contractors accessing the internet or using technological devices on school premises. This use of mobile devices which are brought onto school grounds or use for school associated activity. This policy is also applicable where staff or individuals have been provided with school issued devices for use off-site, such as school laptop or work mobile phone. All users must ensure that they adhere to the principles of the General Data Protection Act 2018 (GDPR) when working with, sharing or storing personal information.

Definitions

Personal data

This is information which relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and students, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

Sensitive personal data

This is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.

The difference between processing personal data and sensitive personal data is that there are greater legal restrictions on the latter. We hold sensitive personal data in pupil and staff records so staff need to be aware of the extra care it requires.

Personal / Sensitive information must be:

1. Used fairly, lawfully and transparently
2. Used for specified, explicit purposes
3. Used in a way that is adequate, relevant and limited to only what is necessary accurate and, where necessary, kept up to date
4. Kept for no longer than is necessary
5. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Staff Responsibilities

Teaching and Support Staff (including volunteers)

All staff have a shared responsibility to ensure that children and young people are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all who work in schools are bound.

Please see Acceptable Use Policy for School Based Employees (appendix A) for further details regarding staff responsibilities and expectations for behaviour whilst accessing the internet, email or related technologies within and beyond school. A copy of this document is made available to all staff and shared with any volunteers, visitors or

contractors. Please see guidelines for use of social networking sites and setting permissions (Appendix C).

It is very important that all staff take the ultimate care when accessing, using and storing any personal and / or sensitive data relating to students / colleagues or the school. Staff must ensure that all personal and / or sensitive school data is stored on the school network where ever possible or suitable protection / encryption software is used to ensure that data remains secure. In the event of loss or theft, failure to safeguard the data by not protecting it as directed could result in a serious security breach, subsequent fine or prosecution by the Government Information Commissioners Office and may also result in a disciplinary offence. Staff are bound by the school's code of conduct and confidentiality policy and must ensure their actions do not breach the Data Protection Act 2018 / General Data Protection Regulations 2018. Password protection alone is not sufficient. All staff with school issued mobile devices will have them enabled with suitable encryption software and / or will be issued with an encryption memory stick if off line remote working is a necessity. Staff must not hold personal or sensitive data unnecessarily or for inappropriate lengths of time. Relevant personal information should be stored in the official files of the school including physical file and / or software files e.g. Sims/Go for Schools. Any unnecessary personal or sensitive information should be deleted regularly.

ICT Systems Network Manager/Technical Staff

The ICT Systems Network Manager and ICT Technicians are responsible for ensuring:

- that the school's ICT infrastructure is secure and not open to misuse or malicious attack.
- that anti-virus software is installed and maintained on all school machines and portable devices.
- that the school's web filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the E Safety Lead and the Designated Person for Safeguarding.
- that any problems or faults relating to web filtering are reported to Designated Person for Safeguarding and recorded on the e Safety Incident Log.
- that users may only access the school's network through a designated password. Passwords are regularly changed.
- that he/she keeps up to date with e safety technical information in order to maintain the security of the school network and safeguard children and young people.
- that the use of the school network is regularly monitored in order that any deliberate or accidental misuse can be reported to the E Safety Lead.
- Implement and oversee a rolling 13 month email deletion policy.

