

Motherwell College  
Information and Communications  
Technology Policy Framework

---

**This Policy Framework covers the use of the Information and Communications Technology (ICT) System of Motherwell College and consists of:**

- A     **The College Network Policy**** which specifies the College's Policy regarding user responsibilities, general computing and the consequences of violation. This policy is displayed in offices, computer rooms and on notice boards around the College. Staff are issued with a copy of the framework which also forms part of the induction process.
  
- B     **A User Agreement**** which specifies the general responsibilities and standards of conduct expected of a user.
  
- C     **The College Internet Access Policy**** which specifies the policy and expected conduct of users of the Internet services available on the College Systems.
  
- D     **The E-mail Policy**** which specifies the policy and expected conduct of users of e-mail services available on the College Systems.
  
- E     **The College Phone Monitoring Policy**** which specifies the policy and expected conduct of users of College phone systems.
  
- F     **Data Protection Act 1998****
  
- G     **Regulation of Investigatory Powers Act 2000****
  
- H     **Scope of Policy****

**Using the allocated individual user account and password is taken as a statement of understanding and willingness to comply with all the terms of the ICT Policy framework of Motherwell College.**

## **A College Network Policy**

### **1.0 Statement**

The Information and Communications Technology (ICT) belonging to Motherwell College is provided for use by students, College staff and contractors' staff in support of the vision and corporate objectives of the College; reasonable personal use is also acceptable, however users should be aware that the College cannot guarantee privacy of network traffic. All users are responsible for seeing that these technologies are used lawfully, ethically and courteously.

### **2.0 Responsibilities**

- 2.1** The College is responsible for securing its facilities to a reasonable and economically feasible degree against unauthorised access and/or abuse. This responsibility includes informing users of expected standards of conduct and the resultant consequences for not adhering to them.
- 2.2** The users of the Network are responsible for respecting and adhering to Scottish, United Kingdom, European and International Law, the College's Internet Service Provider's Acceptable Use Policy, as well as the policies of the College.
- 2.3** Information and Communications Technology (ICT) can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, the integrity of the systems and related physical resources.
- 2.4** It is the policy of Motherwell College to respect all computer software copyrights and adhere to the Terms and Conditions of any licence to which the College is a party. The College will not condone the use of software that does not have a licence and any user found installing unlicensed software will be dealt with under the terms of the relevant Disciplinary Policy and Procedure.

### **3.0 General Computing Policy**

- 3.1** Authorised users of College Network facilities shall be issued with a unique User ID.
- 3.2** Prior to using their unique User ID, users shall agree, through agreement on screen, to uphold the terms of this Policy Framework and its constituent parts.
- 3.3** Authorised users are solely responsible for all actions, including Electronic Messaging, taken while their User ID is in use. Authorised users are responsible for maintaining the confidentiality of their passwords and the security of their accounts.
- 3.4** Any graphics, multimedia programs, instructional material or articles produced wholly or in part using the College Systems remain the Copyright and intellectual property of the Motherwell College.
- 3.5** The ICT Policy Framework may be amended from time to time as deemed appropriate by the College.

**Motherwell College  
Information and Communications  
Technology Policy Framework**

---

**4.0 Measures**

- 4.1** Any attempt to violate the provisions of this Policy, regardless of the success or failure of the attempt, will result in disciplinary action. Disciplinary actions may range from a reprimand, exclusion from the system or penalties afforded under College Policies. Disciplinary action in relation to staff will be in terms of the College Disciplinary Policy and Procedure, including summary dismissal where appropriate.
- 4.2** Any attempt to circumvent Scottish, United Kingdom, European or International Law through the use of College owned facilities may result in litigation against the offender by the appropriate authorities, If such an event should occur, the College will fully comply with authorities to provide any information necessary for the litigation process.
- 4.3** The College reserves the right to monitor use and to withdraw access from Users to all or part of its College Systems and other Information and Communication Technology at any time.

**5.0 Rights of Appeal**

- 5.1** The decision to exclude a user from College Systems will be made by the Director of Finance.
- 5.2** With reference to students, an appeal against the decision should be made using the procedures outlined in the College Learner Appeals Policy. The decision of the Learner Appeals Panel is final.
- 5.3** Staff should appeal using the College Disciplinary Policy and Procedure.

