DATA RETENTION AND DISPOSAL POLICY

POLICY OWNER:	Data and Information
AUTHOR:	Mike Lewis
DATE OF APPROVAL:	January 2022

GDPR requires that Colleges should not keep personal data for longer than is necessary. This policy aims to set out the College's data retention periods that need to be adhered to by all members of staff.

Once personal data is no longer needed, it should be securely deleted/destroyed in accordance with the retention period set. Personal data needs to be destroyed securely and all different types of media on which the data is stored need to be considered.

1. POLICY STATEMENT AND SUMMARY

BMET College must, in respect of its processing of personal data, must be compliant with the General Data Protection Regulation (EU) 2016/679 as it applies to the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR") and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018 (together, "Data Protection Laws").

This Retention Policy should be read in conjunction with the College's Data Protection Policy and IT and Social Media Usage Policy, which sets out the College's overall approach to data protection matters and sets out the rationale for why a Data Retention and Disposal Policy is required for personal data. You must also comply with these Related Policies. Any breach of this Policy may result in disciplinary action.

The College is under a legal obligation only to keep personal data for as long as the College needs it. Once the College no longer needs personal data, the College must securely delete it. The College recognises that the correct and lawful treatment of data will maintain confidence in the College and will provide for a successful working environment.

All College Personnel must comply with it at all times. If you have any queries regarding this Retention Policy, please consult your manager and/ or the Data Protection Officer. College Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All College Personnel areobliged to comply with this Policy at all times.

This Policy sets out how the College complies with our legal obligation not to keep personal data for longer than we need it and sets out when different types of personal data will be deleted.

All records generated as part of College operations must be appropriately stored to enable auditing of the systems, processes, claims and accounts, retrieval of records for other purposes and to meet legal requirements.

The College will retain a document based on the following 5 principles:

1. **The document or record still has a use or business purpose.**
    a. Where the College still has a use for a document and/or record, it should be retained until it is no longer of use.

2. **There is an applicable Statutory Minimum Retention Period or the document is a legal record**
    a. In some cases statute law has set specific minimum time periods for retaining certain documents and/or records.

b. Legal records include contracts and property deeds.

3. **The document or record is relevant to an outstanding claim or current litigation, arbitration or investigation**
    a. If a document and/or record is relevant to an outstanding or likely claim, arbitration or litigation, the document and/or record must be retained.

4. **The document or record has evidential value for a possible claim, litigation, arbitration or investigation**
    a. A reviewer should consider whether any document and/or record could be used to support or oppose a position in an investigation, arbitration or litigation.

5. **The document is subject to Audit**
    a. Where a document and/or record is or might be required for an audit, it must be retained until the audit right has expired.
    b. Where a document is required to be kept for a specified period in accordance with a contractual requirements (for example to satisfy the College's obligations under the Funding Rules of the Education and Skills Funding Agency)

2. RESPONSIBILITIES AND OBLIGATIONS

This Policy applies to all College employees, consultants, contractors and temporary personnel hired to work on behalf of the College ("**College Personnel**").

All College Personnel with access to personal data must comply with this Data Retention and Disposal Policy.

The College has a corporate responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment.

The Director of Data and Information has overall responsibility for organisation archives and procedures for the preparation, transport and storage of archive materials.

Departments responsible for records have responsibility for the preparation of archive materials that meet agreed standards, and for maintaining records of what has been archived.

Individual employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the College's records management guidelines.

Management staff will ensure that any documents that fall within their responsibility are stored appropriately and destroyed in the appropriate manner at the appropriate time. Confidential documents must be shredded or destroyed in a suitable way.

All staff will ensure that records they are responsible for are kept safe, in organised systems, and with appropriate security arrangements. All staff are expected toensure that records they have access to are not left in open, public or unsecured areas without appropriate physical security.

All staff will ensure that records for archiving are prepared appropriately, following the published guidance on sharepoint under Data Management, and are clearly labelled using an approved archive label.

Estates staff will ensure that only properly prepared archive boxes are accepted for archiving, and that these are packed and secured prior to transport. They will ensure that archive materials are processed taking due account of their potential academic or financial value, and are stored properly to allow for subsequent retrieval.

Department managers are responsible for ensuring that all staff are aware of this Policy and comply with its requirements.

All members of staff are responsible for ensuring that their work is documented appropriately and that the records which they create or receive are managed correctly. They also have a responsibility to know what information they hold and where it is held.

3. RECORDS MANAGEMENT

Records are a means of providing evidence of activities which support the business and operating decisions of the College. They can be in any format.

Examples of different types of records include:

- CCTV recordings
- Emails
- Property files
- Staff files
- Minutes
- Financial records
- Diaries

What Is Not A Record?

