



CORPORATE POLICY & PROCEDURE FRAMEWORK

Data Protection Policy and Procedures

1.0 Purpose of this Document

- 1.1 These Policy and Procedures detail the Data Protection Policy and guidelines for Jewel & Esk College

2.0 Policy

Jewel & Esk College is committed to ensuring that the processing of personal data is only undertaken in the legitimate operation of the College's business. The College will ensure that the eight principles on which the Act is based are made known to and observed by all College Staff.

3.0 Scope

- 3.1 The College collects and uses information (data) about its staff, students and other individuals with whom it has contact for a variety of purposes.
- 3.2 Data is legitimately processed for a variety of reasons including the recruitment and payment of staff, the organisation and administration of courses and programmes, the monitoring of health and safety arrangements, the monitoring of separate equality diversity and inclusion strands (i.e. age, disability, gender, race) particularly in respect of student admissions/staff recruitment and the monitoring of performance, achievement and assessment and compliance with statutory obligations, government agencies and other bodies.
- 3.3 In collecting and processing data, the College is committed to complying with the requirements of the Data Protection Act 1998. In terms of the Act information must be collected and used fairly, stored safely and not disclosed to any third party unlawfully.
- 3.4 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 The Data Protection Principles

- 4.1 Embedded within the Act are 8 Data Protection Principles which must be followed. The 8 Principles provide that:

- 4.1.1 Personal data shall be processed fairly and lawfully. Schedule 2 of the Act provides that certain conditions must be met e.g.
 - (i) the data subject has given consent
 - (ii) the processing is necessary.
- 4.1.2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.
- 4.1.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- 4.1.4 Personal data shall be accurate and, where necessary kept up to date.
- 4.1.5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or the purposes.
- 4.1.6 Personal data shall be processed in accordance with the rights of data subjects under the 1998 Act.
- 4.1.7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to personal data.
- 4.1.8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and Freedoms of data subjects in relation to the processing of personal data.

5.0 Status of the Policy

- 5.1 Any member of staff, student or other individual who considers that the Policy has been breached in respect of personal data about themselves should raise the matter with the College's Records Management Officer.
- 5.2 This Policy does not form part of the formal contract of employment but it is a condition of employment that employees abide by Policy and adhere to the guidelines which follow. Failure to adhere to the Policy can therefore result in disciplinary proceedings.

6.0 Jewel and Esk College as a Data Controller

- 6.1 The College as a body corporate is the data controller under the Act and whilst the Board of Governors is therefore ultimately responsible for implementation in terms of the Board of Governors Delegation Scheme contained within the Constitution and Articles of Governance this function is vested in the Principal. However the Records Management Officer is charged with dealing with day to day matters.
- 6.2 The College is registered as a data controller with the Data Protection Commissioner and the Director of Human Resources has been designated as the College's Data Protection Officer.

- 6.3 The College endeavours at all times to maintain data in secure conditions and processes and discloses information in terms of its notification to the Data Protection Commissioner (see Appendix A)
- 6.4 Any member of staff, student or other individual writing to make specific enquiries about their data should contact the Records Management Officer in the first instance.

7.0 Rights of Data Subjects

- 7.1 All staff, students and other individuals are entitled to know;
 - 7.1.1 what information the College holds and processes about them and why;
 - 7.1.2 how to gain access to it;
 - 7.1.3 how to keep it up to date;
 - 7.1.4 what the College is doing to comply with its obligations under the 1998 Act;
 - 7.1.5 the College through this Policy and the issue of further guidance when appropriate will ensure that staff students and other data subjects are notified of the above as appropriate.

