

DATA PROTECTION POLICY

Responsible Officer:	Registrar
Date of Issue:	February 2010
Review Date:	February 2013
Availability:	Staff Intranet

INDEX

1.	INTRODUCTION.....	3
2.	COLLEGE'S APPROACH.....	4
3.	EXTENT OF THE POLICY	4
4.	STATUS OF THE POLICY	4
5.	DESIGNATED DATA CONTROLLER.....	4
6.	COLLECTING, PROCESSING AND STORING PERSONAL DATA.....	5
	6.1 CONSENT	5
	6.2 PROCESSING SENSITIVE INFORMATION.....	5
	6.3 STAFF RESPONSIBILITIES	5
	6.4 DATA SECURITY.....	6
	6.5 LEARNER RESPONSIBILITIES.....	6
7.	RIGHTS TO ACCESS INFORMATION FOR STAFF & LEARNERS.....	6
	7.1 NOTIFICATION OF DATA HELD AND PROCESSED	7
	7.2 ACCESS TO INFORMATION FOR STAFF & LEARNERS	7
	7.3 EXAMINATION MARKS.....	8
	7.4 REFERENCES	8
8.	RETENTION OF DATA	8
9.	CONCLUSION	8
10.	APPENDIX 1	9
	10.1 Staff Guidelines For Data Protection	9
	10.2 Staff Checklist for Recording Data	11
11.	APPENDIX 2	12
	11.1 Data Retention Periods.....	12
12.	APPENDIX 3	14
	12.1 Standard Request Form For Access (Primarily For Learner Access	14
13.	APPENDIX 4	15
	13.1 Standard Request Form For Access To Staff Data	15
	13.1.1 Section A	15
	13.1.2 Section B	15
14.	APPENDIX 5	16
	14.1 Glossary Of Main Terms	16

1. INTRODUCTION

The College needs to keep certain information about its students, employees and other users for a number of different purposes including monitoring students' performance and achievements and it is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

The College collects "Personal data" on learners and staff. Personal data is information, which relates to living individuals (not companies) who can be identified from that information, whether or not in conjunction with any other information. Common examples of personal data which may be used by the College in its day to day business include names, addresses, telephone numbers and other contact details, CVs, performance reviews, salaries and statements of opinion or intention regarding individuals.

To comply with the law, Data Protection Act 1998, the personal data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

This policy explains how the College collects, stores retrieves and uses personal data and is written in accordance with the legislation provided by the Data Protection Act 1998 and its guiding principles. In summary, the data protection principles state that personal data shall:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for longer than is necessary for that purpose
- be processed in accordance with the data subject's rights
- be kept safe from unauthorised access, accidental loss or destruction
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Within the personal data there is some information that is considered to be "sensitive personal data". Sensitive personal data includes information relating to:

- race or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health or conditions;
- sexual orientation/behaviour; or
- information relating to the commission or alleged commission of any offence and any related court proceedings, including the disposal of or sentence in those proceedings.

A glossary of main terms is shown in Appendix 5.

2. COLLEGE'S APPROACH

The College's approach will be to develop an effective procedure that allows the Corporation to approve on an annual basis a Data Protection Policy and to monitor compliance with the policy through an annual statement.

Key components to the approach are that:

- The Corporation (Board of Governors) will have responsibility for approving the Data Protection Policy on an annual basis and overseeing the Data Protection management within the College as a whole
- The Principal and the senior management team will implement and support the policies approved by the Corporation
- The College will appoint a Designated Data Controller
- The Principal, senior management team, Designated Data Controller and Key Senior Managers will complete an annual review of the compliance to the Data Protection Policy and make recommendation to the Corporation through an annual statement
- Senior and middle managers will be responsible for encouraging good Data Protection management practice within their designated areas
- Key risk indicators will be identified and closely monitored through the College's Risk Management Group.

3. EXTENT OF THE POLICY

The Data Protection Policy covers all computerised and manual data processing relating to identifiable individuals. It not only includes information about individuals, but also options and intentions towards an individual such as are contained in curriculum team minutes, emails and references.

4. STATUS OF THE POLICY

It is a condition of employment that employees will abide by the rules, regulations and policies made by the College. Failure to comply with this policy can therefore result in disciplinary action.

Any member of staff or a student at the College, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller. If the matter is not resolved then a formal grievance should be raised in line with the existing College policy.

5. DESIGNATED DATA CONTROLLER

The College as a body corporate is the data controller under the Act. The Corporation is therefore ultimately responsible for implementation of the Act. However the College Registrar is the designated data controller named in the notification to the Data Protection Commissioner and is responsible for

- Maintaining the College's registration with the Office of the Data Protection Commissioner.
- Providing advice, guidance and direction on data protection issues within the College

6. COLLECTING, PROCESSING AND STORING PERSONAL DATA

6.1 CONSENT

With limited exceptions the College can only process personal data with the consent of the individual. If the data is sensitive, express consent must be obtained. This requires a positive voluntary act of consent, which must be informed. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This may include information about previous criminal convictions.