Not all information is necessarily a formal record. Types of information that are not records include:

- information relating to personal or social activities;
- books, magazines, periodicals etc. held for reference purposes;
- stocks of printed publications and publicity materials retained for supply purposes; and
- duplicate copies of records held for convenience or personal reference and where the master set of the records has been identified and retained elsewhere.

4. DATA RETENTION PERIODS

The Data Retention and Disposal Policy is based on the model recommended for Further Education Institutions by JISC in **Annex A**.

The College periodically assesses the types of data that it holds and the purposes the College use it for. ***It is intended that this policy will be regularly updated to reflect and incorporate new and additional record categories.***

If any member of College Personnel considers that a particular piece of data needs to be kept for more or less time than the period set out in this policy, please contact the Data Protection Officer for guidance.

The record retention schedule provides a mechanism to help ensure the College is maintaining necessary records for an appropriate length of time.

Retention of Email

Saved emails should be regularly reviewed and information that is no longer necessary to retain should be deleted.

Some records contain information that is required only for a limited time to ensure a routine action is completed or a subsequent record is prepared.

Such emails should be deleted as soon as they are no longer of use.

Examples are:

- copies of reports, newsletters, or information used only for convenience of reference;
- correspondence produced for information purposes;
- meeting notices and arrangements, cover letters;
- working drafts that are not required to document the steps in the evolution of a document; and
- routine enquiries or correspondence.

Some emails can even be destroyed immediately as they do not provide any corporate value. These are:

- internal email messages received as cc or bcc messages;
- personal emails, jokes, adverts, spam and other unrelated to work emails;
- social communications –lunch dates, leaving events, fundraising events, etc.;
- general announcements, calendar items and reminders; and
- email captured threads of later messages.

Where current records are generated and stored electronically, there is no need for printed copies to be retained or archived.

5. DISPOSAL

Destruction of documents can only take place after the expiry of the minimum storage time as detailed in **Annex A**. Destruction of documents must take place shortly after the expiry of the minimum storage time except in circumstances where it is relevant to keep records, is approved by the Director of Data and Information, and is recorded as an exception to the College policy. Such cases include those where documents are being used in connection with an ongoing case, investigation, audit or dispute. In such cases, the records should be removed from the organisation archive and stored in alternative secure storage to prevent being included in routine review and disposal of records.

Confidential Disposal

Any information on identifiable individuals or commercially sensitive information should be treated as confidential. This needs to be disposed of in a secure manner sothat information does not get disclosed to third parties.

Dispose of unwanted paper documents that do not contain any confidential information by recycling.

Where documents contain confidential information, place the documents in one of the confidential waste cabinets at strategic places on each campus. For staff that are working at satellite sites the documents shouldplace documents in a confidential red shredding bag and store the bag securely until it is collected for shredding by Estates.

The College has a corporate confidential shredding contract with offsite waste management; Estates will make arrangement for the confidential waste to be collected. The confidential waste will be stored in a locked room until the shredding company collect it for secure disposal. A certificate of disposal will be provided once the records have been securely destroyed, which Estates will retain.

A record cannot be considered to have been completely destroyed until all copies including backup copies, have been destroyed, as there is a possibility that the data could be recovered. Records held electronically are subject to the same retention periods as paper records. Remember, in the case of electronic records, multiple copies are likely to exist. Ensure that **all** copies are destroyed.

IT Service desk should be contacted if you have any IT equipment that needs to be disposed of. Until it is collected it should be kept in a secure place.

Authority for Disposal

When your boxes reach the end of the retention period that was set when they went into the archive room, ARM (Archiving and Records Management team) will contact you to inform of their pending destruction. You will need to consult the Corporate Retention Schedule to check if the retention guidance has changed since the records went into storage. If you believe that the records should be retained then you should inform the ARM team and Data Protection officer within one month of receipt of the notification. If no changes have occurred, ARM team will make arrangements with the Estates team destroy the records securely 3 months after the notification being sent to you.

6. PROCEDURE/COMPLIANCE OBLIGATIONS

All records management processes must comply with legislative requirements particularly the Data Protection Act 2018 and the Freedom of Information Act 2000. This requirement also applies to outsourcing arrangements for any recordsmanagement activities. As the College remain responsible for its outsourced activities, it is important to ensure that contractors are aware of their responsibilities under the Act and manage their records accordingly.

When appointing third party contractors the following requirements must be met:

- Select a reputable organisation offering suitable guarantees about their ability to ensure the security of personal data.
- Make sure the organisation has appropriate security measures in place and appropriate checks on their staff.
- The contract makes specific provision for record keeping requirements and compliance measures.
- The contract should also require the organisation to report any security breaches or other problems, and have procedures in place to allow you to act appropriately.

ANNEX A - Records Retention and Disposal Guidance.

The College periodically assesses the types of data that it holds and the purposes the College use it for. ***It is intended that this policy will be regularly updated to reflect and incorporate new and additional record categories.***

Please click on this link to view JISC Records Retention and Disposal Guidance.