8.0 Rights of Access to information

- 8.1 Staff, students and other individuals have a right to a copy of the personal information the College holds about them either in electronic or manual form. Any person wishing to exercise this right is required to put this request in writing to the Records Management Officer. The College may make a charge of £10 on each occasion access is requested.
- 8.2 The College will comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days unless there is good reason for delay. In the event of there being a delay, the delay will be explained in writing to the data subject making the request.
- 8.3 Parents\Guardians of students aged over 16 do not have the right of access to information and will not be given access to data relating to the student unless the student has given written consent for the release of information

9.0 Right to Object to Data Processing

- 9.1 Staff, students and other individuals have a right to object to data processing that causes damage or distress. Any objection to processing must be put in writing and sent to the Records Management Officer.

10.0 Responsibility for the Accuracy of Data

- 10.1 Staff are responsible for:
 - 10.1.1 checking that the information they provide to the College in connection with their employment is accurate and up to date;

10.1.2 informing the College of any changes to the information they have provided, e.g. address, qualifications etc.

10.2 Students are responsible for:

10.2.1 ensuring that all personal data provided to the College is accurate and up to date;

10.2.2 notifying the registrar or Faculty Assistant of any alterations to their address or personal details as provided on the enrolment form.

10.3 The College cannot be held responsible for any errors unless the member of staff or student has advised the College accordingly.

11.0 Processing of Data

11.1 Staff who, as part of their responsibilities, collect data about other people must comply with the Guidelines for Staff (Appendix C).

11.2 Staff must ensure that any personal data is held securely and that information is not disclosed either orally or in writing or accidentally or otherwise to any third party

11.3 Students using the College's computer facilities may, on occasion, process personal data as part of their studies. If they do so they must notify their tutor, who will pursue any necessary enquiries with the Records Management Officer.

12.0 Sensitive Data

12.1 In certain circumstances, the College may only process personal data with the consent of the individual. Some data is considered in terms of the Act as sensitive, for example information about a person's health, racial or ethnic origin, criminal convictions or trade union membership. The information may be processed to ensure the College is a safe place for everyone or in legitimate operation of other procedures, such as sick pay and in the monitoring of equal opportunities.

13.0 Assessment Data and Examination Results

13.1 Assessment grading and examination results will not be published on notice boards where a student can be identified by name. However lists, using discreet individual SQA or other examining body reference numbers are acceptable.

13.2 Results will not be divulged over the telephone unless there is prior agreement to do so. Results may only be divulged by the Head of Faculty, Learning Manager or course tutor and only to the student to whom the results relate, providing security measures to confirm the students' identity as set out in the guidelines for staff, have been followed.

14.0 Retention of Data

14.1 Retention of data is contained within Appendix B. (Retention of Records Containing Personal Data).

15.0 Compliance

- 15.1 Compliance with the 1998 Act is the responsibility of all members of staff of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College's facilities being withdrawn or even criminal prosecution. Any question or concerns about the interpretation of this Policy should be addressed to the Records Management Officer.

Data Protection Policy Appendix A

Purposes of Processing

As outlined the College collects and uses data about its staff and students for a variety of purposes, including:

Staff

- the organisation and management of the College;
- the payment of salaries and wages;
- recording membership of trade union and/or of professional body or society to facilitate payment of subscriptions;
- recording medical history to ensure suitability for appointment;
- issuing staff identity cards;
- CCTV monitoring on College campuses;
- seeking improvements in health and safety;
- staff development;
- recording of age, disability, ethnic origin and gender. Some of this information is required on a voluntary basis and is used to enable the College to evaluate the operation of its Equality Diversity & Inclusion Policy and related Equality Schemes.
- recording of periods of sickness to enable payment of statutory sick pay;
- providing employment references;
- statistical analysis and forward planning;

Students

- Administration (includes personal and academic details) and management of academic processes (e.g. academic quality audits, examination boards and awarding of certificates/diplomas);
- management of halls of residence;
- provision of advice and support to students (through the Student Services [Hardship Funds and Student Loans], Counselling Service and the Careers Service);
- issuing of matriculation cards;
- seeking improvements in health and safety;
- CCTV monitoring on College campuses;
- recording and monitoring of age, disability, ethnic origin and gender. Some of this information is requested on a voluntary basis and is used to enable the College to evaluate the operation of its Equality Diversity & Inclusion Policy and related Equality Schemes. This information is also requested by the Scottish Further & Higher Education Funding Council to ensure that provision and support reflects the multi-cultural community.