## **B User Agreement**

When you log on as a User of the ICT facilities of Motherwell College you agree that:

### **1.0 General**

**You will :**

- 1.1 be the sole person authorised to use this User ID;
- 1.2 be solely responsible for all actions taken under your User ID while it is valid;
- 1.3 not let others use your User ID and your Password nor inform others of your User ID or Password;
- 1.4 not delete, examine, copy or modify files and/or data belonging to other users without their prior consent;
- 1.5 not deliberately impede other users through mass consumption of system resources;
- 1.6 not take any unauthorised, deliberate action which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction, regardless of system location or time duration;
- 1.7 accept that, data stored to a C:\Drive can and will be removed by Network Services at any time.

### **2.0 Electronic Mail**

**You will :**

- 2.1 be responsible for all electronic mail originating from your User ID;
- 2.2 not forge, or attempt to forge, electronic mail messages;
- 2.3 not attempt to read, delete, copy or modify the electronic mail directed to other users without prior consent;
- 2.4 not send, or attempt to send, harassing, obscene and/or other threatening e-mail to another user of any e-mail service;
- 2.5 not send 'for-profit' messages or chain letters.

### **3.0 Network Security**

**You will not :**

- 3.1 attempt to use College Systems in attempts to gain unauthorised access to remote systems;
- 3.2 attempt to gain unauthorised access to College Systems from remote systems;
- 3.3 attempt to decrypt the system or user passwords;
- 3.4 copy College System Files;

Motherwell College  
Information and Communications  
Technology Policy Framework

---

**3.0 cont**

- 3.5 attempt to 'crash' College Systems or programs;
- 3.6 attempt to secure a level or privilege on College Systems higher than authorised;
- 3.7 load programs or computer software applications onto the College Systems or computer hard disk without the written authorisation of the Network Systems Manager;
- 3.8 wilfully introduce computer 'viruses' or other disruptive/destructive programs into the College Systems or into external networks.

**4.0 ICT Policy Framework**

**The Framework requires that you:**

- 4.1 are aware of the College Information and Communications Technology Policy Framework including all its constituent parts and accept its terms and conditions;
- 4.2 accept that violation, or attempted violation, of your responsibilities as a user may lead to your exclusion from the System;
- 4.3 have read and understood this User Agreement and accept full legal responsibility for all of the actions that you commit using the College's Systems according to any and all applicable laws;
- 4.4 understand that from time to time the College Systems and attached equipment may fail unexpectedly while you are using them and you will not hold the College responsible for lost time or data.

## **C Internet Access Policy**

### **1.0 Introduction**

Motherwell College provides an Internet Service allowing access by students and staff. This is a privilege, not a right. The policy expresses the College view on access rights, use and conduct of all users of the College Internet service.

### **2.0 The Policy**

- 2.1** The College will determine which News Groups are available.
- 2.2** All staff and students who have successfully completed introductory training or who are under instruction, will be given access via the College Internet Service.
- 2.3** The following will be recorded and monitored - user identification, terminal location, log on and off time, dates and particular sites visited.
- 2.4** The College has a commitment to equality and the Equal Opportunities Policy recognises the dignity of every individual. The downloading, saving or printing of pornographic material, including any obscene or sexually explicit images, or images containing nudity of any kind or other material contravening the Equal Opportunities Policy, Student Code of Practice and Race Equality Policy is strictly forbidden and will lead to disciplinary action which may range from exclusion from the service to penalties under College Policies.

### **3.0 Implementation**

- 3.1** The Network Systems Manager will ensure that activity is monitored on a regular basis and has the duty to report any violation.
- 3.2** Access to the College Internet Service is a privilege and can be withdrawn at the discretion of the Director of Finance.

### **4.0 Sanction Policy**

- 4.1** At first violation of the Internet Access Policy by a student a letter will be sent to the user's home address, detailing the violation relating to their User ID and Password.
- 4.2** Should the student user be under 18 years at the time of the offence, access will be denied at first violation.
- 4.3** At the second violation of the Internet Access Policy by a student, a letter will be sent to the user's home address, by Recorded Delivery, detailing the violation relating to their User ID and Password. In addition the user will be invited to attend Student Services for an interview.
- 4.4** At the third violation of the Internet Access Policy by a student a letter will be sent to the user's home address, by Recorded Delivery, detailing the violation relating to their User ID and Password. Access rights will be withdrawn and the Student Disciplinary Procedure will be used to review future attendance at College.
- 4.5** All violations by staff are dealt with under the Staff Disciplinary Policy and Procedure. In respect of paragraph 2.4 this may constitute gross misconduct and lead to summary dismissal.