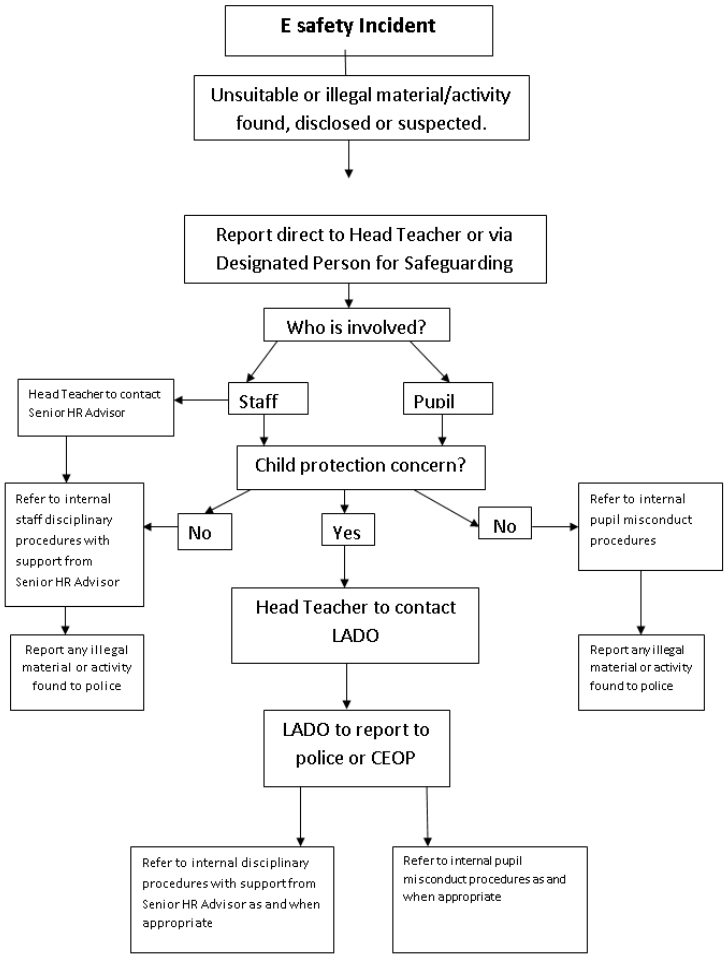
Children and Young People

Children and young people are responsible for:

- Signing agreement to, and abiding by, the Acceptable Use Rules for students (appendix B)
- Using the internet and technologies in a safe and responsible manner within school.
- Informing staff of any inappropriate materials, cyberbullying or contact from unknown sources (age dependent)
- Actively participating in the development and annual review of the Acceptable Use Rules.

Incident Reporting

In the event of misuse by staff or students, including use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Head teacher/Designated Safeguarding Lead immediately and the e Safety Incident Flowchart followed.



N.B. LADO is now referred to as DO (Designated Officer)

In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT should be reported immediately to the Head Teacher, Designated Safeguarding Lead and ICT Systems Network Manager

All incidents must be recorded on the E Safety Incident Log to allow for monitoring, auditing and identification of specific concerns or trends.

Monitoring

The school reserves the right to monitor all ICT use including web access and email use without prior consent of staff / students.

School ICT technical staff regularly monitor and record user activity, using Fortigate proxy servers on site including any personal use of the school ICT system (both within and outside of the school environment) and Impero classroom management software which records ICT access and use. Users are made aware of this in the Acceptable Use Policy.

Online Safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation, radicalisation, sexual predation – technology often provides the platform that facilitates harm. Magdalen College School regularly reviews the curriculum and procedures to ensure the student body is protected and educated in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three area of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views

- **Contact:** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults

- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying

Further details and links to Teaching Online Safety in School (DfE) are available in Keeping Children Safe in Education 2021, Annex C.

The Curriculum

The school strives to embed e Safety in all areas of the curriculum and key online safeguarding messages are reinforced wherever ICT is used in learning.

- A programme of skills and competencies are taught to ensure that students are able to explore how online technologies can be used effectively, but in a safe and responsible manner.
- Students are made aware of copyright issues, data protection, intellectual property and reliability of information sourced on the internet as part of the e Safety curriculum.
- Opportunities for informal discussions with students about online risks and strategies for protecting yourself online are built into our curriculum, to ensure that our students are armed with accurate information.
- Students, parents and staff are signposted to national and local organisations for further support and advice relating to e safety issues, including BeatBullying, Childline, SHARP and CEOP.
- Some faculties may wish to use social network feeds / media to send out revision topics / reminder messages and good news information. To ensure safe working practices are followed the safest option is to disable the ability for recipients to respond. Additional support and advice should be sought from the Media Co-ordinator.

Students with additional learning needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each student. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e Safety awareness sessions and internet access.

Email Use

Staff

- The school provides all staff with a professional email account to use for all school related business, including communications with children, parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Under no circumstances will staff members engage in any personal communications (i.e. via hotmail or yahoo accounts) with current students outside of authorised school systems.
- All emails should be professional in tone and checked carefully before sending, just as an official school letter would be.
- Staff should inform their line manager or the e Safety Lead if they receive an offensive or inappropriate email via the school system.
- The school operates a rolling 13 month email deletion policy. Staff are required to ensure any emails that need to be retained are required to be stored elsewhere prior to being 13 months old.

Students

- The school provides individual email accounts for students to use as part of their entitlement to understand different ways of communicating and using ICT to share and present information.
- Students will use their school issued email account for any school related communications, including homework or correspondence with teachers. Email content will be subject to monitoring and filtering for safeguarding purposes.
- Students are able to email staff (on their school email address) using their school email only and for school-related issues only.
- Students will be taught about email safety issues, such as the risk of exposing personal information, opening attachments from unknown sources and the management of inappropriate emails. Students will also be guided in the correct tone to use in email correspondence and regularly reminded of restrictions on abusive or inappropriate content.
- The forwarding of chain letters is strictly prohibited in school and should be reported to a member of staff immediately.

Both

- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the ICT Systems Network Manager. Account holders must never share their password with another user, or allow access to their email account without the express permission of the Head Teacher. It is recommended that email account holders change passwords at least once each term to maintain security. A forced password change will take place at least annually.

