ICT ACCEPTABLE USE POLICY

August 2021

INTRODUCTION

MGTS provides access to computing and IT resources to help learners and staff with their studies and work.

Staff, learners and visitors at MGTS have access to various computing and IT resources. The majority of these resources have access to the Internet and the World Wide Web (web). The Internet and web can be considered to be the greatest informational resource ever produced by mankind but it can also be an un-regulated, un-governed environment which contains materials that would be considered to be illegal in the UK, plus content that the management team consider unsuitable for staff, learners and visitors engaged in work and study at MGTS.

Access to the MGTS computing and IT resources is a privilege. If a user violates the Acceptable Use Policy (AUP) the user may have their access rights limited or withdrawn, be subject to disciplinary action, or even criminal proceedings in the most severe cases.

If any learner does not understand any elements of the following policy they should discuss them with the Operations Manager. Should any learner inadvertently breach the terms and conditions of this policy, they should inform the Operations Manager as soon as possible.

GENERAL PRINCIPLES

Computing and IT resources at MGTS must be used in a manner which is ethical, legal and appropriate to MGTS' aims and goals. Users of computing and IT resources, which are shared resources, should use facilities in such a way as to encourage a scholarly atmosphere and must not obstruct the work of others. Each user has a responsibility to learn how to use the resources appropriately and responsibly. MGTS encourages the use and exploration of its IT resources but discourages behaviour which may inconvenience or harm other users and data.

Learners must not engage in any activity which is illegal, offensive or likely to have negative repercussions for MGTS and must not upload, download, use, retain, distribute or disseminate any images, text, materials or software:

RESPONSIBILITY

Individual users are responsible for their own actions, and are thus liable for any consequences thereof. MGTS cannot accept responsibility for ensuring that actions of users are acceptable. Whilst we will take steps to monitor use of facilities, we cannot police them absolutely. In all cases the user, or users,

concerned will be considered liable for their actions.

SECURITY

MGTS will endeavour to take reasonable care to ensure that users' data is safe and secure, however this is done in good faith, and no responsibility can be taken for any loss or damage howsoever caused. Facilities are provided "as-is" without any warranty or guarantee of suitability for any purpose, implied or otherwise.

ENFORCEMENT

In the event of a known or suspected breach of policy, MGTS may take immediate action to ensure both the security and accessibility of its computing and IT resources. Breaches of the Acceptable Use Policy will be dealt with according to their severity.

ACCEPTABLE USE POLICY - Computing and IT Facilities

When using MGTS computing and IT facilities users MUST NOT:

- Alter the settings of the computer
- Allow other people to use your account
- Give their password to someone else to use, and/or disclose their password to someone else, and/or be otherwise careless with their password (N.B. personal passwords should be changed regularly)
- Disrupt the work of other people
- Corrupt or destroy other peoples' data
- Violate the privacy of other people
- Offend, harass or bully other people
- Waste staff effort or resources
- Store files not related to their study or work at MGTS on MGTS computing resources
- Engage in software piracy (including infringement of software licences or copyright provisions)
- Generate messages which appear to originate with someone else, or otherwise attempting to impersonate someone else
- Physically damage or otherwise interfere with computing facilities, including attaching any un-approved hardware to MGTS computers
- Waste computing resources by playing games or using software which is not needed for your studies or work
- Engage in any activity which is rude, offensive or illegal
- Use the MGTS IT facilities to draw people into terrorism and/or extremism
- Download and/or run programs or other executable software from the Internet or knowingly introduce viruses or other harmful programmes or files
- Enable unauthorised third party access to the system
- Use the IT facilities of MGTS for commercial gain without the explicit permission of the appropriate authority
- Engage in any activity that denies service to other people or brings the name of MGTS into disrepute

When using MGTS computing facilities users MAY:

- Join a public forum (e.g. Social networking site, news group, etc) if this is a specific requirement of their course or work
- Only attach headphones and external memory drives to MGTS computers
- Alter computer settings to improve accessibility in a manner which has been previously agreed with the IT support, and the original settings are restored after use.

When using MGTS computing facilities users MUST:

- Log out of your account if you are leaving a computer for an extended period of time, or otherwise lock the screen if you leave the keyboard and computer
- Take appropriate actions to physically secure equipment issued to you for the purposes of study or work

MONITORING

Learner internet usage is monitored on a daily basis. All websites are recorded and logged by individual user, website and duration.

BREACHES OF POLICY

Incidents, which are deemed to be in contravention of this policy, will be assessed for their severity and as a result may lead to formal disciplinary action. In extreme circumstances, the police may be called. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

The list below provides examples of potential ways in which a user may contravene this policy. This list is not exclusive or exhaustive and there may be other matters of a similar nature, which would be considered as a breach of this policy. The consequences of the breach will depend on the level of severity:

- Playing computer games
- Sending nuisance (non-offensive) email
- Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area
- Assisting or encouraging unauthorised access
- Sending abusive, harassing, offensive or intimidating email
- Maligning, defaming, slandering or libelling another person
- Misuse of software or software licence infringement
- Interference with workstation or computer configuration
- Theft, vandalism or wilful damage of/to IT facilities, services and resources
- Forging email. i.e. masquerading as another person
- Loading, viewing, storing or distributing pornographic or other offensive material
- Unauthorised copying, storage or distribution of software
- Any action, whilst using MGTS computers deemed likely to bring MGTS into disrepute Attempting unauthorised access to a remote system
- Attempting to jeopardise, damage circumvent or destroy IT systems security at MGTS
- Attempting to modify, damage or destroy another authorised users data
- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities
- Attempting to use MGTS IT facilities, systems and resources to draw people into acts of terrorism or extremism or promoting terrorism/extremism.

Upon receipt of a reported suspected breach of policy, an investigation will be carried out, in confidence, and the findings will be considered in accordance with MGTS' Disciplinary Policy and Procedures. For learners, this will be considered under the learner disciplinary procedures.

LEGAL CONFORMITY

Some of the UK legislation applicable to computer use is listed below. This is by no means an exhaustive list and users are reminded of their responsibility to be aware of their legal obligations.

- Obscene Publications Act 1959
- Sex Discrimination Act 1995
- Race Relations Act 1976
- Protection of Children Act 1978
- Data Protection Act 1984
- Telecommunications Act 1984
- Interception of Communications Act 1985
- Copyright, Designs, Patents Act 1988
- Computer Misuse Act 1990
- Criminal Justice and Public Order Act 1994
- Defamation Act 1996
- Disability Discrimination Act 1998
- Data Protection Act 1998
- Human Rights Act 1999
- Regulation of Investigatory Powers Act 2000
- Malicious Communications Act 1988
- Counter-Terrorism and Security Act 2015

David Bridgens
Chief Executive

Reviewed: August 2021	**Next Review:** August 2022