Disclosure of Information

The College discloses information about its staff and students to the following.

Staff

- relevant Government and Scottish Executive and other bodies to which the College has a statutory obligation to release information, including:
- the Scottish Funding Council;
- the Scottish Qualifications Authority and other examining bodies;
- the Inland Revenue;
- Scottish Enterprise;
- the Department for Work & Pensions (formerly Department of Social Security);
- potential employers of College staff;
- potential providers of education and training to College staff;
- external agents employed by the College in the conduct of its business.

Students

- relevant Government and Scottish Executive and other bodies to which the College has a statutory obligation to release information including:
- the Scottish Funding Council;
- the Scottish Qualifications Authority and other examining bodies;
- Scottish Enterprise
- the Students Awards Service;
- the Child Benefit Agency;
- the Department for Work & Pensions (formerly the Department of Social Security);
- Local Education Authorities;
- Local Authority Council Tax Offices;
- the Benefits Agency;
- current or potential employers of our students;
- current or potential providers of education/training to our students.

Instructions on Disclosure

Disclosure to persons or institutions not listed above will be made only with the permission of the member of staff or student, unless exceptional circumstances apply, as provided by law.

**Data Protection Policy
Appendix B**

Retention of Records containing Personal Data

This list is not exhaustive, but provides guidance as to best practice.

Type of Record	Suggested Retention Period of	Reason for Length of Period
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from end of employment	References and potential litigation
Application forms / interview notes	At least 6 months from date of interview	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	6 years from date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from the date of redundancies	Limitation Act 1980
Income Tax and NI Returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records related	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As Above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As Above	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident Books and records and reports of accidents	3 years after the date of last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
Health Records	During employment	Management of Health and Safety at work Regulations
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999
Ionising Radiation Records	At least 50 years after last entry	Ionising Radiation Regulations 1985

Student records, including academic achievements and conduct	At least 6 years from the date that the student leaves the institution in case of litigation for negligence	Limitation period for negligence.
	At least 10 years for personal and academic references	Permits institution to provide references for a reasonable length of time
	Certain personal data may be held in perpetuity	While personal and academic references may become "stale", some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data.
Student Work	At least 6 months after end of last attended session	Moderation and validation of assessments by awarding body. HMI Inspection

Data Protection Policy Appendix C

Guidelines for Staff

1.0 Introduction

The Data Protection Act 1998 came into force on 1 March 2000 and the full provisions of the Act came into force on 24 October 2001. The Act covers all personal data held in computerised and manual filing systems.

The College has adopted a Data Protection Policy covering the arrangements made by the College to implement the requirements of the Act. All staff must be aware of and ensure that they comply with the Policy.

The guidelines cannot cover every eventuality. Further information and advice is available from Linda Curtin, Records Management Officer on ext7370 or email lcurtin@jec.ac.uk. Copies of the Data Protection Policy are available on the college website www.jec.ac.uk

2.0 Aim of the Act

2.1 The aim is to ensure data is collected and used in a responsible way and to provide individuals with some control over the use of personal data, in particular unforeseen secondary uses, and to provide protection from unwanted or harmful uses of the data.

2.2 To achieve this aim, the College, as data controller, requires to adhere to the following key concepts:

2.2.1 Purpose

The College should process personal data only when it has a clear purpose for doing so.

2.2.2 Fairness

As has been highlighted previously there are many legitimate purposes for processing personal data, even where individuals may not wish this to happen. For processing to be fair, the individual must be informed of the purposes for which his/her data is to be processed. Processing will only be fair when it meets one of a number of criteria set out in the Act, for example, that it is necessary in order to pursue the lawful interests of the College.

