# Great Marlow School

***Excellence • Compassion • Integrity***

# ICT Acceptable Use Policy – All Students

| | |
|---|---|
| Recommended by the Leadership Team: | Dec 2024 |
| Approved by Governors' Policies Sub Committee: | Dec 2024 |
| Ratified by Governing Body/Board: | Dec 2024 |
| Review Due: | Autumn Term 2025 |

Indicate as appropriate:

There **has not been** a change to the previous policy.

# Information Systems Policy

The information systems policy covers the use of ICT systems to support learning, the use of telephones, email and the internet by students, and the use of online tools provided by Great Marlow School. This policy consists of four sections:

**1. Acceptable use of ICT equipment**

**2. Email and internet**

**3. Social Networking, Social Media and email: Protecting your Reputation when using online resources**

**4. Safe use of online resources**

## 1. Acceptable use of ICT equipment Principles

Great Marlow School is committed to safeguarding its ICT infrastructure to ensure it can be used in the most effective manner to support teaching and learning processes. Ensuring the safety and integrity of the school's ICT infrastructure is the responsibility of all students.

Great Marlow School encourages students to fully use the ICT infrastructure and to make use of portable ICT equipment offsite to support them in their work. Great Marlow School encourages this use in a responsible and professional manner. Portable computers include for example laptops, tablets and other portable ICT devices.

As a student of ICT services of Great Marlow School you have a right to use its computing services; that right places responsibilities on you as a student which are outlined below.

Ignorance of this policy and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Students are advised of this policy during their induction to school and are required to sign the ICT Acceptable Use Policy each time they logon to a school computer.

For the purposes of this policy the term "computing services" refers to any ICT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the Internet). Students who connect their own ICT to the School's network and the services available are particularly reminded that such use requires compliance to this policy.

## Purposes

- To protect the school's networks and equipment
- To protect the school's data
- To protect Great Marlow School and its students from activities that might expose them to legal action from other parties

## Guidelines Password security

Access to all systems and services is controlled by a central computing account. Students are allocated their Student ID's and password credentials when joining the Academy.

Issuance and continued use of your Student Account is conditional on your compliance with this policy. Student passwords are not to be shared or revealed to anyone. Those who use another person's student credentials and those who share such credentials with others will be in breach of this policy.

Initial default passwords issued to any student should be changed immediately following notification of account set up. Passwords should be changed immediately by notifying the IT Department if the student believes or suspects that their account has been compromised.

## General Conditions

In general, use of Great Marlow School "computing services" should be for your studies.

- Your use of the school's computing services must at all times comply with the law.
- Your use of the school's computing services must not interfere with any others' use of these facilities and services.
- You must not use your school email account to register to personnel or none educational services of any kind without the permission of the IT Manager and senior leadership team.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program, App or data which has not been specifically authorised for your use.
- You must not use any applications that bypass the schools firewall and/or web filtering safeguards. These have been put in place for your protection. This includes applications installed on personnel devices.
- You must not use or copy any data or program belonging to other students without their express and specific permission.
- You must not alter computer material belonging to another student without the students' permission.
- You must not use Great Marlow School's computing services or any social media platforms to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use Great Marlow School's computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such.
- You must not use the school's computing services to conduct any form of commercial activity without express permission.
- You must not use the school's computing services to disseminate mass (unsolicited) mailings.
- You must not use any IRC or messenger software including, but not limited to AOL, MSN, Yahoo! or other "Messengers", IRC or "chat" clients unless expressly authorized to do so for work related purposes
- You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the school's facilities.
- You must not use any form of network monitoring which will intercept data
- You must not play computer games of any nature whether preinstalled with the operating system or available online

## Data Security

Where possible students are encouraged to use the schools various online services to access data, shares, home drives instead of using removable drives. There are multiple ways to access files and resources both in and out of school to help with this process.

There are a variety of methods of remote access to systems available (Office 365, Email, Teams and Foldr) which allow you to work on data in-situ rather than taking it outside the Academy, and these should always be used in preference to taking data off-site.

The ICT Department offers a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them for advice.

### Anti-Virus and Firewall Security

All computers are installed with current versions of virus protection and firewall software by the ICT Department. Students are not to alter the configuration of this software unless express permission has been obtained from the ICT Department. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

Students must ensure that they are running with adequate and up-to-date anti-virus software on their personal devices at all times. If any student suspects viral infection on their machine, they should disconnect the device (or shut it down) and inform the ICT Department immediately. If the ICT Department detects a machine behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe.

## Physical Security

The students' use of ICT equipment should always adhere to the following guidelines:

- The ICT Acceptable Use Policy (displayed on every PC upon login)
- Treat equipment safely, in the same manner as a reasonable person would
- Keep liquids away from ICT equipment
- Do not place heavy objects on ICT equipment
- Do not drop ICT equipment or objects onto it
- Any portable computer must be securely locked away when not in use
- Portable computer security is your responsibility at all times and must be kept up to date
- Do not leave the portable computer unattended in a public place or within the academy
- Do not leave the portable computer on view outside school. It should be locked away out of sight.

## Remote Access

Remote access to Great Marlow School network is possible where this has been granted by the ICT Department.

Remote connections are considered direct connections to Great Marlow School network and remote services. As such, generally accessing services remotely, subjects the student to the same conditions, requirements and responsibilities of this policy.

All connection attempts are logged.

## Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.

Such records and information are sometimes required - under law - by external agencies and authorities. Great Marlow School will comply with such requests when formally submitted.

## Breaches of This Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of student related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a student may contravene this policy but in general such breaches will be dealt with using Great Marlow School's Disciplinary Policy and Procedure.

In the event a Portable Computer is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the academy.

## 2. Use of Email and Internet

The provisions of this Policy apply to all students.

### Purposes

To provide guidance on inappropriate use of Great Marlow School email and internet facilities. To clarify when that Great Marlow School may monitor usage of these facilities.

### Guidelines

### Use of email

E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication. Students email service should only be used for school purposes. Any requirement to use email outside your educational needs must be approved by the IT department and/or Leadership team.

Students should be careful that before they open any attachment, or link to an e-mail they receive, they are reasonably confident that the content is in no sense obscene or defamatory to avoid contravening the law. Equally, if a student receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, unless specifically requested to do so by an investigator appointed by the academy. All suspicious emails must be reported to the IT department for investigation so the Great Marlow School can safeguard itself from further attacks.

Any other use of e-mail for either personal or Great Marlow School purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under Great Marlow School's Disciplinary Policy and Procedure.

Where Great Marlow School has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.

The Great Marlow School also reserves the right to access a student's e-mail account.

### Use of Office 365/Teams

When students are working on a computer in school or at home on a Microsoft Teams lesson:

- I will behave appropriately at all times abiding by the school's Behaviour for Learning Policy
- I will only use my own school email address and login details
- I will not tell other people my passwords
- I will not give out any personal details via Microsoft Teams
- I will make sure that all computer related contact with other students and adults is appropriate
- I will not deliberately look for, save or send anything that could offend or upset others
- If I accidentally find anything inappropriate on the internet, I will tell my teacher or a trusted adult immediately
- I will be responsible for my behaviour when using computers in school or at home because I know that these rules are to keep me and others safe
- I will not record any part of the lesson unless specifically directed to by a member of staff
- I will be dressed appropriately, and I will have everything I need for the lesson ready
- I will tell a trusted adult if I am contacted by someone, I do not know
- I know that my use of Microsoft 365 applications can be checked and that my parent or carer will be contacted if a member of school staff is concerned about my safety or my conduct while online

- I understand that further inappropriate behaviour on Microsoft Teams will result in my access to Microsoft Teams being limited or removed completely

### Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources. However, it is legitimate for students to make use of the Internet in its various forms during break times as long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.

Unauthorised use of the Internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be dealt with under the school's Behaviour for Learning Policy and the sanctions will be in line with those indicated in the policy. Great Marlow School reserves the right to audit the use of the Internet from particular Personal Computers or accounts where it suspects misuse of the facility.

### Use of the WiFi network

The primary reason for the provision of WiFi access is for the easy retrieval of information for educational purposes, or to make use of learning resources. However, it is legitimate for students to make use of the WiFi network for educational purposes as long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.

Unauthorised use of the WiFi, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. Under no circumstances are applications to be used to bypass the academies firewall and web filtering safeguards.

Great Marlow School reserves the right to audit the use of the WiFi from particular personal phones or internet enabled devices through the identity of the IP address where it suspects misuse of the facility.

### Monitoring the use of e-mail, WiFi and the Internet.

It is not the school's policy, as a matter of routine, to monitor students use of the school's e-mail service, WiFi or of the Internet via the school's networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the school may grant permission for the auditing of a student's telephone calls e-mail or the Internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Leadership team. These staff are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Leadership team or to advise the appropriate line manager/head of department of the actions that may need to be taken in any particular case.

## 3. Social Networking, Social Media and Email: Protecting your Reputation

Your reputation and conduct is part of your current development and future career, therefore managing your online reputation is essential. Anything you post online or send by email is potentially public and permanent, even if you subsequently delete posts and emails and if you use privacy settings.

### Principles

### Be Responsible and Respectful at all Times

• You must be conscious at all times and not post anything you may later regret.

• You must not engage in activities involving social media which might bring yourself or Great Marlow School into disrepute.

• Always assume Images and media uploaded to social media will be permanent.

• You must not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations or Great Marlow School.

## 4. Safe use of online resources

### Password Policy

Students must assume personal responsibility for their usernames and passwords. Never use anyone else's username or password.

You must always keep your individual student name and password confidential. These student usernames and passwords should never be disclosed to anyone. Passwords and student names should never be shared.

In some instances students may be given the right to change passwords from the one originally issued. If you wish to change your password for any reason please contact the IT department.

5. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour for Learning policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policies and agreements (individual agreements) for Students, Staff and Visitors.

Great Marlow School

Bobmore Lane
Marlow
Bucks
SL7 1JE
Tel: 01628 483752
Fax: 01628 475852
info@gms.bucks.sch.uk
www.gms.bucks.sch.uk

**HEADTEACHER:** Mr K Ford
**DEPUTY HEADTEACHERS**
Mr G Pendlebury
Mr N Maguire

# ICT Acceptable Use Agreement: Students 2024/2025

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own student name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address when communicating with teachers.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not browse, download, upload, create, store, display or distribute any material that could be considered offensive, illegal or discriminatory. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is approved by my teacher and my parent/carer.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Headteacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring it into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me and others safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature …….. Date ……

Full Name …….. (Printed) Year / Form Group ……