All prospective staff and students will be asked to sign their consent to process on the relevant College form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form will result in the offer being withdrawn.

6.2 PROCESSING SENSITIVE INFORMATION

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate/monitor other College policies, such as the sick pay scheme or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. Offers of employment or course places will be withdrawn if an individual refuses to consent to this.

6.3 STAFF RESPONSIBILITIES

All prospective staff will be asked to sign their consent to process on the relevant College form, regarding particular types of information when an offer of employment is made. A refusal to sign such a form will result in the offer being withdrawn.

All staff are responsible for

- checking that any information that they provide to the College in connection with their employment is accurate and up to date
- informing the College of any changes to information, which they have provided
- checking the information that the College will send out from time to time, giving details of information kept and processed about staff
- informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are at Appendix 1.

6.4 DATA SECURITY

All staff are responsible for ensuring that:

- any personal data held is kept securely – such as in a locked filing cabinet, drawer, room with restricted access and, if computerised, it must be password protected
- data stored on removable disks must be removed before disposal
- papers containing personal information are shredded before disposal
- databases are closed and workstations securely locked when leaving the computer
- personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

6.5 STUDENT RESPONSIBILITIES

All prospective learners will be asked to sign their consent to process on the relevant College form, regarding particular types of information when an offer a course place is made. A refusal to sign such a form will result in the offer being withdrawn.

All students are responsible for ensuring that:

- Personal data provided to the College is accurate and up to date.
- That changes of address, etc are notified to their Personal Tutor or Curriculum Administrators.

Students who use the College computer facilities may, from time to time, process personal data. If they do so they must notify the course tutor who should ensure the DP Policy is followed or seek guidance from the Data Controller.

7. RIGHTS TO ACCESS INFORMATION FOR STAFF & LEARNERS

Staff, students and other users of the College have the right to access any personal data that is being processed about them either on computer or in structured paper files. They are also entitled to a description of any such data held, details of the purpose for which the data is being, or is to be, processed and the details of any persons to whom the data may be disclosed. Individuals are also entitled to any information available about the source of that data.

7.1 NOTIFICATION OF DATA HELD AND PROCESSED

All staff, students and other users are entitled to know:

- what information the College holds and processes about them and why.
- how to gain access to it.
- how to keep it up to date.
- what the college is doing to comply with its obligations under the act.

The Notification and Register Entry can be viewed by accessing the Information Commissioners web link (College Registration Number is Z5677241)

http://www.ico.gov.uk/tools_and_resources/register_of_datacontrollers.aspx

Upon request the College Data Controller can supply a copy of the Register Entry.

7.2 ACCESS TO INFORMATION FOR STAFF & STUDENTS

If it is not possible to access information informally, or formally, during normal College business then any individual wishing to exercise their right to access information should make a request in writing to the College Registrar.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached in Appendix 4 of this document. The College will make a charge of £10 on each occasion that access is requested.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request. Any member of staff receiving a request in writing should pass this to the College Registrar immediately.

The data subject has the right to prevent personal data being processed, has rights in relation to automated decision-making, has the right to have inaccurate personal data corrected or erased and has a right to compensation for any damage caused by contravention of the Act.

When a valid access request is made the College will:

- Advise the data subject whether any personal data is being processed concerning them;
- If so, supply a description of that personal data, state the purposes for which it is being processed and the people or class of person to whom it may be disclosed;
- Disclose the information to the data subject; and

- Advise the data subject of the logic involved where a decision relating to, or significantly affecting, the data subject is made on the basis of processing that personal data by automatic means.

The College reserves its rights to refuse to fulfil access requests where permitted by the relevant legislation.

7.3 **EXAMINATION MARKS**

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide due to the time taken by awarding bodies to return and verify results.

7.4 **REFERENCES**

A reference is subject to the Data Protection Act and a data subject has a right to access this information.

8. **RETENTION OF DATA**

All personal data, including any information about health, race or disciplinary matters will be destroyed within our published minimum data retention periods (Appendix 2) unless there are specific requests and reasons not to.

9. **CONCLUSION**

Compliance with the 1998 Act is the responsibility of all members of Milton Keynes College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution.

For the purpose of this document, the terms "Governing Body" and "Corporation" should be interpreted as having the same meaning.

10. **APPENDIX 1**

10.1 **Staff Guidelines For Data Protection**

All staff will process data about students on a regular basis, when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on a day-to-day basis will be personal data rather than sensitive personal data and will cover categories such as:

- general personal details such as name and address,
- details about class attendance, course work marks and grades and associated comments.
- notes of personal supervision, including matters about behaviour and discipline (where this includes “health” information it will be treated as sensitive).

