Contents

1. Introduction 3
3. People, Risks and Responsibilities 4
3.1 Policy Scope 4
3.2 Data Protection Risks 4
3.3 Responsibilities 5
4. Data Storage 5
5. Data Use 6
6. Data Accuracy 6
7. Subject Access Requests 7
7.1 Rights to access information for Staff and Learners 7
7.2 Access Information for Staff and Learners 7
8. Disclosing Data for Other Reasons 8
9. Providing information 8
10. Contact Details 8

1. Introduction

Metropolitan School of Business and Management UK (MSBM) needs to gather and use certain information about individuals. This can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

This data protection policy ensures MSBM:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and process individuals' data
- Protects itself from the risks of a data breach

The College needs to keep certain information about its learners, employees and other users for a number of different purposes including monitoring learners' 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.

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 learner 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

3. People, Risks and Responsibilities

3.1 Policy Scope

This policy applies to:

- The college
- All staff, members and learners associated with our qualifications
- All contractors, suppliers, consultants and other individuals working on behalf of us

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- E-mail addresses
- Telephone numbers
- Any other personal information

3.2 Data Protection Risks

This policy helps to protect us from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

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.

3.3 Responsibilities

Everyone who works for or with MSBM has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

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 learners' 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.

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 of a course place is made. A refusal to sign such a form will result in the offer being withdrawn.

All learners are responsible for ensuring that:

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

Learners 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 Data Protection Policy is followed or seek guidance from the Operations and Compliance Manager.

4. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Academic Director, who takes on responsibility for data protection.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for any reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard back up procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

5. Data Use

Personal data is of no value to us unless the business can make use of it. However, it is when personal data is accessed and used that it can be at greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by E-mail, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT Manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

6. Data Accuracy

The law requires us to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate and it is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- MSBM will make it easy for data subjects to update the information MSBM holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Marketing Manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

7. Subject Access Requests

7.1 Rights to access information for Staff and Learners

Staff, learners 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.

All individuals who are the subject of personal data held by MSBM are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by E-mail, addressed to the Operations and Compliance Manager at info@msbm.org.uk. The data controller can supply a standard request form, although individuals do not have to use this. Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

7.2 Access Information for Staff and Learners

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 Director of Operations.

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 and to ensure clarity please make every effort to use the standard form attached in Appendix 3 of this document. Confirmation of your identity will be required before any information is released hence the College in keeping with good practice would like to give the data subject an opportunity to arrange an appointment to review the details held. This would then allow security around the release of your information, give you an opportunity to review all the details held, enable you to be selective and take away only what's necessary to fulfil your requirements. Please note that 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 consult with the Operations and Compliance Manager 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.

8. Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, MSBM will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

9. Providing information

MSBM aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. The privacy statement is made available to all employees at MSBM.

10. Contact Details

If you have any queries about the contents of the Data Protection Policy, please contact our Administration team by any of the following mechanisms:

Telephone: 01908 303653

E-mail:

info@msbm.org.uk or alternatively please post

the form to: Academic Coordinator, MSBM

London, 29th Floor, One Canada Square, E14

5DY, Canary Wharf. London. United Kingdom |

Tel: +44 (0) 207 712 1588 | Fax: +44 (0) 207

712 1501.

Appendix 1: Staff Guidelines for Data Protection

Staff Guidelines for Data Protection

All staff will process data about learners 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 learners give their consent to this sort of processing, and are notified of the categories of processing, as required by the 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 learner'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 learner’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 learners 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.
- To protect the well-being of our students including children and vulnerable adults
- 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 has 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; and 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. Mobile disks such as USB sticks should only be used to transport data in exceptional circumstances. Sensitive data should be encrypted and a strong password will be required to protect any transported personal data.

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 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 learner 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 learner is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the learner is pregnant or a Jehovah's Witness.

Staff must not disclose personal data to any learner 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:

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 learner/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 learner 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?

Appendix 2: Data Retention Periods

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, including stress related illness.	Term of employment plus 6 years.	Limitation Act 1980.
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.
Learner records, including academic achievements and conduct. All documentation relating to the delivery of ESF in the 2007-2013 period must be retained until 2022 at the earliest.	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.

Appendix 3: Standard Request Form for Learner Access

Standard Request Form for Learner Access

The completion and submission of this form initiates the formal request to access personal information that MSBM holds for you. Individuals are encouraged to read the Data Protection Policy prior to initiating this request.

Date:	
Name:	
Learner ID:	
Contact number:	
E-mail address:	

Please tick as appropriate:
I wish to have access to:

- ☐ All the data that MSBM UK currently has about me as part of an automated system and/or part of a relevant filing system;

Or

- ☐ Data that MSBM UK has about me in the following categories, please tick appropriate boxes below Other (please provide further details):
- ☐ 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
- ☐ Other information (Please specify below)

If you are a learner, please provide the address to which correspondence should be sent	
If you are an employee please provide name, contact address and telephone number:	

Notes:
If an Inspection of files is required then it 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

Signature | Date of form submission | Click here to enter a date.

Please email the completed form to: info@msbm.org.uk or alternatively please post the form to: Academic Coordinator, MSBM London, 29th Floor, One Canada Square, E14 5DY, Canary Wharf. London. United Kingdom | Tel: +44 (0) 207 712 1588 | Fax: +44 (0) 207 712 1501.

For Office Use Only	**Date**	**By Whom**
Date form received		
Checked by Director of Operations		
Date of approval		
Date of confirmation letter sent to individual		
Updated on Systems		

Appendix 4: Standard Request Form for Staff Access

Standard Request Form for Staff Access

The completion and submission of this form initiates the formal request to access personal information that MSBM holds for you. Individuals are encouraged to read the Data Protection Policy prior to initiating this request.

Date:	
Name:	
Department	
Contact number:	
E-mail address:	

Please tick as appropriate:
I wish to have access to:

- ☐ All the data that MSBM UK currently has about me as part of an automated system and/or part of a relevant filing system;

Or

- ☐ Data that MSBM UK has about me in the following categories, please tick appropriate boxes below Other (please provide further 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
- ☐ Other information (Please specify below)

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

Notes:
*If an Inspection of files is required then it 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

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

Signature _____ Date of form submission Click here to enter a date.

Please email the completed form to: info@msbm.org.uk or alternatively please post the form to: Academic Coordinator, MSBM London, 29th Floor, One Canada Square, E14 5DY, Canary Wharf. London. United Kingdom | Tel: +44 (0) 207 712 1588 | Fax: +44 (0) 207 712 1501.

For Office Use Only	Date	By Whom
Date form received		
Checked by Director of Operations		
Date of inspection		
Date of confirmation letter sent to individual		
Updated on Systems		