Managing remote access

For data security and safeguarding purposes it is crucial that staff are aware of the following restrictions on use when accessing the school network off site using remote access:

- Only equipment with the appropriate level of security should be used for remote access (i.e. encryption on any devices where sensitive and / or personal data is stored or accessed).
- Log-on IDs and PINs should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns).
- For security purposes, network access information should not be written down or stored with the device in case of theft or unauthorised access.

Internet Access and Age Appropriate Filtering

Internet Service Provider: Fluidone

All students are entitled to safe and secure internet access and schools have a duty to deliver this as part of the learning experience. The Head teacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate web filtering is in place to protect young users from inappropriate or harmful online content. To this end, the school has the following filtering measures in place:

- Web filtering levels are managed and monitored in school via an administration control tool currently Fortigate Proxy Server, which allows an authorised staff member to instantly allow or block access to a site or specific pages and manage user internet access.
- Age appropriate content filtering is in place across the school, ensuring that staff and students receive different levels of filtered internet access in line with user requirements (e.g. Youtube is accessed via Youtube education)
- All users have unique usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering. Class log-ins, dependent on age, may also be used.
- Any changes to filtering levels are carefully considered to ensure consistency of policy and student safety. Approved requests are recorded via email and retained.

In addition to the above, the following safeguards are also in place

- Anti-virus and anti-spyware software is used on all network and stand alone PCs of laptops and is updated on a regular basis.
- A firewall ensures that information about children and young people cannot be accessed by unauthorised users outside the school network.
- Encryption codes on wireless systems prevent hacking
- The CEOP Report Abuse button and SHARP reporting facility is available on the school website to allow students or staff to report online safeguarding issues.

Staff

- Expectations for staff online conduct is addressed in the Acceptable Use Policy for School based employees.
- Staff are expected to preview any websites before use, including those which are recommended to students and parents for homework support.

Use of School and Personal ICT Equipment

School ICT Equipment

- A log of all ICT equipment issued to staff, including serial numbers, is maintained by the ICT Systems Network Manager.
- Personal data is not stored on mobile school devices (e.g. laptops, tablets or USB Memory Sticks) without the relevant encryption software being installed.
- Photographs or videos of students, such as class photos or assembly evidence must not be stored on personal equipment.
- Time locking screensavers are available on all devices in school to prevent unauthorised access
- Personal ICT equipment, such as laptops or memory sticks would be subject to the same filtering and security processes whilst using the school's network.

Mobile Devices

Student use:

- Mobile devices are not permitted to be used on site at all, in years 7-11. All students should have mobile devices switched off before entering the school site and not switch them on again until they leave the site at the end of the day. The exception for this is students in the sixth form, who are permitted to use mobile devices within the TGC and Library only. Misuse of mobile devices (misuse includes using phones outside of the permitted boundaries) on school grounds will result in the device being confiscated.
- Sixth form students are permitted to use laptops and tablets during lessons for the purposes of their studies and must not use social networks, texts and other social communication during lessons.
- Parents/Carers are responsible for installing adequate filtering for use in conjunction with 3 and 4G mobile data services.
- If there is reason to suspect that a student's mobile device contains inappropriate, harmful or illegal content, the device will be confiscated and a search conducted by a senior member of staff in line with disciplinary powers awarded to staff in the Education Act 2011. Searches will be conducted in the presence of at least one other senior staff member and any actions/findings (including contacting the relevant authorities) recoded in the incident report log. Where evidence of illegal activity is discovered (e.g. indecent images of young people) the device will be locked in a secure area, parents will be notified and the police contacted immediately. *Please see E Safety Incident Flowchart on p.4.*

Staff use:

- Personal mobile devices are permitted on school grounds, but should be used during break and lunch times only and not during working hours.
- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.
- Personal mobile devices should not be used to contact students or their families without the prior consent of a member of SLT.
- Personal mobile devices should never be used to take videos or photographs of students. School-issued devices **only** should be used in these situations.
- School trips/visits – All trip leaders/organisers will be issued with a school mobile phone for use during off site visits and trips.

- Staff must ensure that all sensitive school data is stored on the network where-ever possible or suitable protection/encryption software is used.
- Personal tablet mobile devices are permitted on school grounds, but should be used during break and lunch times only and not during working hours unless specifically authorised by the Headteacher to do so.
- Staff are provided with laptops to allow for school related work to be completed off site. Personal use of the laptop from home (such as web browsing/online shopping etc.) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of staff only (i.e. not family members)
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.
- Staff will ensure that school laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.

Removable Media (Memory Sticks/USB)

- Sensitive or personal student data e.g. identifiable exam results or SEN data or sensitive or personal staff data must not be stored on mobile devices. If necessary an encrypted memory stick can be provided by the school.
- Any passwords used for memory sticks/or other devices will remain confidential to the user.

Photographs and Video

Digital photographs and videos are an important part of the learning experience for children and young people and, as such**,** schools have a responsibility to ensure that they not only educate students about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and young people about the use of digital imagery within school.

