DATA PROTECTION

POLICY

1. Policy Statement

1.1 The college will ensure that personal data is treated in a manner that is fair and lawful.

2. Purpose

2.1 The college is required to comply with:

a. The terms of the 1998 Data Protection Act, and any subsequent relevant legislation.

b. Information and guidance displayed on the Information Commissioner's Website (www.ico.gov.uk)

2.2 To ensure Compliance with the Act is the responsibility of all members of the college. Any breach of this Data Protection policy may lead to disciplinary action being taken, or access to the college's facilities being withdrawn, or a criminal prosecution. Any questions or concerns over the operation or interpretation of this policy should be addressed to the college's Data Protection Officer.

3. Need for data retention:

3.1 The college needs to keep certain information about staff, students and other individuals to allow it to, for example, monitor performance and achievement, and for health and safety reasons. The college must also process some of this information for various reasons, including complying with legal obligations to funding bodies and the government. To comply with the law the information must be used fairly, stored safely and not disclosed to any other person unlawfully.

4. Scope:

4.1 This policy relates to information about individuals that should not be made available to the public. It does not include any information that is already in the public domain; as such information is not covered by the 1998 Data Protection Act. All staff, students and other individuals are entitled to:-

- Know what information the college holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the college is doing to comply with its obligations under the 1998 Data Protection Act

4.2 They can gain access to this information by making a Subject Access Request.

5. Definitions

5.1 Data

Data can be in computer or paper form and is any system that is a "structured set of personal data" and the records can be "centralised, decentralised or dispersed". In effect this means all of BMet College Group's employee and student records.

5.2 Personal Data

Personal data is information that relates to a living individual who can be

identified from that information, either by itself or when used in conjunction with other information in the possession of, or that which is likely to come into the possession of, the Data Controller. This 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. By contrast, information about a person which is publically available, such as work contact details, does not fall under the scope of the Data Protection Act, although discretion may be required in certain circumstances with regards to information disclosure.

Personal Data might be on paper or held electronically (e.g. database, Word, Excel) or it might be a written document, a file, or a picture (e.g. a photograph or CCTV images).

5.3 Sensitive Personal Data

Sensitive personal data is information that could be used to discriminate against an individual or may cause them to be treated differently from others. Specifically this is information about: racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; Trade Union membership; physical or mental health or condition; sexual life; commission or alleged commission of a crime; proceedings related to the commission or alleged commission of a crime, the disposal of any such proceedings or the sentence of a court in relation to such proceedings.

5.4 Data Subject

The Data Subject is the living individual who is the subject of the data. This will include employees, students, contractors, suppliers, visitors and anyone else about whom the College collects personal data.

5.5 Data Controller

The Data Controller is the legal 'entity' who determines the purposes for which data is collected. In the case of BMet College Group, the college itself is the Data Controller rather than any specific individual(s).

5.6 Data Processor

Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

5.7 Processing

Processing of data is the collection, storage, use, disposal and dispersal of data.

5.8 Third Party

A third party is any person or entity other than the Data Subject, Data Controller or an authorised Data Processor.

5.9 Data Protection Officer

The Data Protection Officer is responsible for maintaining the College's registration with the Information Commissioner's Office and providing advice and guidance to assist in ensuring compliance with the Data Protection Act. The College's current Data Protection Officer is the Head of MIS.

5.10 Privacy Notice

This Notice is included on College Application/Enrolment Forms and normally on

other documents used to collect data to indicate how any data provided will be processed by the College and who it may be shared with.

5.11 Data Protection Notification
Details of our Data Protection registration held by the Information Commissioner's Office are available on the College intranet and the Information Commissioner's (ICO) website. The registered Notification contains a list of the types of data that the College is entitled to process.

6. Statutory Framework

6.1 The 1998 Data Protection Act sets out a number of Data Protection Principles which the college must comply with. These state that personal data must:

- Be obtained and processed fairly and lawfully and not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and 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

7. Other Related Policies and Codes of Conduct

- The Control of Records and Archiving Policy deals with storage, retrieval and destruction of records.
- The Freedom of Information Policy covers information available to the public.
- The ICT Acceptable Use Policies cover appropriate use of ICT.
- The ICT Access and Security Policy deals with data security.
- The CCTV Policy deals with use of CCTV images.

8. Principles

As a college we are required to take specific measures to ensure that all information (personal data) held about living individuals, in either paper-based or electronic format, is processed according to the eight Principles of the Data Protection Act.

These require that personal data must be:

1. Processed fairly and lawfully
2. Obtained and processed for specific and lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Held for no longer than necessary
6. Processed in accordance with the data subject rights

7. Kept safe from unauthorised access, accidental loss or destruction
8. Transferred outside the European Economic Area (EEA) only if adequate safeguards for personal data exist in that country

9. Rights to Access Information

9.1 Data Subjects have the right to access any personal data that is being kept about them on computer or in other paper files.

9.2 The Act allows individuals to:

- Obtain a copy of their own data
- Have inaccurate personal data corrected or erased
- Prevent data being used for direct marketing
- Opt out of any automated decision making processes
- Where appropriate, seek redress for any unwarranted damage or distress caused

9.3 The College will make an administration charge of up to £50 on each occasion that access is requested, although the College may waive this charge in certain cases.

