BS.2.10.a INFORMATION SECURITY POLICY

March 2025

1 INTRODUCTION

MGTS provides access to computing and IT resources to help learners and staff with their studies and work. The purpose of this policy is to define clear rules for the use of information systems and other information assets at Midland Group Training Services Limited (MGTS).

Information security is the protection of information against accidental or malicious disclosure, modification, or destruction.
Information is an important, asset of MGTS which must be managed with care and all information has a value to MGTS and our competitors or criminal actors.
Access controls are put in place to protect information by controlling who has the right to use different information resources and by guarding against unauthorised use. Formal procedures must control how access to information is granted and how such access is changed.
This policy also mandates a standard for the creation of strong passwords and their protection.

2 DEFINTION, PURPOSE, SCOPE AND RISKS

Definition

Access control rules and procedures are required to regulate who can access MGTS's information resources or systems and the associated access privileges. This policy always applies and should be adhered to whenever accessing MGTS's information in any format, and on any device.

Purpose

The purpose of this policy is to prevent unauthorised access to MGTS's information systems. The policy describes the registration and de-registration process for all MGTS information systems and services.
These policies apply especially to new starters, leavers and those moving roles or responsibilities.

Scope

This policy applies to all information, information systems, networks, applications, locations, and users of MGTS or supplied under contract to it. This includes hardware such as laptops, PC's and mobile devices.

Risks

There is a risk that MGTS's information may be disclosed or accessed prematurely, accidentally, or unlawfully. Individuals or companies, without the correct authorisation and clearance, may intentionally or accidentally gain unauthorised access to MGTS's information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of MGTS and may result in financial and/or reputational loss and an inability to provide necessary services to our customers.

3 PHYSICAL ACCESS

Physical Access is every individual's responsibility for any device they are issued or use to access MGTS's systems.
Individuals are to:

- Ensure that the location of device(s) issued to them are always known.
- Ensure they follow the mandatory password access controls for devices in MGTS.
- Prevent access to any MGTS device or device accessing MGTS's data from any person not authorized by MGTS to access the device and data.
- When they are not using the device, they must ensure that the device is locked and any display screen or any other access port available via the device must be made secure from unauthorized viewing or access prior to leaving the device.
- Devices may not be left unattended in the office at any time when there is no MGTS employee present.
- Devices that are to be left in the office for an extended period or overnight must be shut down to enforce password protection and secured in a locked drawer.
- Access to physical network devices within the MGTS office is restricted.
- Access to the network room is controlled by authorised staff who use a controlled key process to maintain security.
- Any suspected or known unauthorized access to a device must be reported immediately to the MGTS person responsible for IT.

4 PHYSICAL ACCESS TO BUILDINGS

- Physical Access to the MGTS's office is limited to staff or authorised visitors. Access is controlled by a coded padlock on the door.
- All visitors and staff are required to register on the Secure Access Management System (SAM) on entering and exiting the premises.
- Visitor access beyond the reception area to the MGTS training facilities is supervised by a member of MGTS staff and access beyond the inner doors is controlled by a coded padlock.
- On termination of employment the HR Director will immediately instruct Zenzero to terminate pass credentials.
- Any keys issued must be returned to the HR Director on termination of employment.
- Cleaning staff are permitted access to the training centre for cleaning only.

5 PASSWORDS

Choosing Passwords

- Passwords are the first line of defence for our IT systems and together with the user ID helps to establish that people are who they claim to be.

- A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our information, computers and systems.

Defining ‘weak’ and ‘strong’ passwords

- A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.
- A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least eight characters.
- Contain a mix of alpha and numeric, with at least one digit.
- Is not based on anything, which could be guessed easily by someone or obtained from personal information such as name, telephone number or date of birth.

Protecting Passwords

It is of utmost importance that passwords always remain protected. The following guidelines must be always adhered to:

- Never reveal your passwords to anyone.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different systems.
- Do not use the same password for systems inside and outside of work.

Changing Passwords

- Default passwords must be changed immediately.
- If you become aware or suspect that your password has become known to someone else, you must change it immediately.

6 USER ACCESS MANAGEMENT

Each user must be allocated access rights and permissions to computer systems and data that;

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.