2.2.3 Transparency

Individuals have responsibility for enforcing their rights. To enable them to do so, they require to know the purpose of the processing and the measures the College has taken to ensure the processing is fair.

3.0 Personal Data

3.1 Personal data refers to any data relating to a living individual who can be identified from the data, this includes photographs and videos or from the data and other information which the College has in its possession, or which is likely to come into its possession. Personal data also includes any expression of opinion about the individual and any indication of the College's intentions in respect of the individual.

- 3.2 The data includes information which is:
- 3.2.1 being processed by computer;
 - 3.2.2 being recorded with the intention that it should be processed by means of computing equipment;
 - 3.2.3 being recorded manually as part of a filing system or with the intention that it should form part of a filing system.
- 3.3 It is essential that staff are aware that personal data processed over the world wide web or other internet software is included in the above.

4.0 Processing of Data

4.1 Staff processing data as a legitimate part of their employment (e.g. teaching, administration) do so under the College's notification to the Data Protection Commissioner. The main areas of notification are included in Appendix A of the College's Data Protection Policy.

4.2 Many staff process data about students on a regular basis. Whilst much of this will be non sensitive there will be some which is regarded as sensitive. Examples of non sensitive data include:

4.2.1 Non Sensitive Data:

- a) name and address;
- b) date of birth;
- c) details on class attendance, course work marks;
- d) reports and references;
- e) notes of personal supervision including matters about behaviour and discipline;

Examples of sensitive data include:

4.2.2 Sensitive Data:

- a) student's physical and mental health;
- b) religion or religious views;
- c) sexual life;
- d) political views and activity;
- e) trade union membership;
- f) race/ethnicity;
- g) nationality;

Such information can only be collected and processed with the student's express consent.

5.0 Checklist for processing Data

- 5.1 Before processing any personal data, all staff should consider the following
 - 5.1.1 Do you really need to record the information?
 - 5.1.2 Is the information “non sensitive” or is it “sensitive” personal data?
 - 5.1.3 If it is sensitive, do you have the data subject’s express consent?
 - 5.1.4 Has the data subject been told that this type of data will be processed?
 - 5.1.5 Are you sure that the data is secure?

6.0 Record Keeping

- 6.1 Staff have a duty to make sure they comply with the 8 data protection principles set out in the Act earlier in this policy. In particular staff must ensure:
 - 6.1.1 records are accurate;
 - 6.1.2 records are up to date;
 - 6.1.3 records are kept and disposed of safely.

7.0 Manual Records

- 7.1 It is important to ensure that manual records as well as computer based records comply with the requirements outlined above.
- 7.2 All information held in manual records will need to be disclosed to an individual who makes a request for access to information under the Act. It is essential that all statements made about an individual are written in a way that is fair and accurate. In particular staff should ensure that no libellous statements are made which would result in legal action. Personal notes written about an individual in any form (even on a scrap of paper or post – it) would need to be disclosed if they were retained in a filing system.

8.0 Security

- 8.1 All staff are responsible for ensuring that any personal data which they hold is kept securely.
- 8.2 Personal information should, so far as is possible be kept in
 - 8.2.1 a locked filing cabinet
 - 8.2.2 a locked drawer or
 - 8.2.3 if computerised, be password protected or
 - 8.2.4 kept only on disk which itself is kept securely

- 8.3 It is recognised that it is impractical for manual information to be locked away at all times during the working day, and that normal practice would be for filing cabinets and drawers to be unlocked during the day and locked overnight. It is nevertheless important to ensure that information is not accessible during the day to those who should not be permitted to see it.
- 8.4 Staff who process personal data at home or other locations must take reasonable steps to ensure that the data is kept securely and is not accessed, disclosed or destroyed.
- 8.5 Staff using a home or laptop computer should ensure they have an up-to-date virus scanning programme installed. Laptop computers should be kept constantly in view when travelling.
- 8.6 When personal data is to be destroyed, paper or microfilm records should be disposed of by shredding or incineration, computer hard disks or floppy disks should be re-formatted, over written or degaussed.