10. Data Gathering

10.1 All personal data relating to staff, students or other people with whom we have contact, whether held on computer or paper-based, is covered by the Data Protection Act. This includes staff/student/parent records in our Management Information System, electronic files (such as spread sheets or Word documents) containing information about individuals (and print-outs of these), and hand-written information which would include entries in diaries, phone-call logs, minutes of meetings and mark books. Included are any written expression of opinion about an individual and any indication of the intentions of any person in respect of the individual. Where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data".

10.2 Only relevant and necessary personal data may be collected and the person from whom it is collected should be informed of the intended use and any possible disclosures of the information that may be made. Privacy statements will be included on any forms that are used to collect personal data, and fair processing notices will be issued to staff and students/parents annually.

10.3 In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained from the person it relates to. 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 includes information about previous criminal convictions.

10.4 For extensive information about the Data Protection Act follow this link Data Protection Guidance

11. Data Storage/Transfers

11.1 Personal data will be stored in a secure and safe manner.

11.2 Electronic data will be protected by standard password and firewall systems operated by the college. Staff should inform the college immediately if they can access something that they believe they should not be able to. Any electronic files on the network containing personal data must be stored in secure areas with restricted access. Any electronic files stored in shared locations must be encrypted with a strong password. All electronic documents should employ Protective Marking. All documents that contain sensitive/personal information should be marked as "OFFICIAL - SENSITIVE". For a more detailed explanation of how this works please follow this link: *Protective Marking*

11.3 Files containing personal information can only be stored in the cloud using a platform and account approved by the college. Personal accounts for drop box, google or other platforms are not considered to be secure and able to be controlled by the college and therefore must not be used.

11.4 The use of removable media devices such as memory sticks to store any sensitive or personal data is not allowed. Where it is necessary to move such information using physical media, prior approval should be sought from the data protection officer. Wherever possible, paper-based personal data should not be taken offsite. Where this is necessary, appropriate arrangements for secure transport and storage should be made and checked with the Data Protection Officer.

11.5 Work related e-mails should only be sent using work accounts and not personal ones. There should be no automated forwarding of e-mails to personal accounts. E-mails are an unsecure medium, and any personal data sent over e-mail should be encrypted, with the password sent in a separate e-mail or communicated verbally.

11.6 Computer workstations in public facing administrative areas will be positioned so that they are not visible to casual observers and should have privacy screens on their monitors. All staff and students should lock their computer whenever they leave it unattended for any amount of time. Passwords should not be shared with anyone.

11.7 Paper-based data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data, by being kept in a lockable cabinet/area. For example, STAR reports contain highly sensitive data on students and must be kept in a secure location and not shown to other students, parents or anyone outside the college. Paper-based personal data must not be displayed on interactive displays, walls or left on desks. It must be shredded when no longer needed. Like electronic documents, paper documents that contain personal data should use protective marking (see 11.2 above).

11.7 All paper waste containing sensitive information will be shredded. Shredders can be found in each central administration area. Some buildings will have additional shredders.

11.8 To comply with the seventh principle of the Data Protection Act, covering security:-

- All re-assigned ICT hardware will be re-imaged or re-set to factory defaults.
- All electronic waste items will have their data storage medium physically destroyed. For example, hard disks will be broken-up.

11.9 To avoid data loss, a back-up of the college's MIS data will be taken regularly and stored separately on an encrypted medium. For paper-based data, cabinet/area

keys must be kept secure and not shared with anyone who does not need to have them.

11.10 CCTV footage is classed as personal data, and it must be kept secure. Access to viewing of the footage must be strictly controlled and a log must be kept of people who have viewed any footage. Under subject access rules anyone has a right to view any CCTV images/footage which we have of them. For more detail see the College's CCTV Policy.

11.11 Telephone calls can only be recorded with the consent of the caller.

11.12 If students or other individuals do not want us to contact them unnecessarily then the appropriate flags should be used in the system and the individuals should not be contacted regarding the relevant thing that they have objected to being contacted about. For example, where we have flagged a student as not wanting to be contacted about courses and learning opportunities then staff must not contact them about with marketing messages about new courses.

12. **Data Checking**

12.1 It is the responsibility of staff and students to ensure that the information the college holds about them is accurate and up-to-date. On at least an annual basis students and staff will be given the opportunity to ensure that personal data held is correct and it will be the staff or student's responsibility to inform the college of any required changes.

12.2 Any errors discovered must be rectified and, if incorrect information has been disclosed to a third party by the college, that third party must be informed of the corrected data.

13. **Data Disclosures**

13.1 Personal data will only be disclosed to organisations or individuals to whom the Data Subject's consent for viewing the data has been given, or to organisations that have a legal right to receive the data without the Data Subject's consent being given.

13.2 When requests to disclose personal data are received by telephone it is the responsibility of the college to ensure the caller is entitled to receive the data and that they are who they say they are. It will be necessary to call them back, via a switchboard or other means of verification, to ensure that the possibility of fraud is minimised.

