Magdalen College School, Oxford ("the School")

Policy – Computer Usage and Internet Access - Pupils

Introduction and Scope

1. 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, facsimile machines, email, software applications, the school computer wired and wireless networks and Internet connection by School pupils.

2. The School provides the IT and communication systems for the purposes of the pupils' work and the use of these systems is subject to this Policy at all times. Breach of this Policy in a pupil's use of the School's IT and communication systems will be considered a disciplinary issue.

3. 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

Email

4. 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 the intended recipient.

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

6. A record of school emails sent and received by pupils is kept. School 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 pupil's email Inbox.

7. All email messages and attached files are automatically scanned for viruses 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 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 member of IT Services.

8. 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.

9. Pupils must not send emails to groups or lists of recipients, be they pupils, staff or persons connected with the school, unless there is a valid reason for doing so related directly to their schoolwork.

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

    a. Abusive, pornographic or obscene, 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.

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.

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.

11. 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.

Internet

12. The School has put technical measures in place to prevent access to any Internet website 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.

13. 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.

14. The use of proxies, virtual private networks, anonymisers and other methods to obfuscate the sites being visited and content accessed is strictly forbidden and use of such is likely to be treated as a disciplinary offence.

15. 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

16. 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.

17. 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.

18. 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

19. 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.

20. 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 section 10 of this Policy.

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

    a. automatic checking for viruses of emails, email attachments, copied files and downloaded content.
    b. automatic measures in place to prevent software from being downloaded to, installed on or deleted from the School's computers by pupils.
    c. automatic blocking of and recording access to certain files and pages on the Internet
    d. blocking the connection of unauthorised devices to the network
    e. monitoring of files downloaded onto the School computers and electronic devices.

22. 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:

    a. where the School has reasonable grounds to believe that a pupil is breaching this or any other policy of the School;
    b. for the purpose of assisting in the investigation of wrongful acts;
    c. to comply with any legal obligations;
    d. for the purpose of defending or prosecuting any legal action brought against the School.

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

24. 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 unless proper checks have been made to ensure that this will not involve any breach of that legislation.

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

Security

26. 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.

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

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

29. 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.

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

31. If pupils bring a portable computer, mobile phone, personal music player, organiser and/or any related or similar equipment onto School premises, they must ensure its security at all times. They must in particular

    a. never leave computer equipment including discs, CDs, USB storage devices 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

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 changing rooms or other public places. Pupils should lock such items in lockers or hand them to appropriate staff members.

32. If any equipment described above is lost or stolen, pupils must immediately report the incident to their tutor/housemaster. 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.

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

34. 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

35. Pupils must not connect or attempt to connect any personal device to the wired network without express authority from a member of IT Services and they should be aware that the School has in place automatic measures to prevent this.

36. 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.

37. 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, and pupils must allow installation of necessary software to such devices as required by IT Services.

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

Personal Use

39. A very limited amount of personal use by pupils of the School's systems 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 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 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 similar file formats.

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.

Consequences of a Breach of this Policy

40. 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 to the computer system by inserting a disk, CD or DVD, USB storage device 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 the pupil.

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, Wordpress, 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 Chatrooms

Chatrooms are usually accessed by pages on the World Wide Web and often do not have a clear educational objective. They are set up so that several users can read and post contributions concurrently. These Chatrooms are not censored, and because of the anonymous nature of the communication, there is concern that Chatrooms 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 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.