9.0 Disclosure of Data

- 9.1 Staff must not disclose personal data to anyone except as required within the course of their duties. All staff are responsible for ensuring personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- 9.2 Staff should note that unauthorised disclosure is a disciplinary matter.

10.0 Confidential References

- 10.1 Confidential references written by external referees received by members of College staff are required to be disclosable to the individual who is the subject of the reference. However, they will generally only be disclosed with the referee's consent. A decision on whether to disclose a reference will be made by the Director of Human Resources as indicated under Section 13.

11.0 Photographs and Videos

- 11.1 When taking photographs or making video recordings of staff and/or students, as individuals, as small groups or organised groups, the individual(s) concerned should be informed of the purpose(s) and asked to give consent.
- 11.2 For general photographs or video recordings of public places and campuses, consent is not required.

12.0 The College Website and College Intranet

- 12.1 Personal data placed on the College's web site will be available in countries which do not have a data privacy regime considered adequate by the European Union. Where it is wished to make staff and/or students personal data available in this way, the staff and/or students concerned should be informed that they have the right to object to the use of their data where it would cause them significant damage or distress.

- 12.2 Personal data placed on the College intranet will be available to all network users and some external partners.
- 12.3 Where personal data is to be used for other purposes, for example publicity photographs the consent of the staff and/ or student(s) concerned must be obtained.
- 12.4 When individuals input personal data over the Web, such as names and addresses of individuals who request publicity materials, then the relevant web page should indicate the purpose for which the data is collected.
- 12.5 Individuals must be given the opportunity to opt out of parts of the collection or use of the data not directly relevant to the specific purpose for example, where the name and address is provided in order to receive publicity materials, an application form etc., if a follow up scheme is used to discover why candidates did not come to the College, the individual should be notified of the scheme and given the opportunity to opt out of it.

13.0 Request for Access to Information

- 13.1 Requests for access to information by staff, students or other individuals must be made in writing to the Records Management Officer.
- 13.2 On receipt of a request for information and the required fee (£10) the information will be collected and collated as appropriate.
- 13.3 The Records Management Officer will determine whether all the information received can be released to the individual requesting the information. It may not be possible to release information which makes reference to another individual, unless it is possible to delete reference to that individual.
- 13.4 The Records Management Officer will ensure that all information collated in response to a request is provided within the 30 days timescale.

14.0 In case of Emergency

- 14.1 In case of emergency it may be justifiable to release information.
- 14.2 Where a relative or close family friend is seriously ill, it may be felt necessary to release a student's phone number to a friend or relative. A judgement needs to be made when a request is received as to whether the College would be justified in releasing the information irrespective of the strict requirements of the 1998 Act.

15.0 Warning

- 15.1 Information must not be disclosed to bailiffs and similar individuals wishing to serve writs or to enforce judgements in civil matters. The student or member of staff concerned should be advised of the approach in case they wish to pursue the matter.

16.0 Review of Policy

- 16.1 This Policy will be reviewed annually.

Data Protection Policy

Appendix D

Employment Practices Data Protection Code Part 3 - Monitoring At Work

1.0 Background

- 1.1 In July 2003 the Information Commissioner published the third part of the Employment Practices Data Protection Code – Monitoring at Work.
- 1.2 The purpose of this Code is to advise employers on what is permissible if monitoring the activities of employees is undertaken.
- 1.3 It should be noted this Code does not impose new legal obligations – the Code is designed to enable employers to comply with the Data Protection Act 1998 and to adopt good practice.