- Written consent will be obtained from parents or carers before photographs or videos of young people will be taken or used within the school environment, including the school website or associated marketing material.
- Permission will be sought from any student or staff member before an image or video is taken and the purpose of the activity and intended use of the image will be made clear.
- Staff are not permitted to use personal mobile devices to take photographs or videos of students.
- Where photographs of students are published or displayed (e.g. on the school website) first names only will be displayed. Best practice would be to use non-identifying captions (e.g. Year 9 pupil playing football)
- Wherever possible, group shots of students will be taken, as opposed to images of individuals and images should never show young people in a manner to cause embarrassment.

Video conferencing

- Permission is obtained from parents and carers prior to their child's involvement in video conferencing.

- All students are supervised by a member of staff when video conferencing, particularly when communicating with individuals or groups outside of the school environment (e.g. international schools)
- All video conferencing activities are time logged and dated with a list of participants.

Parent/Carer Involvement

As part of the schools commitment to developing e-safety awareness amongst children and young people, every effort is made to engage parents and carers in the process.

- All students and their parents/carers will receive a copy of the Acceptable Use Rules on first time entry to the school. Students and their parents/carers are both asked to read and sign acceptance of the rules, a copy of which will be stored at school.
- Wherever possible, and subject to prior arrangement, the school will endeavour to provide parents/carers without internet access the ability to research online safety materials and resources.
- Annual E Safety awareness training will be organised by the school for parents to attend.
- The school provides access to SIMs data via an online portal. Each parent / carer is issued with a username and password to access this service. These credentials must remain confidential and not be divulged to third parties.

‘School Name’ E Safety Incident Log

Details of ALL E-Safety incidents to be recorded by the E-Safety Lead. This incident log will be monitored termly by the Head teacher, Designated Person for Child Protection and E-safety governor.

Date of incident	Name of individual(s) involved	Device number/location	Details of incident	Actions and reasons	Confirmed by
1/10/10	Joe Bloggs	PC 63 Rm 4	Child accessed inappropriate chat site using child log-in. Adult language and pornographic images viewed.	Hector Protector launched effectively by young person. Synetrix help desk contacted. Website now blocked and filtering levels reviewed and altered.	Davey Jones (Deputy Head CPO)

Appendix A

Acceptable use policy for school based staff
Effective from September 2014

1. Policy Statement

In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within a school or educational setting. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate technological developments.

The purpose of the Acceptable Use Policy is to clearly identify for the whole school community:

I. the steps taken in school to ensure the safety of students when using the internet, email and related technologies.
II. the school's expectations for the behaviour of the whole school community whilst using the internet, e-mail and related technologies within and beyond school.
III. the school's expectations for the behaviour of staff when accessing and using data.

2. Scope of policy

The policy applies to Magdalen College School employees and volunteers. Visitors on site need to be made aware of the expectation that technologies and the internet are used safely and appropriately. The Acceptable Use Policy should be used in conjunction with the school's E Safety policy, disciplinary procedures and code of conduct policy applicable to staff and students. Where the policy is applied to the Head Teacher, the Chair of Governors will be responsible for its implementation.

3. Legal background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all school employees in relation to use of technologies feature within the following legislative documents which should be referred to for further information:

> The Children Act 2004, School Staffing (England) Regulations 2009, Working Together to Safeguard Children 2018, Education Act 2002, Safeguarding Vulnerable Groups Act 2009, Keeping Children Safe in Education 2018. All safeguarding responsibilities of schools and individuals referred to within this Acceptable Use Policy include, but is not restricted to the legislation listed above.

4. Responsibilities

Head Teacher and Governors

The Head teacher and Governors have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the Head Teacher and Governors will:

- Designate the Designated Safeguarding Lead as the lead of 'e-Safety' to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately. All employees, students and volunteers should be aware of who holds this post within school.
- Provide a safe, secure and appropriately filtered internet connection for staff, children and young people within the school.
- Provide resources and time for the e-Safety lead and employees to be trained and update protocols where appropriate.
- Promote e-safety across the curriculum and have an awareness of how this is being developed, linked with the school development plan.
- Ensure that any mobile equipment which holds sensitive or confidential information ***does not leave*** school premises (e.g. tablets, staff laptops, cameras and memory sticks) unless suitable protection / encryption software is in place. All information should be accessed via the school network and not held on the device, wherever possible.
- Share any e-safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to child protection.
- Ensure that e-safety is embedded within all child protection training, guidance and practices.
- Elect an e-Safety Governor to challenge the school about e-Safety issues.
- Make employees aware of the Local Safeguarding Children Board Northamptonshire (LSCBN) Inter-agency Child Protection Procedures at www.northamptonshirescb.org.uk

Designated Safeguarding Lead

The nominated Designated Safeguarding Lead will:

