



## **CORPORATE POLICY AND PROCEDURES FRAMEWORK**

### **Information and Communications Technology Policy and Procedures**

#### **1.0 Purpose**

These Policy and Procedures are designed to detail the correct and acceptable use of the College Network and ICT resources.

#### **2.0 Policy**

***Jewel & Esk College will ensure that the Information and Communications Technology under its control will be used lawfully, ethically and courteously.***

#### **3.0 Scope**

- 3.1 These policies apply to members of the Board of Governors, College staff, visitors, contractors and students who become authorised users of the College ICT.
- 3.2 The College Management Team and staff designated as working within the Network Services are exempt from this policy while conducting monitoring and investigation activities.
- 3.3 This policy should be read in conjunction with the College Equality Diversity & Inclusion Policy and its separate Disability, Race and Gender Equality Schemes.

#### **4.0 Responsibilities**

- 4.1 The Depute Principal is responsible for the implementation and development of this policy.
- 4.2 All staff, students and network users are responsible for complying with the requirements detailed in each section of these policies and procedures.

#### **5.0 Framework Structure**

- 5.1 The ICT Policy and Procedures Framework is divided into 5 distinct policies to address specific requirements of the College ICT service.

These are:

- A** The College Network Policy, which specifies the College's Policy regarding user responsibilities, general computing and the consequences of violation.
- B** A User Agreement, which specifies the general responsibilities and standards of conduct expected from 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 network.
- D** The E-mail Policy, which specifies the policy and expected conduct of users of the Internet services available on the College network.
- E** Remote Access Policy, which covers users accessing the College Network Services from a remote location

- 5.2 Using the account and password allocated to the individual user is taken as a statement of understanding and willingness to comply with all the terms of the ICT Policy of Jewel & Esk College.

## **6.0 Review of Framework**

- 6.1 These ICT Policy and Procedures may be amended from time to time to comply with legislation changes and to include any new conditions deemed appropriate by the College. ICT Policy and Procedures will be reviewed annually.

## **A College Network Policy**

### **1. Statement**

The Information and Communications Technology (ICT), under the control of Jewel & Esk College, is provided for use by authorised college network users in support of the mission of the College; reasonable personal use is also acceptable.

### **2. Responsibilities**

All users are responsible for seeing that these technologies are used lawfully, ethically and courteously.

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.

The users of the Network are responsible for respecting and adhering to Scottish, United Kingdom, European and International Law, the [Internet Service Provider's Acceptable Use Policy](#), as well as the policies of the College.

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.

### **3. General Computing Policy**

Authorised users of the College Network facilities shall be issued with a unique User ID and password.

Prior to using their User ID, users shall agree, through agreement on screen, to uphold the terms of this Policy and Procedures and its constituent parts.

Authorised users are solely responsible for all actions, including Electronic Messaging, taken whilst their User ID is in use. Authorised users are responsible for maintaining the confidentiality of their passwords, and the security of their accounts.

Any graphics, multimedia programs, instructional material or articles legally produced wholly or in part using the Network Services of Jewel & Esk College remains the Copyright and intellectual property of the College.

Data held on College ICT equipment is subject to the Data Protection Act 1998 and subsequent legislation. All users are expected to adhere to the College Data Protection Policy and Procedures.

4. Network Account Policies

Network Account Holders should store files in their respective home folder on the college network. The contents of these folders are backed up regularly. The College cannot guarantee the safety or security of data stored on local or removable drives/media of client machines.

Memory allocations for home folders are 50Mb per student account and 100Mb for a staff account. Users requiring additional storage space are encouraged to purchase a “memory stick” or CDs to store data.

All student access will be disabled and the content of the home folder deleted at the end of the academic year. Continuing students will have the contents of their home folder restored at the start of the new session following successful student registration process for the new session.

The network accounts of staff leaving Jewel & Esk College will be disabled on the day of departure. This includes email access. Home directories and e-mail content of staff leaving become the property of JEC on the day of departure and staff should delete any personal or confidential information prior to departure date.

5. Measures

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.

Any attempt to circumvent Scottish, United Kingdom 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.

In terms of the Employment Practices Data Protection Code: Part 3: Monitoring at Work (Data Protection Act 1998) the College reserves the right to monitor use and to withdraw access from Users to all or part of its Network and other Information and Communication Technology at any time.

Student network access may be withdrawn for non-payment of library fees or other outstanding charges, in which case this decision will be made by the Learning Resources Manager.