With limited exceptions information about a student’s physical or mental health, sexual life, political or religious views, trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student’s consent.

There may be instances where there is a need to record details such as dietary needs, for religious or health reasons prior to taking students on a field trip. If staff need to record this information, they should use the College standard forms.

Other permitted reasons to use sensitive personal data are when the processing is necessary:

- to exercise or perform a non-contractual legal right in connection with the data subject.
- to protect the vital interests of the data subject.
- in relation to legal proceedings or obtaining legal advice.
- or the data subject has already made the information public.
- for the administration of justice.
- for medical purposes or the information is about racial and ethnic origin.
- for the purposes of reviewing the existence of absence of equality of opportunity and treatment.

Despite the above, obtaining the data subjects’ express consent is always preferable.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in the College’s Data Protection Policy. In particular, staff must ensure that records are:

- accurate;
- up-to-date;
- kept and disposed of safely, and in accordance with College policy.

Staff will be responsible for ensuring that all data is kept securely.

It is the responsibility of the College and its staff to ensure the security of all personal data (whether held electronically or otherwise) extends to situations when such data is used away from the College's premises.

Staff should not remove personal data from college premises unless this is needed for work related activities. If data is removed then the appropriate Administrative Coordinator or Manager should be notified and all data must be returned the next working day.

If such personal data is used at home, then the same care should be taken as would be expected to apply to other "valuables".

If there were a need to access personal data from home then the preferred route would be via the intranet rather than removing it from College premises. Floppy and mobile disks should only be used to transport data in exceptional circumstances.

When personal data is used away from College premises, all staff must be extra vigilant regarding the security of such data, as the normal organisational security precautions cannot be called upon to assist.

In particular if personal data is used in a public place it should be kept under close supervision at all times and never left unattended (unless deposited in a secure place of storage).

If there is any doubt regarding the use of personal data in situations away from the College's premises, then guidance should be sought from the Data Controller.

The College will designate, where necessary, staff roles in each area as 'authorised staff', and this will be reflected in their job descriptions. These staff are the only staff authorised to hold or process data that is:

- Personal data; or
- Sensitive data.

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary:

- in the best interests of the student or staff member, or a third person, or the College; and
- he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

This should only happen in very limited circumstances, e.g. a student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

Staff must not disclose personal data to any student or other member of staff without the express consent of the data subject, or in accordance with College policy.

Staff must not disclose sensitive personal data to any person be it another member of staff or a member of the public without the express consent of the data subject unless one of the exceptions applies.

Before processing any personal data, all staff should consider the checklist:

10.2 **Staff Checklist for Recording Data**

- Do you really need to record the information?
- Is the information non-sensitive personal data or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student/employee been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data, and do you have authority to do this from a member of College Senior Management Team?
- Have you reported the fact of data collection to the authorised person within the required time?

11. **APPENDIX 2**

11.1 **Data Retention Periods**

The College will not keep personal information for longer than is necessary. The retention periods indicated below have a statutory basis and are minimum periods to satisfy the appropriate legislation. If a member of staff decides to retain personal information for longer than the periods indicated they must have a reason that is valid by reference to the Data Protection Principles and agree this in writing with the Registrar.

Type of Personal Information	Minimum Retention Period	Reasons
Personnel files including training records.	6 years from the end of employment.	References and potential litigation.
Staff application forms and interview notes for unsuccessful applicants.	6 months from the date of the interview.	Sex Discrimination Act 1975, Race Relations Act 1976 and Disability Discrimination Act 1995.
Income Tax and NI returns, including correspondence with tax office.	6 years after the end of the financial year to which the records relate.	Income Tax (Employment) Regulations 1993.
Statutory Maternity Pay records and calculations.	3 years after the end of the financial year to which the records relate.	Statutory Maternity Pay (General) Regulations 1986.
Statutory Sick Pay records and calculations.	Term of employment plus 40 years.	Social Security Contributions & Benefits Act 1952.
Wages and salary records.	Current year plus 6 years.	Taxes Management Act 1970, Limitation Act 1980, Equal Pay Act 1970, Minimum Wage Regulations 1998.
Accident books and records and reports of accidents.	Term of employment plus 40 years	Limitation Act 1980.
Health records.	During employment.	Management of Health and Safety at Work Regulations.
Health records where reason for termination of employment is connected with health,	Term of employment plus 6 years.	Limitation Act 1980.

including stress related illness.		
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1994.	Term of employment plus 40 years.	COSHH 1994, Control of Asbestos at Work Regulations 2002, Control of Lead at Work Regulations 2002, Control of Substances Hazardous to Health Regulations 2002.
Student records, including academic achievements and conduct.	Registered student relationship with College plus 6 years	Limitation Act 1980.
CCTV Security Tapes	30 days (unless investigation made and then as long as reasonably required for evidential purposes)	Potential investigation into incidents.
Contact details kept on personal files (e.g., card index, Microsoft Outlook).	Until it is apparent that the person is no longer at the named location.	It is inaccurate processing if the information is held any longer.
Personal information of any sort on a web page/site.	No longer than a period specifically agreed with the person.	Danger of inaccurate and irrelevant processing.

