

Data Protection Policy in relation to Data Protection Act 1998



1. Introduction

The College collects and processes a range of personal data relating to members of staff and learners, for a variety of purposes related to employment and the learning experience. For example, this information can relate to the recruitment of staff and learners; continuing professional development for staff; ensuring learner progress and achievement is recorded and ensuring that members of staff are paid. Other examples include the collection of information relating to absence of staff and learners and information related to the application of formal College processes.

In addition, some information is recorded for the purposes of equal opportunities monitoring and to enable the College to meet its obligations to provide statistical report to the Scottish Funding Council and other bodies, and to comply with legislation.

With the ability to collect and process data comes a responsibility to ensure that this data is collected, used and stored appropriately. The College's processing of personal data is covered by the Data Protection Act 1998. The College recognises and complies with the principles specified in the Data Protection Act 1998. This policy sets out the College's data protection responsibilities and details the rights of individuals to request copies of their personal data, outlining the procedure by which such requests should be made.

2. Scope

This policy covers any individual about whom the College holds personal data and applies to data held both on computer and manual records.

3. Principles of Retention of Data

3.1 Personal Data

This describes data which relates to a living individual who can be identified from those data, and other information which is in the possession of, or is likely to come into the possession of, the data controller (See paragraph 3.4 below). Personal data includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

3.2 Sensitive Personal Data

This describes personal data which relates, for example, to an individual's racial or ethnic origin, sexual orientation or religion or belief. The College will process sensitive data on an individual only for the purpose of providing statistical analysis

of a group of applicants, staff or learners as part of the monitoring we carry out to establish the effectiveness of our Single Equality Scheme. Sensitive personal data, for example, race/ethnic origin, religious or political beliefs, sexual life, trade union information, medical conditions, criminal convictions or allegations of criminal offences, carry other conditions. Sensitive personal data may only be processed where the individual has given explicit consent; for purposes of performing any right or obligation; and to protect the vital interests of the individual.

3.3 Data Protection Principles

The Data Protection Act 1998 includes eight data protection principles of good information handling. These state that personal data will be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- kept for no longer than is necessary;
- processed in line with your rights;
- secure;
- not transferred to other countries without adequate protection;

In response to these principles, personal data will be held by the College for one or more specified and lawful purpose(s). Personal data will be used for the specific purpose only and will not be disclosed for any reason incompatible with that purpose. Personal data will be accurate and kept up to date. Personal data will not be kept longer than is necessary for that purpose and complying with any archive policy agreed by the College. Individuals will be entitled to access personal data without due delay or expense and will be advised where access to data is required by any other third party data user. The College will apply appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, personal data. In exceptional arrangements members of the Senior Executive Team may require wider access to address specific College needs.

3.4 Data Controller

The College is a Registered Data Controller (No. Z9194349) with the Information Commissioner. The Register of Data Controllers, which contains details of the classes of data processed by the College and the purposes for which this is used, can be searched online at www.ico.gov.uk.

3.4 Breaches of this Policy

Unlawful procurement, unfair processing, inaccurate information, unlawful disclosure, inadequate/irrelevant/excessive information are all breaches of this policy. Any abuses of this policy by a member of staff may result in action taken in accordance with the College's Staff Disciplinary Policy and Procedure.

4. Retention of Records

The College will retain staff records in accordance with the archive arrangements set out in the College's Retention Policy, copies of which are available on request from Human Resources. The Retention Policy is also available on the Staff Intranet.

The College will also retain student records and other corporate information in line with the College's Retention Policy, which sets out internal archive arrangements and any record keeping requirements set by the relevant statutory bodies.

5. Access by Existing and Former Members of Staff to Personal Data

An existing or former member of staff has the right to request access to his or her personal file whether held on computer or on manual record in accordance with the procedure detailed below and subject to the College's Retention Policy (Section 4 above).

An individual who wishes to request information or access to personal data held on computer or on manual record should write to:

Head of HR Services
Motherwell College
1 Enterprise Way
MOTHERWELL
ML1 2TX

Reasonable notice should be given when requesting access to personal data. The College will not charge a fee for access to data covered by the Data Protection Act if the request is no more than twice per year. If a member of staff wishes to access personal data on more than two occasions in any year, a fee of £10.00 per occurrence will be charged to the individual. The College is entitled to ask for such evidence as it may reasonably require to verify the identity of the individual making the subject access request, before any information is provided.

Where subject access is granted, the enquiring member of staff must view the file(s) in the presence of a member of Human Resources staff, subject to any third party confidentiality specified. The individual may request a hard copy of any information held in relation to him/her, in response to his/her subject request. The College will respond to requests promptly and within a period of 40 days. Where the request for access is made by a former member of staff, all information will be directly supplied in hard copy.

