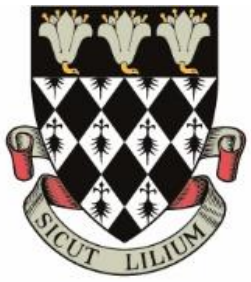

MAGDALEN
COLLEGE SCHOOL

FOUNDED IN 1480
BY WILLIAM OF WAYNFLETE

Computer Usage and Internet Access Policy - Pupils

Contents

Introduction and Scope

This Policy relates to the use and monitoring of all of the School's IT and communication systems, including all computers (whether physical or virtual, desktops, laptops, tablets or other computing devices), telephones, mobile telephones, e-readers, email, software applications, the school computer wired and wireless networks, remote connections to school systems and resources from off site, and Internet connection by School pupils.

The School provides the IT and communication systems for the purposes of the pupil's work and the use of these systems is subject to this Policy at all times. This policy also applies in cases where non-MCS devices are connected to any of the School's networks, systems or data. Breach of this Policy in a pupil's use of the School's IT and communication systems will be considered a disciplinary issue.

This Policy applies to all pupils who use the School's IT and communication systems. A short guide for parents on safe use of the Internet is attached as Appendix 1.

Relevant background

This policy is written having had regard to the following guidance and regulation:

- *Keeping Children Safe in Education (KCSIE)* (Revised September 2024)
- *Working Together to Safeguard Children* (Updated July 2022)
- *Independent Schools Standards Regulations* (April 2015)
- *The Education (Independent School Standards) Regulations* (January 2015)
- *Prevent Duty Guidance for England and Wales* (Revised September 2023)
- *The use of social media for online radicalisation* (July 2015)

Principles of Expected Online Behaviour

As a member of the school community you should follow these principles in all your online activities:

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.

- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues.)
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Email

1. Email correspondence is not private. Emails can be easily intercepted, copied, forwarded and stored without the original sender's knowledge. Pupils must take into account the fact that any email they send may be read by a person other than their intended recipient.

2. Any attachments which contain important or confidential material should be treated in the same manner as the email in terms of security and privacy.

3. A record of emails sent and received by pupils is kept. Emails sent and received by pupils can be opened by IT Services under the direction of the Master, Usher or other senior member of staff. This includes messages which were deleted from the email Inbox.

4. All email messages and attached files are automatically scanned for viruses and other forms of malware before being introduced into the network, but this does not provide a complete guarantee of protection. Therefore, it is recommended that pupils are extremely careful when opening emails and attachments to emails from unknown sources. It is equally important that caution must be exercised when clicking links in emails. Do not click a link unless you have checked that it links to a suitable location, for example by hovering the mouse pointer over the link before clicking. If pupils have any doubts about opening an email or attachment, they should speak to a teacher or member of IT Services.

5. A school email address may be used as proof of attendance at the school and in some cases used to obtain goods or services at beneficial terms. Contracts can be entered into by email in the same way as they are by letter or on the telephone. Pupils must at all times take care to ensure that they do not inadvertently enter into contracts which bind the School by email, and they should be aware that contracts must only be entered into in accordance with the normal procedures and subject to the standard terms and conditions of such agreements.

6. Pupils must not under any circumstances send messages or attachments whether within the School or outside the School, to individuals or Internet web-sites, which are:

    a. Abusive, obscene or pornographic, including the use of foul language,

    b. malicious,

    c. discriminatory in any sense for example concerning sex, sexual orientation, age, race, religion, gender or disability,

    d. defamatory about any other person or organisation,

    e. bullying or intimidating in content.

7. If pupils receive any such messages from outside the School they must report them to their tutor or housemaster or a member of IT Services and must not forward them either within or outside the School.

8. Accessing, storing, displaying or sending emails of the type described above is likely to be treated as a disciplinary offence and will be treated accordingly. You should be aware that written derogatory remarks, even when made in jest, could constitute libel or discrimination for which pupils and/or the School could be sued.

9. Access to School email using email programs on mobile devices is granted subject to acceptance that in the event of loss of the device the school may remotely wipe the device to remove data.

Other Online Communication Media

1. Using other electronic communication media, whether that involves text, pictures, or audio/video transmission, for example in Microsoft Teams, Zoom, Firefly, OneNote, is subject to the same rules as email communication, when using your School credentials for access. This applies whether at school or off site and from any device.

Internet

1. The School has put technical measures in place to prevent access to any Internet web site which contains sexual, illegal or other inappropriate content. It is extremely unlikely that a pupil would need to access a site which contains such content for the purposes of their studies, but in these circumstances he/she must obtain the express permission of the School (in the first instance via his/her tutor/housemaster) in advance. Internet access is monitored as well as blocked and pupils found to be intentionally attempting to access inappropriate sites will be in breach of this Policy.

2. Pupils are ultimately responsible for any access from their computer to Internet sites containing inappropriate material. The ability to access Internet sites through the school security systems does not imply that access is allowed by the School to any such sites.

3. The use of proxies, virtual private networks (VPN), anonymisers and other methods to obfuscate the sites being visited and content accessed is strictly forbidden while on the School network and use of such is likely to be treated as a disciplinary offence.