13.3 Personal data will not be used in newsletters, websites or other media without the consent of the Data Subject. Photos of students will only be used with their permission. Students are entitled to withdraw the permission at any time. Where a photo of a student is used either no name or the first name only should accompany the image.

13.4 Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which notifies the college of a specific, legitimate need to have access to personal data. It must be signed by the requesting officer and show their rank. It must also clearly state the nature of what is being investigated.

13.5 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate. The record should be signed and dated.

14. **Subject Access Requests**

14.1 If the college receives a valid request from a Data Subject to see any or all personal data that the college holds about them this will be treated as a Subject Access Request and the College will respond within 40 calendar days (unless there is a valid reason to take longer in which case we will write to them). The college will, if necessary, ask the Data Subject for proof of identity. If the disclosure contains data relating to a third party then the college will follow the advice from the Information Commissioner's Office.

14.2 Verbal requests from a Data Subject to view or have copies of their personal data will be dealt with wherever possible at a mutually agreed time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the college will comply with its duty to respond within the 40 calendar day time limit.

14.3 A signed and dated record of the Subject Access Request disclosure should be kept.

15. **Concerns**

15.1 Any student, parent or member of staff who feels that this policy has not been followed in respect of their personal data should initially raise the matter with the college's Data Protection Officer.

16. Procedures

16.1 Almost all staff will process data about students on a regular basis. The information that staff deal with on a day-to-day basis will be standard and will cover categories such as:

- General personal details such as name and address
- Details about class attendance, coursework marks and grades and associated comments
- Notes of personal supervision, including matters about behaviour and discipline

16.2 Information about a student's physical or mental health; sexual life; political or religious views or trade union membership is sensitive and can only be collected and processed with the student's consent. If staff need to record this information, they should use the appropriate form, where a form exists, and only approved staff should record such information. Examples include recording information about dietary needs, for religious or health reasons prior to taking students on a trip and recording information that a student is pregnant, as part of personal tutor duties.

16.3 The college will designate staff in each area as authorised staff. These are the only staff authorised to hold or process data that are:

- Not standard data, or
- Sensitive

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

- To protect the vital 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, for example; a student is injured and unconscious, but in need of medical attention and a tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

17. Individual Staff Responsibilities

17.1 All staff have a duty to make sure that they comply with the data protection principles, which are set out in this policy. In particular, staff must ensure that records are:

- Accurate
- Up-to-date
- Fair
- Kept and disposed of safely, and in accordance with the college's policy

17.2 Authorised staff will be responsible for ensuring that all data is kept securely. Staff shall not disclose personal data to any other staff member, student or anyone else, except with authorisation of the data subject, or in line with the college's policy. Before processing any personal or sensitive data, all staff should consider the Staff Checklist for Recording Data below.

17.3 If in any doubt, and the situation is not an emergency, then staff should seek guidance from the college's Data Protection Officer.

18. Training and Communications

18.1 All staff that have a regular need to record, process or review personal information as part of their substantive role will be provided with initial training as part of their role specific induction, and will receive refresher training on an annual basis. This includes, but may not be limited to staff in the Data and Information, Student Services, HR and Finance teams.

18.2 All other members of staff will be briefed on this policy, and provided with a copy of a checklist, as part of their corporate induction, and will receive an annual communication to remind them of the importance of the policy and its associated guidance.

18.3 Specific training will be provided where required, for example when there is a significant change to the technologies available to store and process data.

Staff Checklist for Recording Data

- Do not store personal or sensitive information on portable media including memory sticks or portable hard disc. Only store personal data in the cloud using the approved platform and your college username and password.
- Remember that students, staff and parents are entitled to see almost all information that we hold about them. If they make a request to see that data it could include E-mails about them, information in student monitoring systems including ProMonitor.
- Lock your computer screen when you are not there using the Ctrl Alt Del Enter function.
- Protect your passwords, do not share them. Make them secure by using non-alphabetic characters and symbols.
- Documents that contain sensitive information should be stored in secure areas and be password protected. For example Microsoft Office has a Protect Document function from the File menu.
- Paper based documents such as attendance printouts must be kept securely in locked cabinets when not in use.
- All documents should only be shared with those that should see them.
- Paper documents that are no longer required must be shredded. Reprographics, administration hubs and some other departments have shredders.
- Do not send sensitive information in E-mails. This includes, for example, when communicating with other organisations that process data such as the Learner Records Service.
- Do not put the names of students on published photos of them.
- Do not put personal information in newsletters, or any other public documents.
- Information can only be given to the police with the use of specific paperwork. A WA170 form should be provided by the police showing the nature of the crime and the appropriate authorisation. If in any doubt do not provide information and contact the Data Protection Officer.

The consent to process information that is needed for day-to-day operations is obtained at enrolment. Examples include: marking work, marking attendance registers and writing reports and references. If you are collecting non-standard information the below checklist can act as a quick reference guide.

- Are you authorised to collect/store/process the data? If unsure speak to the college's Data Protection Officer
- If so do you really need to record the information?
- Is the information standard or is it sensitive?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- 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 vital interests of the student or the staff member to collect and retain the data?
- Have you reported the data collection to the authorised person within a reasonable time?