**5.0 Right of Appeal**

- 5.1** The decision to exclude a user from Internet Services will be made by the Director of Finance.
- 5.2** With reference to students, an appeal against the decision should be made using the procedures outlined in the College Learner Appeals Policy. The decision of the Learner Appeals Panel is final.
- 5.3** Staff should appeal using the College Disciplinary Policy and Procedure.

## **D E-mail Policy**

### **1.0 Introduction**

Motherwell College provides a range of Information and Communications Technologies for use in the pursuit of its vision. This e-mail Policy is an integral part of the College ICT Policy Framework.

### **2.0 Policy Statement**

Access to e-mail is a privilege and certain responsibilities accompany that privilege; users of e-mail are expected to be ethical and responsible in their use.

Under no circumstances may any posting or email originating at the College be in violation of College policy or the equal opportunities policy.

Examples of unacceptable content include:-

- Sexually explicit messages, images, cartoons or a joke;
- Unwelcome propositions, request for dates or love letters;
- Profanity, obscenity, slander/defamation or liable;
- Ethnic, religious or racial slurs;
- Any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious beliefs.

### **3.0 Using the College E-mail Service**

Users are expected to act in accordance with these guidelines based on common sense, common decency and civility applied to all networked computing environments.

- 3.1** Motherwell College encourages appropriate use of e-mail to enhance productivity through the efficient exchange of information in furtherance of learning, education, research, expression and exchange of ideas and within the corporate objectives of the College.
- 3.2** The use of the College e-mail facilities for personal use is permitted provided this use does not conflict with study or work routines. All personal email you send must be marked PERSONAL in the subject heading, and all personal email sent or received must be filed in a folder marked "Personal" in your mailbox. Contact IT Support if you need guidance on how to set up and use a personal folder. All email contained in your inbox and your sent items box are deemed to be business communications for the purposes of monitoring (see item 4.0). Where possible, the College will try to avoid opening emails which are clearly marked as personal. We will, however, open such emails and review the content where malpractice or inappropriate conduct to this policy is suspected.
- 3.3** The sender of e-mail must be clearly and accurately identified. Concealing or misrepresenting your name or attempting to dissociate yourself from responsibility for your actions is a serious abuse subject to withdrawal of your privileges and appropriate disciplinary action.
- 3.4** Alteration of the source of electronic mail, message or posting is unethical and may have legal implications.

Motherwell College  
Information and Communications  
Technology Policy Framework

---

- 3.5 Users should not initiate wasteful and disruptive practices or engage in any activity that would interfere with their work or disrupt the intended use of Network Services. This is an abuse subject to withdrawal of your privileges and appropriate disciplinary action.
- 3.6 The sending of unsolicited, abusive, threatening or harassing materials is forbidden and is a serious abuse subject to withdrawal of your privileges and appropriate disciplinary action.
- 3.7 The sending of chain letters, broadcast messages and unwanted images is forbidden and is a serious abuse subject to withdrawal of your privileges and appropriate disciplinary action. Bulletin boards are available for general notices.
- 3.8 E-mail and other College Systems should not be used for personal financial gain or to support personal commercial activity. This will be regarded as a serious abuse subject to withdrawal of your privileges and appropriate disciplinary action.
- 3.9 Conduct which involves the use of resources that violate a College Policy or Procedure or to violate another's rights, is a serious abuse subject to withdrawal of your privileges and appropriate disciplinary action.
- 3.10 Violations of this policy by staff will be dealt with under the Staff Disciplinary Policy and Procedure. Violations of paragraphs 3.2 to 3.10 above may constitute gross misconduct and lead to summary dismissal.

#### **4.0 Monitoring of E-mail**

Motherwell College reserves the right to monitor the volume and content of e-mail use across the College Systems in support of the business interests of the College and to investigate complaints regarding the use of individual e-mail accounts.