2.0 College Statement

- 2.1 The management of Jewel & Esk College welcomes the Information Commissioner's Code of Practice.
- 2.2 Staff can be assured that no inappropriate monitoring is undertaken.
- 2.3 The College's Information and Communications Technology Policy and Procedures outline that certain safeguards have been put in place (See Monitoring in the College context below).

3.0 Examples of Monitoring

Not all examples of monitoring referred to within the Code apply to Jewel and Esk College. However for the purposes of clarity the following activities are addressed within the Code.

- 3.1 gathering of information through point of sale terminals
- 3.2 randomly monitoring the activities of workers by means of CCTV cameras
- 3.3 randomly opening up individual workers emails
- 3.4 using automated checking software to collect information about workers. e.g. workers sending or receiving inappropriate emails
- 3.5 examining logs of websites visited to check that individual workers are not downloading pornography
- 3.6 keeping recordings of telephone calls
- 3.7 systematically checking logs of telephone numbers called to detect use of premium rate lines

- 3.8 videoing workers outside the workplace to collect evidence that they are not in fact sick
- 3.9 obtaining information through credit reference agencies to check that workers are not in financial difficulties

4.0 Core Principles

- 4.1 The Information Commissioner has identified the following Core Principles in the general approach to monitoring.
- 4.2 It will usually be intrusive to monitor your workers
- 4.3 Workers have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment.
- 4.4 If employers wish to monitor their workers, they should be clear about the purpose and satisfied that any particular monitoring arrangement is justified by real benefits that will be delivered.
- 4.5 Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified.

5.0 “Monitoring” in the College Context

5.1 CCTV Cameras

Whilst the College has installed CCTV cameras, there are no CCTV cameras installed to monitor employees at work. However in the interests of Health and Safety, security of College buildings, staff, students and visitors CCTV cameras are installed specifically to cover critical public areas, certain internal corridors, external pathways and car parks. Where cameras have been installed this has been clearly indicated.

5.2 Email

The College’s policy with regard to the use of the College email services and monitoring email is stated implicitly in the Email Policy contained within the Information and Communications Technology Policy and Procedures. and outline here below.

[Using the College E-Mail Service \(extract from Section D, Page 10 of the College ICT Policy\)](#)

5.2.1 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. The use of internet e-mail accounts will be subject to the provisions outlined in the Internet Access Policy.

5.2.2 Policy Statement

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

5.2.3 Using the College E-Mail Service

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

Jewel & Esk College has no interest in regulating the content of electronic mail 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, message of posting 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.

5.2.4 Monitoring of E-Mail

Jewel and Esk College reserves the right to monitor 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 Director of Human Resources.

5.3 Internet Usage

The College grants Internet access to all staff and contract staff authorised by the Human Resource Section and to all students who have completed the College's matriculation processes. The College's Internet Access Policy contained within the Information and Communications Technology Policy and Procedures states that the following recording takes place: user identification, terminal location, policy acceptance log on and off time, dates and sites visited. The only monitoring which takes place is a search on the log files looking for keywords that may indicate Internet abuse, such as Porn, Sex etc.

5.4 Telephone Monitoring

The College has a call log monitoring system in place. This software does not record telephone conversations but does record numbers called from individual extensions. The only monitoring undertaken is of calls made by external agencies such as ISIS English Language Schools who operate the College's summer language school. The purpose of this monitoring is purely to determine the cost of calls which the College reclaims from ISIS. In exceptional circumstances, such as an investigation undertaken as part of the College's Disciplinary Procedure or criminal activity is suspected the call log system may be interrogated.

6.0 Conclusion

- 6.1 College Management is committed to the continuous review of its Policies and Procedures to take account of changes in legislation and evolving best practice. Compliance with the Data Protection Act 1998 and Codes arising there from is regarded as an essential part of the College's Human Resources practice.
- 6.2 The College concurs with the Information Commissioner's recommendation as to importance of developing a culture in which respect for private life, data protection, security and confidentiality of personal information is regarded as the norm.