- Recognise the importance of e-Safety and understand the school's duty of care for the safety of their students and employees.
- Establish and maintain a safe ICT learning environment within the school.
- Ensure that all individuals in a position of trust who access technology with students understand how filtering levels operate and their purpose.
- With the support of the Deputy Safeguarding Leads, Network Manager and IT Faculty Leader, to ensure that filtering is set to the correct level for employees, young volunteers, children and young people accessing school equipment.
- Log issues of concern
- Liaise with the Deputy Safeguarding Leads, Business Director, Network Manager and ICT Faculty leads so that procedures are updated and communicated, and take into account any emerging e-safety issues and technological changes.
- Co-ordinate employee training according to new and emerging technologies so that the correct e-Safety information is being delivered.
- Co-ordinate the maintenance of an e-Safety Incident Log to be shared at agreed intervals with the Head Teacher and Governors at governing body meetings.

- With the support of the Deputy Safeguarding Leads, Business Director, Network Manager and ICT Faculty Lead, implement a system of monitoring employee and pupil use of school issued technologies and the internet where appropriate.

Individual Responsibilities

All school-based employees, including volunteers must:

- Take responsibility for their use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- Ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an e-Safety incident.
- Ensure that any sensitive / personal data is kept secure at all time. Off-site access to the school network is available via a secure remote desk top service to ensure data remains protected.
- Report any e-Safety incident, concern or misuse of technology to the Headteacher, including the unacceptable behaviour of other members of the school community.
- School issued email addresses and equipment should be used for school led business unless specific written permission to use a personal device has been granted by the Head Teacher, for example, due to equipment shortages.
- Ensure that all electronic communication with students, parents, carers, employees and others is compatible with their professional role and in line with school protocols. This includes email, school website and school social media feeds. Personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.
- Not publish or use or post in any public media environment any text, image, sound or video of individuals without the express agreement of the person / persons involved and not under any circumstances in which it could upset or offend any member of the whole school community or be incompatible with their professional role. Individuals working with children and young people must understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.
- Protect their passwords/personal logins and log-off the network, locking workstations when leaving computers unattended.
- Understand that network activity and online communications on school equipment (both within and outside of the school environment) may be monitored, including any personal use of the school network. Specific details of any monitoring activity in place, including its extent and the manner in which it is carried out, are detailed in the E Safety policy.
- Understand that employees, who ignore security advice or use email or the internet for inappropriate reasons risk dismissal and possible police involvement and / or prosecution by the Information commissioner's Government Office if appropriate.

5. Inappropriate Use

In the event of staff misuse, if an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Head teacher immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

Schools Senior HR Advisory Team, DO (Designated Officer), Police/CEOP (if appropriate)

Please refer to the e Safety Incident Flowchart on page 5 for further details.

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed only if appropriate.

Examples of inappropriate use

- Accepting or requesting pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.
- Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

In the event of accidental access to inappropriate materials, students are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action. Template student Acceptable Use Rules and example sanctions can be found in the Appendix B.

Students should recognise both the CEOP Report Abuse button (www.thinkuknow.co.uk) and SHARP Reporting System (http://www.thesharpsystem.com) as a place where they can make confidential reports about online abuse, sexual requests or other misuse which they feel cannot be shared with employees.

6. Policy Review

The Acceptable Use Policy will be updated to reflect any technological developments and changes to the school's ICT Infrastructure. Acceptable Use Rules for students should be consulted upon by the student body to ensure that all young people can understand and adhere to expectations for online behaviour.

7. Useful Links

NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking
NUT E-Safety: Protecting School Staff- Guidance for Members
http://www.teachers.org.uk/node/12516
UNISON- Guidance on Social Networking
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786

Appendix B

Acceptable use policy for students

ICT Acceptable Use Policy – Guidelines

The school has the responsibility of providing you with safe, reliable and useful ICT resources (network, internet, learning platform etc.) that will help you make the most of your learning opportunities. You have a right to use these resources, with this right however, come the following responsibilities:-

- I will read, understand and follow these guidelines; I will take responsibility for my own use of all ICT making sure that I use technology safely, responsibly and legally.