12. **APPENDIX 3**

12.1 **Standard Request Form For Access (Primarily For Student Access)**

To: The Registrar

I, _____ wish to have access to either

Please tick as appropriate:

All the data that Milton Keynes College currently has about me as part of an automated system and/or part of a relevant filing system;

or

Data that Milton Keynes College has about me in the following categories, please tick appropriate boxes below:

- Academic marks or course work details
- Academic or employment references
- Disciplinary records
- Health and medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc.
- Other information (Please specify below)

Notes:

- *Inspection of files will be by appointment only.
- *You will be required to bring with you some form of identification, preferably to include a photograph, for example a passport or photocard driving licence
- *An authorised person will be present whilst you look at the file.
- *You will not be permitted to remove anything from the file.
- *If you wish to copy any of the contents you must inform the authorised person who will arrange it for you.
- *You must describe the data you wish to access if held in a non-computerised manner.

I understand that I will have to pay a fee of £10

Signed _____

Dated _____

13. **APPENDIX 4**

13.1 **Standard Request Form For Access To Staff Data**

13.1.1 Section A

To: Human Resources Manager

From:

Post:

Department / Section:

Preferred Time(s) and Date(s) for Inspection :

I understand that I will have to pay a fee of £10

Signature: _____ Date: _____

Notes:

*Inspection of files will be by appointment only.

*You will be required to bring with you some form of identification, preferably to include a photograph, for example a passport or photocard driving licence

*An authorised person will be present whilst you look at the file.

*You will not be permitted to remove anything from the file.

*If you wish to copy any of the contents you must inform the authorised person who will arrange it for you.

13.1.2 Section B

Dear _____

An appointment has been made for you to inspect your personal file

on _____ at _____

Please report to _____ on arrival.

Signature: _____ Date: _____

14. **APPENDIX 5**

14.1 **Glossary Of Main Terms**

These are the main terms that are used throughout the Policy and are included here for easy reference,

The Act	The Data Protection Act 1998.
Authorised third party	An organisation that the College is required to share data with for the purpose of contract compliance.
Data	Any information, which will be processed or used on or by a computerised system. This can be written, taped, photographic or other information.
Data Controller	The organisation responsible for ensuring that the requirements of the Data Protection Act are complied with. (Milton Keynes College)
Data Processor	Any person other than a person employed by the College, who processes any data on behalf of the organisation. An external payroll provider will be an example.
Designated Data Controller	Individual appointed by the College to carry out the day-to-day duties of the Data Controller. (The Registrar)
Data Protection Officer	An official that may be appointed by the controller, in compliance with national law, to have the responsibilities, among other things, as listed in Article 18 (2) of the Directive in the Data Protection Act 1998. (The Registrar)
Data subject	As defined in the Directive at Article 2 of the Data Protection Act 1998 - an identified or identifiable natural person.
Data subject's consent	As defined in the Directive at Article 2 of the Data Protection Act 1998 - any freely given specific and informed indication of his/her wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed.
Notification	The process of informing the Commissioner that an organisation or an individual will be processing personal data other than for private use. This replaces registration under the 1984 Act.
Personal data	As defined in the Directive at Article 2 of the Data Protection Act 1998 – any information relating to an identified or identifiable natural person ("data subject").

Processing of personal data (processing)	As defined in the Directive at Article 2 of the Data Protection Act 1998 - any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Sensitive data	Data of a personal nature such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and concerning health or sex life; information relating to the commission or alleged commission of an offence or court proceedings is also sensitive personal data.
Subject Consent	Subject to certain exceptions before processing personal data, the College must have the agreement of the individual to do so. In the case of sensitive data, this must be specific consent, but in other cases, it can be more general.
Relevant Filing System	Any paper filing system or other manual filing system, which is readily structured so that information about an individual is readily accessible.
The Information Commissioner	Person Appointed by the government to administer the provisions of the 1998 Act including notification and to provide guidance and assistance to organisations and individuals.
The Data Protection principles	The underlying principles of the Act that determine what data can be collected, processed and stored. A failure to abide by the principles will be a breach of the 1998 Act.
The Data Protection Tribunal	The tribunal established to deal specifically with matters of enforcement under the Data Protection Act.
Third party	As defined in the Directive at Article 2 of the Data Protection Act 1998 - any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.