ICT Acceptable Usage Policy

This policy must be read and implemented in conjunction with the Data Protection policy and privacy notices.

Internet usage

Acceptable uses

As a general principle, internet access is provided to staff and volunteers to support work related activities. The following list is not intended to be a definitive list but sets out broad areas of use that the organisation.
considers to be acceptable uses of the internet:

- To provide communication within the organisation via email or the organisation website
- To provide communication with other organisations for educational purposes
- To distribute details regarding organisation meetings
- To provide electronic methods of communication
- Any other use that directly supports work related functions.

Unacceptable uses

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Use for racial, sexual, homophobic or other harassment.
- Use of non-educational games.
- To access pornographic, obscene or illegal material.
- To solicit personal information with the intent of using such information to cause harm.
- Entering into a commitment on behalf of the organisation (unless you have explicit permission to do this).
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Publishing defamatory and/or knowingly false material about the organisation, your colleagues and/or our young people on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.

- Revealing confidential information about the organisation in a personal online posting, upload or transmission - including financial information and information relating to our young people, staff and/or internal discussions
- Use of personal email to communicate with or about any OMG students
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of malicious software into the corporate network
- To disrupt the work of other users. This includes the propagation of computer viruses and use of the internet.
- Use of any Bit torrent systems
- Use for personal or private business purposes.

Email

- Whenever e-mail is sent, it should be from an official work email address which includes the sender's name, job title and organisation's name
- Every user is responsible for all mail originating from their e-mail address
- Forgery or attempted forgery of electronic mail is prohibited.
- Attempts to read, delete, copy or modify the e-mail of other users are prohibited.
- Attempts to send junk mail and chain letters are prohibited.
- If you receive e-mail from outside the organisation that you consider to be offensive or harassing, speak to your line manager (harassing internal e-mail will be dealt with under the organisation's guidelines).
- You should be aware that, in the event of the organisation being involved in legal proceedings, any relevant e-mails (including internal e-mail) may have to be disclosed, on the same basis as is the case for written documents.
- Email should be accessed via organisation ICT equipment only, if you wish to use a personal device to download organisation emails, you must get written approval from your line manager first. You will need to ensure that your device is secured by a password at all times, that this password is not shared with any other person and that all reasonable care is taken to prevent unauthorised access to confidential information.
- If you share any personally identifiable data you must ensure this is in line with the GDPR policy and privacy notices. If you use an email attachment all files must be password protected
- If you access email on a personal mobile device, tablet or laptop you must make sure that the device has an appropriate password to prevent non-authorised staff from accessing your company data
- If you log in to your email on a shared computer such as a bookable laptop or at an internet café it is your responsibility to make sure that you are logged out of your email before leaving the computer unattended
- You must close your email and log out if you leave your desktop computer or other device unattended.
- Do not save your email password to any device or browser (even if prompted)
- Do not share your email password with anyone
- If you want to send an all staff email it needs to be authorised by a senior manager

Network systems

- Do not log on to anyone else's account, access their files / emails, or destroy, copy, alter or move anyone else's files
- Only access your own folder on the network or other file service
- Do not change any access rights to folders on computers or network areas
- Always ensure you log out of all network systems and do not 'save password' to devices when prompted
- Do not leave any student or staff personal data in shared areas of the network

Local Computer Storage

- Files that you are working on should be removed from shared laptop (desktop, documents, downloads) folders before handing them back to the IT department as there is a risk that the next user of the device will have access to these files
- Files should also not be saved or left on non-OMG computers such as at an internet café it is your responsibility to delete these files after use
- Storing files on your OMG work computer (desktop, documents) folder is not advised as these

files are not backed up and not always password protected. You are advised to move important files to your shared area on the network drive or to back up your files using a USB Key or external hard disk

- All devices used to save personally identifiable data such as laptops, tablets, cameras, memory sticks or other removable hard drives must be password protected. Any personally identifiable information must be removed or deleted from shared devices before they are returned

IGNITE/OMG HRM/Google Workspace or any other third-party software

- Please ensure you are using your individual login to use these systems
- Always log out of all systems after use, especially on shared devices
- Do not save password to any device or browser (even if prompted)
- Do not leave your computer on with access to system that contain company data. Leaving the room with these system logged in could lead to students having access to email and MIS data.

Google workspace

- IT Department Admin will set up a firstname.lastname@omgeducation.co.uk, Google login to use Google Workspace
- You must only invite other staff to documents using their work email address
- When inviting staff, you must ensure that you use the setting that requires login access (do not use the "anyone with the link can access" setting)
- Consider whether you can use "view only" if staff do not need to edit
- Please ensure you are using your individual login to use these systems
- Always log out of all systems after use, especially on shared devices
- Do not save password to any device or browser (even if prompted)
- Do not leave your computer on with access to system that contain company data. Leaving the room with these systems logged in could lead to students having access to email and MIS data.

ID Cards

- ID Cards must be worn by staff and students at all times
- If you have forgotten your ID Card, please request a temporary pass from the Operations Manager
- All visitors and contractors must have their visitor passes on display at all times
- Students that consistently 'forget' or do not wear their ID Cards will be sent home to retrieve it or must pay £3 for a new set

Scanning / Storing of Personal Information

- When scanning personal documents to OMG scanned area, please ensure you DELETE all files after moving them to your private computer / secure area.
- Do not store personal files and information in the 'Student Shared Area or Shared Drive' as this is accessible by the learners in certain areas
- Staff are provided with their own secure shared area, please ensure the correct staff members have access or are revoked access should their job roles change.

Managers

- It is your duty to report when a staff member leaves so that we can remove their access to company IT systems
- Please let us know in advance the date that they will be leaving and the system that they were using
- Also make us aware of new staff starting so that we can ensure that they have had an IT induction