  This means:-

  - I will take personal responsibility for my own e-safety e.g. when online, I will not give out any personal details or arrange to meet someone without the permission of my parent, carer or teacher (further advice is available at http://www.thinkuknow.co.uk/)
  - I will use email, messaging, mobile apps and social networking responsibly and always will be polite and respectful. When operating school equipment I will only use software, email, messaging, mobile apps and social networking systems that are approved by the school. If I see an email, message or update that I do not feel comfortable with I will inform my teacher, parent or carer. I will never use ICT for bullying or harassing others or in a way that will damage the school's reputation.
  - I will not intentionally gain access to unsuitable or illegal websites e.g. pornography, sexism, racism, homophobia, encouraging violence and I will report, as soon as possible, accidental access to such sites. If I see website that I do not feel comfortable with I will inform my teacher, parent or carer
  - I will not set up a Virtual Private Network using the school's network nor access applications which draw unnecessary significant bandwidths of data with the potential to affect internet speed for other users
  - I will not download or install any software or files on school's ICT equipment (unless it is a requirement of on agreed course of study) or open emails or attachments from people that I do not know.
  - If I use a flash drive (USB memory stick) in school I will a run an anti-virus check on it before using with school equipment.
  - When I am browsing the web I will ask "Is it true?" I will not assume that information published on the web or written in an email is accurate or true.
  - I will ensure that photos, videos or audio recordings will only be taken with the permission of those present and that these will be stored on the school network and used for school purposes only and not be distributed outside the school network without the permission of the Head teacher.
  - I will not publish material which could damage the school or its reputation.
  - I will only access school computer equipment and applications using my own login and password, which I will keep secret.
  - I will not access files that are not my own (hacking) and understand that I may be breaking the law if I were to do so. (Computer Misuse Act 1990)

- I will ensure that my work is my own and is not copied. I understand that if I use someone else's work that I may be breaking the law. (Copyright, design and patents law). I will always include a reference to where I sourced the information. I will not copy other people's work and pass it off as my own (plagiarism).
- I accept that the school cannot offer any guarantee that any use of the school's wireless connection is in any way secure and that no privacy can be guaranteed
- I accept that use of the school's wireless network is entirely at my own risk and that the school accepts no responsibility for any loss of information that may arise from its use.
- I will use school ICT equipment with care and tell my teacher of any damage which occurs as soon as possible.
- I will think and then preview before I print.
- I will regularly review my files and delete them when no longer needed.
- I will only store school-related files and images on the school network.
- I will use the school's network resources responsibly
- I will only use school ICT equipment for school-related work
- I understand that the school may check my computer files, will monitor the internet sites that I visit and read my emails.
- Parents and carers are responsible for installing appropriate filtering for use in conjunction with 4G and 5G mobile data services.
- The school does not accept any responsibility for any personal items lost, damaged or stolen etc. Insurance for any device brought to school is the responsibility of parents and carers.

Failure to comply with these guidelines may result in sanctions being issued, including detention, channelling or exclusion, dependent upon the circumstances. The following specific consequences may also apply:-

- My computer account will be restricted for an agreed period of time.
- My parent or carer will be informed and my account will be restricted for an agreed period of time
- I will be asked to attend a meeting with my parent / carer and school staff to discuss what has happened
- My computer account will be suspended for an agreed period of time
- My computer account will be permanently closed and if applicable police and/or other agencies will be informed

Student Agreement:-

Name: _____ Class: _____

Student Signature: _____ Date: _____

Parent/Carer Agreement:

Parent/Carer Signature: _____ Date: _____

Appendix C

Using Social Networking Safely

A guide for professionals working with young people

Contents

1. Introduction

Social media sites are a great way of keeping in touch with family and friends, as well as making new contacts who may share the same interests as you, or be helpful in your professional development. The 'networking' aspect of social networking is one of the great benefits of these sites. However, as a professional who works with young people, you need to take extra care to ensure that you don't inadvertently make your personal information available to the young people that you work with, or their families. This could leave you open to false allegations, misinterpretation, or the possibility of cyberbullying.

This guide will help you to check that you have chosen appropriate settings on your social media account.

Think who you should add as friends

You'll obviously want to add family and friends to your social media profile, so that you can keep in touch and share what's happening. However, it's worth thinking carefully about who else you may want to add, and also who may request you as a friend.

Remember that by adding someone as a friend to your profile, you are allowing them access to the information you have on your profile. There are ways that you can restrict certain parts of your profile, e.g. posts, certain photo albums, but you are still giving contacts you add access to a lot of personal information about yourself, and can be copied and pasted or passed onto other people without your knowledge.

Adults working with young people are restricted from engaging in personal communications with students outside of their professional role. Therefore, it is never a good idea to add any young people that you come into contact with professionally, or any of their family or friends. In addition, you should refuse any requests to become friends with young people or their family members. This will help to protect you from any misunderstanding of your actions.

Keep a professional distance

It is inevitable that some of the young people that you work with, or their parents, may look you up from time to time online to find out a little bit more about you. If you use your full name and include a real profile picture of yourself, this can be quite easy to do and may give students or parents the opportunity to view more than you would wish on your profile or request you as a friend.

To avoid such difficulties, it is a good idea to use a nickname and/or a different profile picture (e.g. Cartoon character, sunset etc.). That way, when students or parents are searching for you, they will struggle to identify your profile from a list of possibilities. As long as friends and family know what name to search under, they will still be able to find you.