Motherwell College has an interest in regulating the content of electronic mail, to ensure that the College's policies and procedures are being complied with and for legitimate business purposes

#### **5.0 Absence & Sickness**

Staff users should be aware that their emails may need to be viewed if they are absent, particularly if the absence is unexpected. Written approval for access must be given by a member of the Senior Executive Team before this takes place.

#### **6.0 Right of Appeal**

- 6.1 The decision to exclude a user from College Systems will be made by the Director of Finance.
- 6.2 With reference to students, an appeal against the decision can be made, in writing, to the Principal and Chief Executive using the College Complaints Procedure for students. The decision of the Principal and Chief Executive is final.
- 6.3 Staff should appeal using the College Disciplinary Policy and Procedure.

## **7.0 Default Settings of E-mail Service**

### **7.1 Students**

- 7.1.1 Maximum size on inward and outgoing mail 20Mb;
- 7.1.2 Maximum Mailbox size 50Mb;
- 7.1.3 Trash emptied every 30 days;
- 7.1.4 Student e-mail accounts will be withdrawn and deleted on 30 June each year.

### **7.2 Staff**

- 7.2.1 Maximum size of inward mail is 20Mb; unlimited outgoing;
- 7.2.2 Maximum Mailbox size 250Mb;

### **7.3 Disclaimer**

All e-mail originating from the College, both from staff and students, will have the following notice appended;

“This e-mail (including any attachments to it) contains information which is confidential. It is intended only for the use of the named recipient. If you have received this e-mail in error, please let us know by replying to the sender, and immediately delete it from your system. Please note, that in these circumstances, the use, disclosure, distribution or copying of this information is strictly prohibited. We apologise for any inconvenience that may have been caused to you. Motherwell College cannot accept any responsibility for the accuracy or completeness of this message as it has been transmitted over a public network. The College reserves the right to monitor all incoming and outgoing email traffic. Although the College has taken reasonable precautions to ensure no viruses are present in emails, the College cannot accept responsibility for any loss or damage arising from the use of the email or attachments. Any views expressed in this message are those of the individual sender, except where the sender specifically states them to be the views of Motherwell College.”

- 7.4 The College reserves the right to scan electronically all incoming and outgoing email traffic for viruses. Any e-mail which is found to contain a virus will be blocked from entering or leaving the College Systems. The originator and intended recipient of any blocked e-mails will be notified that the message has been prevented from being delivered.

## **E Phone Monitoring Policy**

### **1.0 Introduction**

Motherwell College provides phone systems for use by staff.

### **2.0 Monitoring of College Phones**

Motherwell College reserves the right to monitor the destination, volume and duration of all incoming and outgoing calls to College phones in support of the business interests of the College and to investigate complaints.

Staff should be aware that their voicemail messages may need to be checked if they are absent, particularly if the absence is unexpected. Written approval for access must be given by a member of the Senior Executive Team before this takes place.

The software system used allows a full analysis by each extension number identifying the external number calling (or being called) and the duration of the call. The system does not have the capability to record calls made using College phones.

## **F Data Protection Act 1998**

Motherwell College is registered as a Data Controller and subscribes to the Data Protection Principles as contained in the Data Protection Act 1998. Motherwell College holds and processes personal data for purposes connected with its statutory and business requirements, as outlined in its entry in the Data Protection Register. The processing of personal data relates to staff, students and agents of the College and applies to both computer and manual records (including filing systems and CCTV). The College is committed to ensuring that all those processing data on its behalf are aware of their obligations in processing data under the 1998 Act and that data subjects are made aware of their rights as laid out in the Act.

## **G Regulation of Investigatory Powers Act 2000**

The College is entitled under the Telecommunications (Lawful Business Practice) (Interception and Communications) Regulations 2000, issued under the Regulation of Investigatory Powers Act 2000, to monitor or keep a record of communication to:

- i ensure they are business related;
- ii ensure the College's policies and procedures are being complied with; and
- iii investigate or detect the unauthorised use of the College Systems.

## **H Scope of Policy**

This policy covers all users of the College Systems. However, for the purposes of monitoring and investigation only, the Senior Executive Team and accredited Network Systems staff are outwith the scope of this policy.