The College endeavours to keep personal data up-to-date and accurate, however, individuals have an obligation to notify Human Resources of any changes to personal details.

6. Access by Current and Former Learners to Personal Data

An existing or former learner has the right to request information or access to personal data whether held on computer or on manual record in accordance with the procedure detailed below.

A learner who wishes to request information or access to personal data held on computer or on file should write to:

Information Systems Manager
Motherwell College
1 Enterprise Way
MOTHERWELL
ML1 2TX

Reasonable notice should be given when requesting access to personal data. The College will not charge a fee for access to data covered by the Data Protection Act if the request is no more than twice per year. If a learner wishes to access personal data on more than two occasions in any year, a fee of £10.00 per occurrence will be charged to the individual. The College is entitled to ask for such evidence as it may reasonably require to verify the identity of the individual making the subject access request, before any information is provided.

Where subject access is granted, information from the College's Management Information System will be provided in hard copy. Where other information exists within Departments or Student Services the enquiring individual must view the file(s) in the presence of an appropriate member of staff, subject to any third party confidentiality specified. The individual may request a hard copy of any information held in relation to him/her, in response to his/her subject request. The College will respond to requests promptly and within a period of 40 days. Where the request is made by a former learner, all information will be supplied in hard copy

The College endeavours to keep personal data up-to-date and accurate, however, individual learners have an obligation to notify the relevant academic department of any changes to personal details.

7. Information requests from Third Parties

Requests for information concerning an individual should only be dealt with if in writing, on company-headed paper. If you receive an information request that relates to someone else within the College, or a client or customer, the member of staff should check with the individual prior to disclosing the information. When

a request for a reference is received, staff should also refer to the Reference Guidelines available on the College's Staff Intranet.

In exceptional circumstances and in an emergency situation an individual may respond to a telephone request by passing the information and contact details to the individual for whom the personal data is requested.

If information requested relates to another department or function, then the member of staff should contact the relevant manager and seek clarification. If there is any doubt that personal information can be disclosed in response to an information request, the request should be referred to a senior manager and where necessary the Director with responsibility for Human Resources or Head of HR Services should be consulted.

Unauthorised disclosure of an individual's personal data, in breach of this policy, may result in action taken in accordance with the College's Staff Disciplinary Policy and Procedure.

7.1 Requests from the Police and Law Enforcement Agencies

There is a particular exemption within the Data Protection Act 1998 relating to requests for access to personal information received from the police, law enforcement agencies and other bodies with statutory functions to detect or prevent crime.

Such requests should normally be made in writing and signed by someone of sufficient authority within the agency requiring the information.

If you receive a request from such an agency, you should consult with a member of the Senior Executive Team, Human Resources or the Head of Community and Learner Services, who will make the decision whether personal information can be released.

8. Freedom of Information (Scotland) Act 2002

The College is a public authority under the terms of the Freedom of Information (Scotland) Act 2002, which gives individuals the right to request information held by the College. This information is wider than an individual's personal data and permits individuals, whether or not they are a member of College staff or one of its learners to access information on the College's wider activities. Under the Act, the information will be provided unless it falls within certain exempted categories.

Further information regarding the Freedom of Information (Scotland) Act 2002 can be found within the College's Publication Scheme, which outlines the categories of information available and the method(s) by which this can be

supplied. The Publication Scheme is available to view on the College's website or by contacting the College's Freedom of Information Officer, to whom all requests for information under the Freedom of Information (Scotland) Act should be directed:

Freedom of Information Officer
Motherwell College
1 Enterprise Way
MOTHERWELL
ML1 2TX

Or by email to: acoulter@motherwell.co.uk

9. Training and Data Security

The College is responsible for ensuring secure access to personal data.

The College will provide information and training to members of staff on their rights and responsibilities with regard to data protection requirements and will ensure that staff who have access to personal data are aware of the regulations and procedures regarding disclosure

Individual members of staff required to handle sensitive data in the course of his/her employment at the College will have a confidentiality clause contained within his/her Written Terms and Particulars of Employment.

Access to sensitive personal data and personal data of College staff is strictly controlled and centralised in a secure area. Similar arrangements are in place for learners' personal data held within relevant academic departments and Student Services.

8. Monitoring and Review

Motherwell College will review this policy statement in line with College requirements in response to its statutory obligations and with reference to the College's Single Equality Scheme.

This policy has been updated in accordance with the Employment Practices Data Protection Code on Monitoring at Work in relation to Employment Records (Part 2), Monitoring at Work, (Part 3) and Information about Workers Health Code (Part 4).

POLICY INFORMATION -		
Date of origin:	Date of last review:	Proposed date of review:
2000	February 2009	October 2010