6. Rights of Appeal

The decision to exclude a user from Network Services will be made by the appropriate manager and details of the exclusion will be recorded.

An appeal against the decision can be made, in writing, using the College Student Appeals Policy and Procedure.

Staff should appeal using the College Grievance Policy and Procedures.

## **B User Agreement**

1. When you log on as a User of the ICT facilities of Jewel & Esk College you agree that:

### 2. General

You will:

- accept the College Network Policy;
- be the sole person authorised to use this User ID;
- not let others use your User ID and your Password;
- be solely responsible for all action taken under your User ID
- not access, delete, copy or modify any files and /or data belonging to other users without their prior consent.
- not deliberately impede other users through mass consumption of system resources;
- 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;
- accept that, data stored on hard drives or other College system media may be removed by Network Services at any time
- not cause inappropriate or offensive images or text to be displayed on any screen or equipment.
- not cause inappropriate or offensive images or text to be sent for printing or scanning.

### 3. Electronic Mail

You will:

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

### 4. Network Security

You will not:

- attempt to use College Systems or Networks in attempt to gain unauthorised access to remote systems;
- attempt to gain unauthorised access to College Systems or Networks from remote systems;
- attempt to decrypt the system or user passwords
- take unauthorised copies of System Files or data;
- attempt to “crash” Network systems or programs;
- attempt to secure a level of privilege on Network systems higher than authorised;

- load programmes onto the System, Network or computer hard disk without the authorisation of the Network Services Manager;
- Wilfully introduce computer “viruses” or other disruptive/destructive programs into the College Network or cause them to be distributed.

5. Understanding the ICT Policy Framework

This Framework requires that you:

- are aware of the College ICT Policy and procedure including all its constituent parts and accept its terms and conditions;
- accept that the violation or attempted violation, of your responsibilities as a user may lead to your exclusion from the System;
- have read and understood this User Agreement and accept full legal responsibility for all the actions that you commit using the College's Network according to any and all applicable laws;
- understand that from time to time the College Network 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. Introduction

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

### 2. The Policy

All authorised network users will gain access to the College Internet Service unless explicitly excluded from this privilege.

The following will be recorded and monitored – user identification, terminal identification, logon and logoff time, dates and sites visited.

The downloading, uploading, copying, saving or printing of pornography or any other unacceptable material is strictly forbidden and will lead to disciplinary action, which may range from exclusion from the service to penalties under College Procedures.

### 3. Implementation

The Manager of the Network will ensure that activity is monitored on a regular basis and has the duty to report any violation.

Access and use of the College Internet service is a privilege and can be withdrawn at the discretion of the Principal and Chief Executive.

### 4. Sanction Policy

#### a) *Students*

At first violation of the Internet Access Policy by a student the user will be requested to attend an interview with Student Services to discuss the violation and any remedial action.

Should the Student user be under 18 years at the time of the offence, Internet Access will be withdrawn.

At the second violation of the Internet Access Policy by a student, a letter will be sent to the students address by Recorded Delivery, detailing the violation relating to their User ID and Password. In addition the user will be requested to attend Student Services for an interview to discuss the violation and any remedial action.

At the third violation of the Internet Access Policy by a student a letter will be sent to the students address by Recorded Delivery, detailing the violation relating to their ID and Password. **Internet access** rights will be withdrawn and the Student Disciplinary Procedure will be used to review the future attendance at the College.

b) *Staff*

All violations by staff are dealt with under the Staff Disciplinary Policy and Procedures. This may constitute gross misconduct and lead to dismissal.

c) *Halls of Residence Guests*

Violation of the Internet Access Policy by a Halls of Residence Guest will be notified to the Halls of Residence Manager. The user will be requested to attend an interview with the Halls of Residences manager to discuss the violation and any remedial action.

d) *Visitors*

Violation of the Internet Access Policy by a college Visitor will result in withdrawal of Internet Access and the violation will be reported to the visitors sponsor for appropriate action to protect both the user and the college.

e) *School Winter Leavers*

Violation of the Internet Access Policy by a "School Winter Leaver" will result in withdrawal of Internet Access and the violation will be reported to Schools Liaison Officer. The user will be requested to attend an interview with the Schools Liaison Officer and appropriate action implemented to protect both the user and the college.

5. Right of Appeal

The decision to exclude a user from Network Services will be made by the appropriate Manager and details of exclusion will be recorded.

