ICT Acceptable Use Policy 2022/23

Created by	David Barnes (Network Manager)
Approved by	FPDC
Version	3.0
Date of next review	June 2024

Contents

Computer Access Control – Individual's Responsibility 3
Individuals must not: 3
Internet and email Conditions of Use 3
Individuals must not: 4
Clear Desk and Clear Screen Policy 4
Working Off-site 5
Mobile Storage Devices 5
Software 5
Individuals must not: 5
Viruses 5
Individuals must not: 6
Telephony (Voice) Equipment Conditions of Use 6
Individuals must not: 6
Microsoft 365 Suite 6
Individuals must not: 6
Actions upon Termination of Contract 7
Monitoring and Filtering 7

Acceptable Use Policy

This Acceptable Usage Policy covers the security and use of all Working Men's College information and IT equipment. It also includes the use of email, internet, voice, and mobile IT equipment. This policy applies to all Working Men's College employees, learners, contractors, and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Working Men's College business activities worldwide, and to all information handled by Working Men's College relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Working Men's College or on its behalf.

Computer Access Control – Individual's Responsibility

Access to the Working Men's College IT systems is controlled by the use of User IDs, and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Working Men's College IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any Working Men's College IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Working Men's College IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Working Men's College IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Working Men's College non-authorised device to the Working Men's College wired network or Wi-Fi systems this includes personal USB and other storage devices.
- Store Working Men's College data on any non-authorised Working Men's College equipment.
- Give or transfer Working Men's College data or software to any person or organisation outside Working Men's College without the authority of Working Men's College.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Use of Working Men's College internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Working Men's College in any way, not in breach of any term and condition of employment and does not place the individual or Working Men's College in breach of statutory or other legal obligations.

All individuals are accountable for their actions while using the Working Men's College systems, internet, and email. The list of unacceptable use of the Working Men's College IT systems and services listed below is applicable to all Working Men's College IT systems and services and is consistent with the JANET Acceptable Use Policy.
(http://www.ja.net/documents/publications/policy/aup.pdf)

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Working Men's College considers offensive in any way, including sexually explicit, discriminatory, defamatory, libellous material or material of an extremist nature.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Working Men's College, alter any information about it, or express any opinion about Working Men's College, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Send bulk emails, unless authorised and necessary. Should consult with the IT department in advance to ensure it is not blocked or delayed by email security controls. Bulk emails must be kept as short and clear as possible. Avoid attachments and unnecessary formatting and images. Consider sending a link to a webpage or a shared document instead. Always ensure the email is appropriate and that it will be relevant and of use to each recipient.
- Forward Working Men's College mail to personal (non-Working Men's College) email accounts (for example a personal Hotmail account), unless authorisation has been specifically given by the Working Men's College Data Protection Officer.
- Make official commitments through the internet or email on behalf of Working Men's College unless authorised to do so.
- Download copyrighted material such as music media (MP4) files, film, and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect Working Men's College devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Working Men's College enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers or password protected documents.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Computer screens should be positioned away from windows to prevent accidental disclosures of personal information.

- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Working Men's College remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Further information can be found in the full Remote Access policy.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Working Men's College authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must use only software that is authorised by Working Men's College on Working Men's College computers. Authorised software must be used in accordance with the software supplier's licensing agreements and the Working Men's College Change Management policy. All software on Working Men's College computers must be approved and installed by the Working Men's College IT department. Software installations request outside of curriculum planning are requested using a software install request through your line manager to the IT Dept..

Individuals must not:

- Store personal files such as music, video, photographs, or games on Working Men's College IT equipment.

Viruses

The IT department has implemented centralised automated virus detection with Cloud Based software updates. All PCs have antivirus software installed to detect and remove any viruses automatically. Any suspected breaches of viruses, malware or any suspect activity can be reported using the Working Men's College incident reporting process.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Working Men's College anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

Use of Working Men's College voice equipment is intended for business use. Individuals must not use Working Men's College voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

- Use Working Men's College voice equipment for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators (unless it is for business use).

Microsoft 365 Suite

Use of Microsoft 365 Suite (M365) at the Working Men's college includes applications such as OneDrive for Business (OneDrive), Teams and Stream. Individuals are required to use M365 only for work and work-related purposes and content. The Working Men's college retains full ownership of all data within the tenant. As M365 applications continue to expand we will provide appropriate guidance upon release.

Individuals must not:

- Upload data into college OneDrive that is not work related.
- Store sensitive college data on personal devices. Such data must remain protected within college managed and encrypted devices. Individuals are responsible for deleting any college data from their personal devices once they have left the college.
- Provide shareable link to a file to anyone. Individuals must ensure those who are accessing the file are authorised internal users or a registered external guest.
- Grant direct access to files and folders within OneDrive to external people / bodies (unless the people you are sharing with do have the right to access the data and have been approved).
- Retain downloaded data from M365 onto devices for longer than needed. Individuals must delete all data downloaded on devices via web browsers from any M365 service when is no longer required.
- Invite anyone to a Team. Team Invites should only be sent by the Team owner to authorised users who require access to the Team, it is the Team owner's responsibility for managing the

Team including making sure all users have the right to access data shared within the Team; and the conversations reflect the Working Men's College policies, Data Protection Law and any relevant Data Sharing Agreements and contracts. Individuals can also invite users external to the college to join a Team. Their access is limited, and they cannot create, delete, or edit channels. It is important to be mindful, that once they join the Team, they can see all Chats, conversations and files shared within the Team channels to which they have access, including historic chats and information.

- Send sensitive and special category data via Teams chat messages.
- Invite anyone to a Team meeting. Team meeting Invites should be sent by the Team owner or organiser. Inviting externals to a meeting or call is permitted as long as they have been authorised to join, it is the organiser's responsibility to ensure any contents of the discussion and any files are appropriate for them to access.
- Record users and participants without being informed. When recording a Teams meeting, interview, conversation, training session, lesson or video exam the Individual must inform users and participants that a recording is being made and understand:
    - What the recording and transcript is for as well as how it will be used.
    - Who will have access to the recording.
    - How long it will be kept.

  This information should be added to the agenda or invitation for meetings, as it's not always clear in Teams for example that a recording is taking place (unless stated explicitly). When saving recordings into M365 it is the Individuals responsibility to ensure that it is not shared with everyone or allow everyone in the company to access it – only authorised users and groups should have access. Any recordings that contain personal / sensitive information should be only kept for as long as necessary. When uploading recordings onto M365 Stream, it is the Individuals / owners responsibility to ensure that correct permissions are set so that only authorised users and groups are able to view the video (by default when a user uploads a video to M365 Stream, "Allow everyone in your company to view this video" is checked).

Actions upon Termination of Contract

All Working Men's College equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Working Men's College at termination of contract.

All Working Men's College data or intellectual property developed or gained during the period of employment remains the property of Working Men's College and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on Working Men's College computers is the property of Working Men's College and there is no official provision for individual data privacy, however wherever possible Working Men's College will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Working Men's College has the right (under certain conditions) to monitor activity on its systems, including internet, remote desktop, and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 1998
- EU GDPR (European Union General Data Protection Regulation) - enforceable May 2018

It is your responsibility to report suspected near miss incidents or breaches of security policy without delay to your line management, the IT department, or the IT helpdesk.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Working Men's College disciplinary procedures.