Marden High School

Acceptable Use Policy

Ratified by Governors: 28 September 2021

To be reviewed by Governors: September 2022

Introduction

The purpose of these Acceptable Use Policy documents are to ensure that all users (including, but not limited to Employees, Students, Visitors, Contractors) using Marden High School's computing facilities are aware of school policies relating to their use.

The Internet and computer usage has now become an important part of every individual's life. The use of ICT (Information and Communications Technology) in schools and at home has increased rapidly and is now embedded within schools and education. ICT has given the opportunity for everyone to research quickly, communicate across the world instantly and made global information available locally.

Within Marden High School, we have embraced and invested in ICT over a number of years and this has enabled us to use new technology and systems such as G Suite for Education (including Google Docs). These allow us to work independently and collaborate anywhere, in real time, allowing ICT to become part of effective learning, and preparing our students for the future.

The computing resources within Marden High School are provided to facilitate work and education for users, specifically for educational, training, administrative or research purposes. The regulations that constitute this policy seek to provide for the mutual protection of the school and the rights of its users.

Effective and proper use of information technology is fundamental to the successful and efficient running of the school. However, misuse of information technology – in particular misuse of e-mail, internet and social media – exposes the school to liability and is a drain on time and money.

It is the responsibility of all users of the school ICT facilities to be aware of, and follow school ICT policies and guidelines and to seek advice in case of doubt.

Marden High School Student ICT Acceptable Use Policy

I know that I must use the computers safely

- I know that the school can remotely monitor what I do on the computers.
- I will treat my username and password like my toothbrush – I will not let anyone else use it, and I will not use theirs.
- I will be aware of my personal safety when I am communicating online, and will not share personal information about myself or others.
- If I arrange to meet someone that I have communicated with online, I will do so in a public place and take a responsible adult with me.
- I will tell a teacher immediately about any unpleasant or inappropriate material or messages on the computer, or anything that makes me feel uncomfortable when I see it.
- I understand that the school will look after me and my classmates and can help with advice if anything happens online.

I know that I must use the computers responsibly

- I understand that the computers are here for school work, and I will only play games on them or use them for personal use if I have permission.
- I will only upload pictures or videos from inside the school if I have permission.
- I understand that the school's security and Internet filter is there to protect me, and protect the computer network, and I will not try to bypass it. If I need access to a blocked website, I will ask my teacher.
- I will only download or use music or videos if it is related to my school work.
- I understand that I must not download or display inappropriate pictures or other material from the Internet.

I know that I must help look after the computers

- If I have a problem with my computer, I will tell a teacher immediately so that the problem can be fixed – I won't leave it broken for the next person or attempt to fix it myself.
- I will only use programs that are already on the school computer. If I need a new program, I will ask my teacher - I won't try to install it myself.
- I only try to connect my own computer or mobile device to the Marden-BYOD Wireless network, and only use it in a lesson if I have been given permission. At all other times, my mobile device will be in my bag.
- I will only change settings on the computer if I am allowed to do so – I won't try to change anything that might cause the computer to go wrong.
- I know that food and drink is not allowed in the computer rooms, and that I should not eat or drink around any computer.

I know that I must respect others when using the computers

- I will always treat others the same way I would want them to treat me – just as I would when not using the computers. I will not use the computers to harass or bully anyone.
- I will be polite online, and I will not use strong, aggressive, or inappropriate language. I appreciate that others may have different opinions.
- I will not take or distribute pictures or videos of anyone without their permission.

Marden High School Bring Your Own Device (BYOD) Acceptable Use Policy

This Bring Your Own Device (BYOD) policy applies to all users of the school's Marden-BYOD or Marden-Visitor WiFi.

Mobile devices are a part of modern life and we believe they offer excellent educational opportunities. As with all technology, there are risks involved. Marden High School embraces the use of technology, but within the boundaries set out in this policy.

In this policy, we will use the term device, but this means any electrical equipment that can perform one or more of the following functions:

- Access the Internet
- Take photographs
- Communicate with other devices
- Access a mobile phone network
- Make video or voice recordings

These can include, but are not limited to laptops, Chromebooks, mobile phones, MP3 players, tablet computers and any other similar devices. This policy covers the use and liability for all devices carried or used within Marden High School and on the school grounds.

Marden High School takes no responsibility for the security, safety, damage, theft, insurance and ownership of any device used within the School premises or on the School grounds that is not the property of the School. We will investigate theft but not loss. If a device is stolen or damaged while on School premises, it is to be reported to reception immediately, in order that the incident can be logged and investigated as appropriate. Marden High School's insurance does not cover personal devices whilst on the premises, or during travel to and from the School.

Use of personal BYOD devices is at the discretion of the School and should not be seen as a right. Students' own devices can be used in the classroom at the teacher's discretion for research or for learning. At all other times, these devices should be kept in a bag, and not used while moving around school. Devices are not permitted in an exam or an exam room and if students are found with such a device during an exam, it will result in action being taken in accordance with JCQ regulations. Staff should show a good example to students and not use their own devices unless it is part of a lesson.

All BYOD devices shall only contact the Internet using Marden High School's Guest Wireless (Marden-BYOD or Marden-Visitor). All internet access via the network is logged. The use of mobile data (e.g. GPRS, EDGE, 3G, 4G, etc) to access the Internet in School by students is strictly prohibited. All access must be by the School wireless network which is appropriately filtered.

The use of cameras and recording equipment, including those which may be built in to certain devices, to make images or sound recordings of individuals, is prohibited unless with prior permission of any individual(s) being photographed/recorded. The publishing of these images or recordings must be with the strict permission of the individuals in the recording, and in accordance with any laws or parental agreements.

