MANCHESTER ISLAMIC GRAMMAR SCHOOL FOR GIRLS

FAITH • LEARNING • LIFE

Acceptable Computer Use Policy
March 2023

Document Control

This policy has been approved for operation within:	**Manchester Islamic Grammar School for Girls**
Date of last review:	10/03/2023
Date of next review:	March 2026
Review period:	3 years
Policy status:	Statutory
Owner	MIGSG

Scope of this Policy

This policy applies to all members of the School community who have access to the School's IT systems, including staff, students, volunteers, parents and visitors.

In this policy **'staff'** includes teaching and non-teaching staff, Trustees and regular volunteers. **'Parents'** includes students' carers. **'Visitors'** includes anyone else who comes to the School, including occasional volunteers.

The policy applies to all use of the School's computer systems, including access to those systems using personal devices, and all use of computers (including personal devices) on school property or in connection with school activities, both inside and outside of school.

What is an Acceptable Use Policy?

Help us to help you keep safe.

An Acceptable Use Policy is about ensuring that you, as a member of the MIGSG community can use the internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities e.g. equipment, printers and consumables, Internet and email, virtual learning environments and websites.

An Acceptable Use Policy also seeks to ensure that you are not knowingly subject to **identity theft** and therefore fraud. In addition, that you **avoid cyber-bullying** and just as importantly, you **do not become a victim of abuse**. As part of this, the School has banned certain proxy sites as well as anonymous proxy sites, because they put the school network at risk.

MIGSG recognises the importance of ICT in education and the needs of students to access the computing facilities available within the School. The School aims to make the ICT facilities it has available for students to use for their studies both in and out of lesson times. To allow for this MIGSG requires all students to sign a copy of the Acceptable Usage Policy before they receive their username and password.

Listed below are the terms of this agreement. All students at MIGSG are expected to use the ICT facilities in accordance with these terms. Violation of the terms outlined in this document may lead to loss of access and/or disciplinary action, which will be taken in accordance with the Behaviour Policy of the School.

School Equipment

Vandalism

Vandalism in the context of this policy is defined as **any action** that harms or damages any equipment or data that is part of the School's ICT facilities. This includes, but is not limited to:

- Deliberate damage to computer hardware such as monitors, base units, printers, keyboards, mice or other hardware;
- Change to or removal of software;
- Unauthorised configuration changes;
- Creation or uploading of computer viruses;
- Deliberate deletion of files.

Such actions reduce the availability and reliability of computer equipment and put other users' data at risk. In addition, these actions lead to an increase in repairs of the ICT facilities, which impacts upon every student's ability to use the ICT facilities, and incur costs which reduce the funds available to improve the School's ICT facilities. Parents/Carers will be billed for any vandalised equipment.

Use of removable Storage Media

MIGSG accepts the fact that you may wish to transfer school work done at home to school using a flash memory device. However MIGSG cannot guarantee that your work will be able to be transferred properly using these.

Printers and Consumables

Printers are provided in the library for use by students. You must use the printers sparingly and for educational purposes only. Take the time to check the layout and proof read your work using the 'Print Preview' facility before printing.

All printer use is recorded and monitored and therefore if you deliberately use the printer for non-education or offensive material you will be subject to the behaviour management measures of the School which, depending on the circumastances, include the following:

- Warning/Demerit
- Parental contact
- Loss of access to email, internet and/or print facilities
- Report to the Trustees
- Report to appropriate external agencies such as the Police

Internet

Content Filtering

Through our Internet service provider, MIGSG provides internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you come across any inappropriate website or

content whilst using the ICT equipment, **you must report it to a member of the ICT department immediately.**

Online behaviour

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

- Ensure that your online communications, and any content you share online, are respectful of others.
- All posts on Google Classroom must be appropriate in their tone and content.
- 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).
- Respect the privacy of others. Do not share photos, videos, contact details or other information about members of the school community without their permission, even if the content is not shared publicly.
- 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. Any illegal activity may be reported to the police.
- Staff must only use their School account when communicating with students electronically. Likewise, students must not communicate with staff using personal email or social media accounts.
- Do not access Internet Chat sites. Remember you could be placing yourself at risk.
- Never give or enter your personal information on a website, especially your home address, your mobile number or passwords.
- Do not access online gaming sites. Remember that your use of the Internet is for educational purposes only.
- Do not download or install software from the Internet; this is considered to be vandalism of the School's ICT facilities.
- Do not use the Internet to order goods or services from on-line, e-commerce or auction sites.
- Do not subscribe to any newsletter, catalogue or other form of correspondence via the Internet.

Using the School's IT systems

Whenever you use the School's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password.
- Do not share your school username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems.
- Do not attempt to access parts of the system which you do not have permission to access, or look for vulnerabilities in the systems.
- Do not attempt to install or run your own software on, or otherwise alter, school IT systems.

- Do not vandalise the School's IT systems. Vandalism includes not only physical damage, but also destroying files created by others, and any action which disrupts the normal operation of the systems (e.g. connecting private devices to TV screens without permission).
- You should take care regarding the contents and validity of all emails you receive.
- You must never open hyperlinks in emails or any attachments to emails unless you know and trust the sender, and are confident that the email is genuine.
- Remember that the IT systems are there to enable educational, school-related activities.

Remember that the School monitors use of its systems, and can view content accessed or sent via its systems.

On occasion, students may reasonably be required to make available for inspection personal devices and the contents of privately owned online accounts, including smartphone apps.

Loss arising from system faults

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the school will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, miss-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the School's ICT system is at your own risk. MIGSG specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

Network monitoring

For reasons of safeguarding and wellbeing MIGSG uses monitoring software across the computer networks. This software checks all computer activity and searches for keywords and phrases that could be used for grooming or other activity that may put children at risk. This software checks all document types that are opened within school.

Compliance with related school policies

You must ensure that you comply with the School's E-Safety Policy, along with all other school policies.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. Serious misconduct could lead to permanent exclusion or dismissal. In addition, a deliberate breach may result in the School restricting your access to school IT systems.

If you become aware of a breach of this policy or the E-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online, you should report it to the Designated Safeguarding Lead.