2. Suggested Social Media Privacy Settings

Employers are routinely checking social networking sites, so it is vital that every user actively reviews their Privacy Settings on a regular basis to ensure that their information is only shared with the intended people and your personal and professional reputation is protected.

Suggested Social Media Privacy Settings
It can be very hard to work out which Privacy Settings are best for you. What is recommended to keep yourself safe?

Part 1: Friends

You cannot choose your family, but you can choose your friends. Casual acquaintances are less likely to be careful with your information than close friends. Think carefully about who you accept as a friend on social media. It is not a competition to see who can have the most friends!

You see your colleagues every day at work; do they need to be friends on Social media too? That moment of anger may be seen by more people than you intended.

Teachers and other public figures run the risk of accounts being set up in their name. By friending these accounts you allow the fraudster to see things you thought were private. If you are invited to be the friend of someone whose account could be fraudulent, send them an email to their work email address (which is less likely to be hacked than webmail, Gmail or Yahoo) or telephone them (not text) and double check that the invitation is genuine. It could save you being embarrassed as a fraudster or mischief-maker gets access to your profile information.

Part 2: Privacy Settings

There are various scenarios that could occur if you don't take sufficient care over the use of your social networking profile. For example, if you don't set appropriate privacy settings, much of the information you post could be open to anyone else on the platform to see. Even if you are careful with privacy settings, it is still possible for people you are connected with to share your private content with a wider audience (i.e. tagging or commenting on posts and pictures – in both situations the content copies from your profile into theirs and can be viewed by their online friends).

Part 3: Inappropriate staff use of Social Media

You also need to be aware of bringing your workplace or your professional role into disrepute through inadvertently posting inappropriate comments about work on your profile. For instance, criticizing policy or fellow colleagues, young people or parents and could lead to misunderstandings or, in some cases, disciplinary action being taken against you.

Some examples of staff online difficulties are listed below:-

1 A young NQT recently posted a status update on Social media saying ***"OMG must stop ****ing about and get my maths boosters planned as I go to teach kids in about 20 mins"*** – to his great embarrassment, he discovered that his profile was not as secure as he believed when a parent printed off a copy of what was said and made a complaint to the Head.
2 A Teaching Assistant who claimed she was absent from work due to sickness on the last day of term, foolishly wrote a social media status updated later that day saying ***"Just off to the airport now, see you all in 2 weeks"*** The Teaching Assistant had used privacy settings to restrict her profile and had only accepted one trusted work colleague as a social media friend. Her colleague, who knew of her plans, comments on the status to say ***"Have a great time-you deserve it! I won't tell anyone"***. Unfortunately, the colleague had forgotten that she had previously added the Head Teacher as a friend, who now received a copy of the entire conversation, including the absent employees comments, on the newsfeed of her own Social media account.
3 A member of staff, using a private social media profile, engaged in a discussion with a friend about her terrible day at work. The staff member had added a small number of work colleagues as friends over the years and, as she lived locally, had also added some parents as contacts. When asked why her day was so horrible by her social media friend, she replied: ***"So sick of working with f***ing (Child's full name) – just because he's got dyslexia and can't string a sentence together doesn't mean he can get away with being a little s***!!!!!!"***. Both colleague and worried parent, who had viewed the conversation, made anonymous complaints to the Head Teacher and Chair of Governors.
4 An experienced teacher, and regular social media user with good privacy settings, was horrified to discover that a student in her class had seen a personal album of photos which she had uploaded of a holiday away with friends. Amongst the album were a number of drunken photos of the staff member, including some provocative gestures and images of her in swimwear. It was discovered that the student was in fact related to one of the staff member's friends and had been able to access the images by clicking on comments that his relative had made on the teacher's personal photos. Thankfully, none of the images had been copied and shared with other students or parents.

5
Appendix D

BRING YOUR OWN DEVICE POLICY
FOR STAFF AND PUPILS

Aims

The aims of this policy are to ensure that use of personal ICT equipment used in relation to school business meets the same standards of safeguarding of pupils, staff and the school as for school-owned equipment.

Scope of this policy

There are several situations where equipment which is not owned by the school is used in relation to school business:

- **a)** Staff using a device which is not owned by the school whilst at school for their work as an alternative to using school equipment.
- **b)** Staff using a device which is not owned by the school for personal use whilst on school premises
- **c)** Staff using a device not owned by the school whilst away from the premises in connection with their work
- **d)** Pupils using a device not owned by the school whilst on the premises or elsewhere in connection with their studies or otherwise
- **e)** Visitors using devices not belonging to school whilst visiting school
- **f)** Where this policy refers to “computer” this term is used generically to include smart phones, tablets, laptops and desk top computers.