4. VPN use from devices off the school network, e.g. at home, is forbidden *while logged in to the school's cloud systems on the device being used*, including Office 365. Access to our online systems is monitored and connections to school resources, including cloud resources, from unusual IP addresses will be reported. In cases flagged as being a likely result of password breach and account takeover, your School Office 365 account may be blocked resulting in loss of access to School resources including the portal, files and email. If this occurs you will need to contact IT Services to remove the block and discuss.

5. Much of the information that appears on the Internet is protected by copyright. Unauthorised copying or modifying of copyright-protected material, including software, breaches copyright law and is not permitted as it may make the pupil and/or the School liable to legal action.

Confidentiality

1. Pupils must not use the School's IT and communications systems whether alone or in conjunction with any other device to make an unauthorised disclosure or copy of confidential information belonging to or held by the School.

2. The unauthorised disclosure or copying of information belonging to the School is likely to be treated as a disciplinary offence and could give rise to disciplinary action.

3. Such confidential information shall include without limitation details of staff contact information, pupil contact information, personal data, reports, examination results etc., which are not otherwise available via public channels of communication such as the school website.

Monitoring and Data Protection

1. In order to protect the interests of the School and to maintain the effectiveness, integrity and security of the School's networks, the School may monitor and intercept any and all computer use, including email communications and Internet use by pupils.

2. In order to prevent cyberbullying the school has in place a system to monitor what is typed on computer keyboards and to identify pupils who are typing language in breach of other sections of this Policy.

3. The following automatic procedures are undertaken routinely or from time to time:

    - automatic checking for viruses and other malicious software of emails, email attachments, copied files and downloaded content;
    - automatic measures in place to prevent software from being downloaded to, installed on or deleted from the School's computers by pupils;
    - automatic blocking and recording of attempted access to certain files and pages on the Internet;
    - blocking the connection of unauthorised devices to the School's networks;
    - monitoring of files downloaded onto the School computers and electronic devices.

4. Human monitoring of the content of emails, Internet use or telephone calls is not routinely carried out by any member of staff but may be carried out in some situations. For example:

    - where the School has reasonable grounds to believe that a pupil is breaching this or any other policy of the School;
    - for the purpose of assisting in the investigation of wrongful acts;
    - to comply with any legal obligations;

- for the purpose of defending or prosecuting any legal action brought against the School.

5. Pupils should not expect their personal use of the School's IT and communication systems to remain private.

6. The holding, processing and disclosure of personal data in electronic form is regulated by the provisions of data protection legislation. Personal information relating to a living individual who can be identified from that information should not be sent by email or otherwise distributed outside the School unless proper checks have been made to ensure that this will not involve any breach of that legislation.

7. Pupils must also comply with the School's Data Protection Policy.

Security

1. Pupil access to the School's IT and communication systems is subject to satisfactory security checks being carried out in the reasonable discretion of the School.

2. Pupils must keep their user account password secret and not tell it to anyone.

3. Pupils must ensure their passwords are changed promptly when they are informed that their password is about to expire.

4. Pupils must not give their school badge / smartcard to any other pupil.

5. Lost school badges must be reported to tutors, IT Services or Reception as soon as possible. Anyone finding a badge must hand it in at Reception.

6. In cases where two factor authentication (2FA) is required, pupils must ensure the device running the 2FA app, such as a mobile phone, is suitably secured via password, PIN or biometric ID and not shared with any other person.

7. Pupils must not log on using somebody else's account, even with that person's permission, unless expressly asked to do so by a member of staff.

8. Pupils are responsible for any activity taking place on a computer on which their user account is currently logged in. Pupils must never leave themselves logged in and thus allow someone else to use that computer, even unknowingly. If they will be away from the computer for any significant length of time they must either lock the computer or log off.

9. If pupils are provided with, or bring in their own portable computer, mobile phone, personal organiser and/or any related or similar equipment, they must ensure its security at all times. They must in particular

    a. never leave computer equipment including discs, USB storage devices, CDs and DVDs in an unattended vehicle, or unattended in public.

    b. always lock mobile equipment when not in use so that it cannot be used without entering their logon ID in order to prevent unauthorised users using it in their absence.

    c. keep their passwords and PIN numbers confidential (and the IT system will force pupils to change them regularly.)

    d. lock the device if they leave a device unattended so that it cannot be used without entering their logon ID. Never leave such items unattended in public places.

10. If any equipment described above is lost or stolen pupils must report the incident to their tutor/housemaster immediately. The incident will be fully investigated, and may be treated as a disciplinary issue if a pupil has failed to take adequate steps to safeguard the security of equipment in their possession.

11. Pupils must not attempt to gain access to any part of the network to which they are not permitted access.

12. Pupils must not disconnect any cables from or connect any cables to the network data ports without express permission to do so from IT Services.

Computer and other equipment not provided by the School

1. Pupils must not connect or attempt to connect any device to the network without authority from IT Services and they should be aware that the School has in place automatic measures to prevent this. Authority will be implicitly granted if pupils are able to connect their device to the wireless network.