An appeal against the decision can be made in writing, using the Student Appeals Policy & Procedure.

Staff should appeal using the College Grievance Policy and Procedure.

## **D. E-Mail Policy**

### 1. Introduction

Jewel and Esk 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 and Procedures.

### 2. Policy Statement

Access to email is a privilege and certain responsibilities accompany the privilege; users of email are expected to be ethical and responsible in their use.

### 3. Using the College E-Mail Service

Users are expected to act in accordance with these guidelines based on common sense, common decency and civility.

Jewel and Esk 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 mission of the College.

The use of the College e-mail facilities for personal use is permitted provided this use does not conflict with work routines.

Jewel & Esk College has no interest in regulating the content of electronic mail other than for virus and spam prevention but it cannot guarantee the privacy or confidentiality of electronic documents. However, in view of the content of clause 4 of the e-mail policy, staff are strongly recommended to indicate under the subject heading where an e-mail is personal.

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.

Alteration of the source of electronic mail is unethical and may have legal implications.

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.

The sending of unsolicited, abusive, threatening or harassing material is forbidden and is a serious abuse subject to withdrawal of your privileges and appropriate disciplinary action.

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.

E-mail and other Network services 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.

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.

4. Monitoring of E-Mail

Jewel and Esk College reserves the right to monitor and restrict the volume of email use across the Network and to investigate complaints regarding the use of individual e-mail accounts.

In the pursuance of legitimate business of the College, Jewel & Esk College reserves the right to survey the contents of emails when there is suspicion, or information has been received that e-mail facilities are being used illegally or in breach of this Policy.

Such monitoring will be carried out in accordance with the guidelines within the Data Protection Act.

It may be necessary, for purely business purposes, to access incoming or stored e-mails of members of staff who are absent through holiday or illness and e-mails stored by former employees. Such access must be handled with sensitivity with all possible steps being taken to avoid inadvertently opening personal e-mails. Authority for this activity may only be given by a member of the College's Senior Executive Team. A record of such incidences will be held in the Data Protection Register, held by the college.

5. Right of Appeal

The decision to exclude a user from Network Services will be made by the appropriate Manager and details of the exclusion will be recorded.

Staff should appeal using the College Grievance Policy and Procedures.

6. Default Settings of E-Mail Service

Maximum mailbox size is limited to 100MB per staff member.

## **E. Remote Access Policy**

### **1. Introduction**

Jewel & Esk College provides a range of ICT for use in the pursuit of its vision, which includes equipment for remote or offsite use and remote access to limited Network Services.

This Remote Access Policy is an integral part of the College ICT Policy Framework.

### **2. Policy Statement**

The provision of College equipment for remote access to Network Services is a privilege and certain responsibilities accompany those privileges.

### **3. Procedures when using remote Access**

Users are expected to act in accordance with the following guidelines:

Web-based access to College Systems is provided to members of staff to enable them to work remotely and gain access to limited network systems (email; Library Catalogue; VLE). Whilst accessing College network resources, the user is covered by the College ICT Policy Framework.

Web-based access to the College Library Catalogue and the VLE is provided for students to enable them to pursue their studies on-line. Whilst accessing the College network resources, students are covered by the College ICT Policy Framework.

Where the College provides staff with Internet access through a third party Internet Service Provider (ISP) the use of this service is covered by the Acceptable Use Policy (AUP) of the relevant ISP.

All equipment and software, provided by the College, to enable remote access remains the property of Jewel & Esk College.

### **4. Insurance**

Members of staff and students who have the loan of laptops or other IT equipment will be expected to add these to their household contents insurance as declared items. Acceptance of loan of IT equipment is taken as user acceptance of responsibility for any loss and/or damage to such IT equipment during term of loan.

5. Withdrawal of Remote Access Privileges

The College reserves the right to deny remote access to network services for violation of the ICT Policy Framework.

The College reserves the right to recover equipment or withdraw support for remote access if:

- There is evidence that the privilege has been abused.
- The user has allowed access by an unauthorised third party.
- The member of staff leaves the employment of the College.
- A student leaves the course or the course terminates.

6. Right of Appeal

The decision to exclude a user from remote access will be taken by the appropriate manager and details of exclusion will be recorded.

The decision to withdraw equipment, software and remote access support will be taken by the Depute Principal.

Staff should appeal using the College Grievance Policy and Procedures.

Students may appeal using the Student Appeals Policy and Procedures.