Potential risks against which this policy mitigates

1. Bringing onto school premises unacceptable material or compromising personal privacy of staff
2. Compromising confidentiality in relation to school information outside of the school
3. Infecting school systems with electronic viruses and other similar threats
4. Claims by users against the school for loss or damage to personal devices whilst in use for school business and/or whilst on the school premises

Pupils’ use of their own devices

Only those pupils in the sixth form are permitted to use their own computers whilst in school and they must:

- **a)** have permission of their form tutor to use a computer or tablet in relation to their work
- **b)** only connect to the guest network whilst in school and never attempt to connect to other school networks or use the guest network whilst not on the premises
- **c)** ensure that their device has up to date (supported) operating systems and appropriate anti-virus software (approved by the school) installed to reduce risks of virus infection when connected to the guest network
- **d)** only use the device in lessons with the permission of the teacher, and only for the purposes of their work, or in the TGC during study periods or break times
- **e)** not use a device in any part of the school other than in e) above

f) not make any attempts to circumvent the school's network security at any time, including the setting-up of proxies and use of programmes to bypass security
g) accept responsibility for their own equipment and accept that the school will, in no circumstances, accept liability for any loss or damage to equipment not belonging to the school whilst on the premises or in use for school work.

Staff use of their own devices

For personal use

Staff are permitted to bring personal devices (eg mobile phone) into school for personal use and these may be used outside of paid hours or during PPA time (teaching staff), and should not be used whist in contact with pupils (staff should not use their personal devices, for example, around the site, but should confine this to a staff room or empty classroom, for example).

For use in connection with their work

All staff who are required to use a computer in connection with their work are provided with access to a suitable device by the school. In the event that a member of staff wishes to use their own device in connection with their work they may only do so with written consent of the headteacher, using the form in appendix Y. Permission will be granted when staff are able to confirm that:

a) there is a sound business reason for use of a computer other than that provided by the school
b) the device in question has up to date (supported) operating systems and anti-virus software (approved by the school) installed
c) the device is free from material which compromises the school's acceptable use policy
d) they give permission to the ICT technical staff to inspect the device to ensure that these safeguards are in place
e) it is connected to the school's guest network whilst in use for school business on the premises
f) no school information is stored on the device itself and storage of school information is cloud-based in the school's cloud storage accounts (ie it is not permissible to store school information in cloud storage owned by or subscribed to by the member of staff personally).
g) password protection is in place so as to protect school information whilst the device is in school and away from the premises. This includes, for example, the protection of passwords for school systems (eg Go4S) to prevent unauthorised access to these systems whilst the device is in and out of school.
h) the device is not used by anyone other than the member of staff or, when used by anyone other than the member of staff a different log in profile is used to prevent unauthorised access to school information and systems
i) not make any attempts to circumvent the school's network security at any time, including the setting-up of proxies and use of programmes to bypass security
j) accept responsibility for their own equipment and accept that the school will, in no circumstances, accept liability for any loss or damage to equipment not belonging to the school whilst on the premises or in use for school business

Visitors

Visitors, including governors, may use their personal devices in connection with work at Magdalen. The same protocols set out for staff apply.

Related policies
All stakeholders must view this policy in the context of the E-**S**afety **P**olicy, the **S**afeguarding and **C**hild **P**rotection **P**olicy and the Data Protection **P**olicy.

Appendix Y
Application for use of personal device by a member of staff in connection with school business

(Please note for multiple devices separate applications must be submitted).

Name of member of staff making the application	
Nature of device (laptop, phone, tablet)	
Make and model of device (eg ipad air 3)	
Serial number of device (usually found in the settings on the device)	
Nature of work the device will be used for	
Justification for use of the personal device in connection with school business	

I can confirm full compliance with the BYOD policy:	
a) there is a sound business reason for use of a computer other than that provided by the school	(tick all that apply)
b) the device in question has up to date (supported) operating systems and anti-virus software (approved by the school) installed	

c) the device is free from material which compromises the school's acceptable use policy	
d) I give permission to the ICT technical staff to inspect the device to ensure that these safeguards are in place	
e) it is connected to the school's guest network whilst in use for school business on the premises	
f) no school information is stored on the device itself and storage of school information is cloud-based in the school's cloud storage accounts (ie it is not permissible to store school information in cloud storage owned by or subscribed to by the member of staff personally).	
g) password protection is in place so as to protect school information whilst the device is in school and away from the premises. This includes, for example, the protection of passwords for school systems (eg Go4S) to prevent unauthorised access to these systems whilst the device is in and out of school.	
h) the device is not used by anyone other than the member of staff or, when used by anyone other than the member of staff a different log in profile is used to prevent unauthorised access to school information and systems	
i) I will comply fully with the school's acceptable use policy and, in particular, will not make any attempt to circumvent the school's security systems or set up proxies	
j) I take full responsibility for the device and will not claim against the school for any loss or damage incurred whilst the device is on the school's premises or in use for school business.	
Signature Date of request	
Headteacher decision Signature, date	
Date decision conveyed to member of staff	