2. Pupils connecting their own devices to the school networks must accept and be bound by any further policies which will be presented electronically via the device on connection to the network.

3. Pupils will only be able to connect personal devices to the school wireless network if they have suitable security measures installed, including but not limited to anti-virus

software, time-activated automatic device lock, and they must allow installation of necessary software to such devices as required by IT Services.

4. A breach of the prohibition contained on connecting devices to the School's network is likely to be treated as a disciplinary offence and will be treated accordingly.

Personal Use

1. A very limited amount of personal use of the School's systems by pupils is permitted subject to the following rules:

    a. School work must always take priority over any personal use of the School's systems.

    b. Any personal use must not delay or interfere with the proper performance or usage by another pupil or a member of staff.

    c. Sending personal emails from the School network and email systems should be kept to a reasonable minimum. All personal email messages must make it clear that they are sent in a personal capacity and not on behalf of the School.

    d. Personal emails sent through the school's email system should be deleted within a short time of being read or sent.

    e. Pupils may not use the School's systems to transfer, store or download information and files for their personal use including but not limited to MP3 files and other audio or video file formats unless those files are made available via School streaming systems such as Planet eStream.

2. If a pupil's personal use exceeds an acceptable level in the reasonable opinion of the School (in the first instance via their teacher) or if a pupil does not comply with these rules their access to the system may be curtailed and they may be subject to disciplinary action.

3. Use of the School's IT and communication systems is granted for the time a pupil is enrolled at the School. Once no longer at the School, access to non-public school systems will be removed and no further access may be assumed.

Consequences of a Breach of this Policy

1. Breach of this Policy in a pupil's use of the School's IT and communication systems will be considered a serious disciplinary matter and will be dealt with accordingly.

Examples of offences which may be considered to be serious and resulting in a severe punishment are:

a. excessive visiting of non-School related Internet sites during normal lessons and study periods.

b. Introducing a virus or other malicious software to the computer system by inserting a disk, USB storage device, CD or DVD into a School computer without running a virus check, via email or from downloading an Internet file.

c. Misuse of the computer system which results in any claim being made against the School.

d. Accessing pornography or any other illegal material including, but not limited to, material relating to terrorism or gambling or sexist or racist material on the Internet and/or circulating such material.

e. Unauthorised copying or modifying of copyright material.

f. Unauthorised downloading of software or files.

g. The connection of an unauthorised device to the network.

h. Use of the Internet for criminal activity.

In less serious cases pupils may have access to the Internet removed or other disciplinary action taken against them.

Appendix 1: Safe use of Internet guidelines for parents

General Guidelines

The Internet is a valuable resource that can raise educational standards by offering pupils opportunities to search for information from a very wide range of sources based throughout the world. Unfortunately, not everyone who uses the Internet is honest or trustworthy. Some of the information to be found on the Internet may be inappropriate for pupils. Because of these concerns, we have several different technologies in place to help protect pupils including firewalls, filters and security scanning software. We expect pupils to follow the rules whenever they are online in school. The pupils are responsible for good behaviour on the Internet just as they are in all other aspects of life at school. The code of conduct applies at all times, in and out of school hours, whilst using school equipment.

One of pupils' responsibilities is to report immediately to a teacher or parents anything happening through the Internet that gives cause for concern.

Social Media

An ever-growing number of web sites and services are categorised under the heading Social Media. These include Facebook, Twitter, Instagram, WhatsApp, YouTube, Snapchat and many more. They generally offer a way of sharing facts, opinions, media content with people over the Internet and typically have an element of communication with unknown people.

Social media services have much to offer that is of benefit in educating young people. However, due to the anonymous nature of their communication and the often lax content restrictions there are also dangers and pitfalls to be aware of. Some sites have become used for more questionable practices than others. Parents should consider to what degree they are happy with their children using individual social media services on the Internet. There is much helpful information and advice available for this fast-moving field on the Internet aimed at parents and children. One example being www.childnet.com.

Internet Fora, Boards and Chatrooms

Many Internet sites are available, via apps or accessed by pages on the World Wide Web, providing a messaging, image sharing or communication service similar to the most commonly known social media platforms. They are set up so that several users can read and post contributions concurrently. They often do not have a clear educational objective and little to no moderation on what is posted and available to see. As these services are often not censored,

and because of the anonymous nature of the communication, there is concern that such platforms may be used to exert undue influence over young people. Therefore, it is recommended that pupils are not permitted to access them **unless supervised**.

Use of Email

Email is an extremely powerful communication tool. Pupils will benefit by being able to communicate with other people around the world in connection with their studies. The School provides all pupils with their own email accounts. Pupils should be aware that any message sent using their school email accounts bears the School's email address and is equivalent to sending a letter on school headed notepaper. We expect a high standard of literacy and accuracy in communications - especially when the pupils are contacting people outside the School. A Spell Checker is installed as part of the email software used at School to help with this.

Surfing the Internet at Home

To help to keep pupils safe online, it is always recommended that parents should turn the parental control on and most ISPs offer this function when you sign up with them.

Reviewed:	December 2024
By:	Director of IT
Next Review:	December 2025