Marden High School does not require students to install any apps onto their personal devices. Any Internet access, apps or updates that may be used or downloaded onto any device whilst using the School's wireless network is undertaken at the owner's risk, with the School having no liability for any consequent loss of data or damage to the individual's device.

We encourage users to protect their own devices e.g. with the use of password or PIN as appropriate. Users are responsible for the use of their own device(s) while on the School site.

Personal devices should not be used in a manner that would portray Marden High School in an unfavourable light.

Devices should not be used to intimidate, abuse or perform any unfavourable acts against, staff, students or any person associated with Marden High School.

Any costs/fees incurred while using devices are not chargeable against Marden High School and are the sole responsibility of the owner.

When on the School site and switched on, all devices must be set to silent.

Charging of personal devices of any kind may not be used in School. Any chargers owned by the school have been PAT tested according to the Health and Safety Executive's advice.

Marden High School Staff ICT Acceptable Use Policy

Guidelines for Staff

The school has provided computers for use by staff as an important tool for teaching, learning, and administration of the school. Use of school computers, by both members of staff and pupils, is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the Director of ICT in the first instance.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the school's computer system may result in disciplinary action (including possible termination), and civil and/or criminal liability.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, the school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the school neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the school.

Computer Security and Data Protection

- You will be provided with personal accounts for accessing the computer system, SIMS and www.mardenhigh.net, with your own usernames and passwords. This account will be tailored to the level of access you require, and is for your use only. As such, **you must not disclose your password to anyone**, including IT support staff. If you do so, you will be required to change your password immediately.
- You **must not allow a pupil to have individual use of a staff account** under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, you **must** ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.
- You **must not** store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by the school.
- You **must not** transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the school.
- When publishing or transmitting non-sensitive material outside of the school, you **must** take steps to protect the identity of any pupil whose parents have requested this.
- If you use a personal computer at home for work purposes, you **must** ensure that any school-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.
- You **must** make your own backup of data kept on any storage system other than the network storage drives or your 'My Documents' folder. This includes USB memory sticks (even those owned or issued by the school) or a personal computer.
- You **must** ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Equipment taken off-site is not routinely insured by the school. If you take any school computer equipment off-site, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.
- If you are accessing email, SIMS or any other sensitive information, your projector should either be 'frozen' or switched off to ensure this information cannot easily be seen by staff, visitors or students in or near your classroom

Personal Use

The school recognises that occasional personal use of the school's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use

- **must** comply with all other conditions of this AUP as they apply to non-personal use, and all other school policies regarding staff conduct;
- **must not** interfere in any way with your other duties or those of any other member of staff;

- **must not** have any undue effect on the performance of the computer system; and
- **must not** be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and **must not** be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
- You **must not** connect personal computer equipment to school computer equipment without prior approval from IT Support staff, with the exception of storage devices such as USB memory sticks.
- If you keep files on a personal storage device (such as a USB memory stick), you **must** ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation of harmful software onto the school computer system.
- Marden High School takes no responsibility for the security, safety, damage, theft, insurance and ownership of any device used within the School premises or on the School grounds that is not the property of the School. We will investigate theft but not loss. If a device is stolen or damaged while on School premises, it is to be reported to reception immediately, in order that the incident can be logged and investigated as appropriate. Marden High School's insurance does not cover personal devices whilst on the premises, or during travel to and from the School.

Conduct

- You **must** at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
    - Making slurs or jokes related to Age, Disability, Gender reassignment, Marriage and civil partnership, Pregnancy and maternity, Race, Religion and Belief, Sex or Sexual orientation.
- You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You **must** not intentionally damage, disable, or otherwise harm the operation of computers.
- You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive downloading of material from the Internet;
    - Excessive storage of unnecessary files on the network storage areas;
    - Use of computer printers to produce class sets of materials, instead of using the print room.
- You should avoid eating or drinking around computer equipment.

Use of Social Networking websites and online forums

Staff must take care when using social networking websites such as Facebook or Twitter, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You **must not** allow students to link to your personal social media accounts. In addition you must not link to any students social media accounts.
- You **must** ensure that personal information is not accessible via a 'Public' setting.
- You should avoid contacting any pupil privately via a social networking website, even for school-related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.
- Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.
- Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school or that may damage the school's reputation.

- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

Use of Email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the school. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You **must not** purchase goods or services on behalf of the school via e-mail without proper authorisation.
- All school e-mail you send should have a signature containing your name, job title and the name of the school.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Supervision of Pupil Use

- Pupils **must** be supervised at **all** times when using school computer equipment. When arranging use of computer facilities for pupils, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff **must** ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Privacy

- Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the school does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.
- You should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).
- The school may also use measures to audit use of computer systems for performance and diagnostic purposes.
- **Use of the school computer system indicates your consent to the above described monitoring taking place.**

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the school, as well as other staff or pupils.
- You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- You **must** consult a member of IT Support staff before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.
- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting

or relating to the business of the School or capable of being used or adapted for use within the School shall be immediately disclosed to the School and shall to the extent permitted by law belong to and be the absolute property of the School.

- By storing or creating any personal documents or files on the school computer system, you grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

Reporting Problems with the Computer System

It is the job of the IT Support team to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of IT support staff as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone or in person so that they can be acted on immediately; any other problem can be reported via an email to it.support@mardenhigh.net, in person or via telephone.
- If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of IT Support staff **immediately**.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You **must** immediately inform a member of the IT Support staff, or the Head Teacher, of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within school that you feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

Reports should be made either via email to IT.Support@mardenhigh.net, via telephone, or in person. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

1. "Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data. This list is not exhaustive. Further information can be found in the school's Data Protection Policy.