7 USER REGISTRATION

- Access to MGTS’s information services is controlled.
- Each user is identified by a unique user ID which will take the form of their individual MGTS email address.
- This unique ID will be used to grant access to any system or software so that users can be linked to and made responsible for their actions.
- There is a standard level of access (email access, file access, authorised software, printing and document scanning), other services can be accessed

when specifically authorised.
- Access to MGTS systems must be authorised by the MGTS person responsible and is then administered by Zenzero, our IT Provider.
- When staff leave MGTS, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the HR Director to request the suspension of the access rights by completing a leavers ticket for Zenzero to suspend.

8 USER RESPONSIBILITY

It is a user's responsibility to prevent their user ID and password from being used to gain unauthorised access to MGTS's systems by;

- Following the Password Policy Statements outlined above.
- Ensuring that any Laptop or PC or other device, when left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing their Line Manager if their role and access requirements change at any time.

9 REMOTE WORKING

- Any mobile devices including laptops, tablets and phones that have access to MGTS data must use a VPN service when using a public Wi-Fi connection.

10 NETWORK ACCESS CONTROL

- The use of non-authorised modems/routers/networking devices connected to MGTS's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with.

User Authentication for External Connections

Where remote access to MGTS's network is required, an application must be made to the Line Manager who must request the member of staff's remote access to the MGTS network is secured by a supplied VPN. Zenzero will action the request via the ticketing system following authorisation from the MGTS person responsible for IT.

Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section and the password section must be applied.

All access to operating systems is via a unique login ID that will be audited and can be traced back to each individual user. The login ID must not give any indication of the level of access that it provides to the system (e.g., administration rights). System administrators must have individual administrator accounts that will be logged and audited.

Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The access must;

- Be compliant with the User Access Management section and the Password section.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

11 SOFTWARE INSTALLATION

Zenzero controls and restricts the use of all utility programs (such as anti-virus, disk cleaner, file managers, screensavers, etc.) and other software programs by maintaining a compiled list of approved software.

12 APPLYING THE POLICY – PRIVILEDGE MANAGEMENT

- "Special privileges" are those allowed to the system manager allowing access to sensitive areas (for example, passwords, customer, or company data). The system manager for MGTS is Zenzero.
- Privileged access must be requested and authorised by the MGTS person responsible for IT.

13 ACCEPTABLE USE OF INFORMATION ASSETS

Information System – includes servers, learners and customers, network infrastructure, system and application software, data, and other computer sub-systems and components, which are owned or used by MGTS.

Staff, learners, and visitors at MGTS have access to various computing and IT resources. Many of these resources have access to the Internet and the World Wide Web (web). The Internet and web can 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 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.

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.

Users 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.

Threats

A threat if left unchecked, could disrupt the day-to-day operations of the school, the delivery of education and ultimately has the potential to compromise local and national security.

Types of Threats:

a) Cybercriminals and Cybercrime

Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either selling illegally gained information to a third party, or using directly for criminal means. Key tools and methods used by cybercriminals include: • Malware – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals • Ransomware – a kind of malware that locks victims out of their data or systems and only allows access once money is paid • Phishing – emails purporting to come from a public agency to extract sensitive information from members of the public.

b) Hacktivism

Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause. When targeted against local government or school websites and networks, these attacks can cause reputational damage locally. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Hacktivist groups have successfully used distributed denial of service (DDoS – when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of a number of councils already.

c) Insiders

Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.

d) Zero-day threats

A zero-day exploit is a cyber-attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator. It is an attack that exploits a previously unknown security vulnerability. This poses a risk to any computer or system that has not had the relevant patch applied, or updated its antivirus software.

e) Physical threats

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster, natural or otherwise, that impacts upon our IT systems.

f) Terrorists

Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

g) Espionage

Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily.

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.

14 ACCEPTABLE USE OF MGTS 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**:

- 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 their account if leaving a computer for an extended period, 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

15 MONITORING

User internet usage is monitored and recorded daily.

16 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 using 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 user's 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.

17 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

13 FURTHER INFORMATION

Further information and advice on this policy can be obtained from the MGTS person responsible for IT.

Parent Document: BS.1.03.a QUALITY POLICY

Policy Owner: Chief Executive

Date	Summary of Changes	Version:	Author (Updated by):
March 2025	Update to new format of policy and amalgamation of IT Acceptable Use and Cyber Security policies. Previously Policies No. 21 and 56.	BS.2.10.a	David Bridgens Chief Executive

Next Review: March 2026

Policy Approved By:

Ruth Plane

Ruth Plane
Quality and Compliance Manager
27.03.2025