BESA’s Records Management Policy

This Policy sets out the principles for ensuring that BESA knows what information it holds, where it is, and can retrieve and distribute it efficiently. It applies to all records – whether paper or electronic – created or used by staff, and supersedes all local records management policies.

**1) Aims**

BESA’s records are a vital corporate asset: they provide evidence of its actions and decisions, and must be managed actively and systematically to ensure transparency, accountability and legal compliance.

The principal aims of records management at BESA are to:

* protect the interests of BESA, its staff, members and other stakeholders by maintaining high quality information for as long as it is required, and to ensure its timely and secure destruction
* comply with statutory and regulatory requirements affecting the use and retention of records
* support decision making, teaching and research by maintaining accurate and reliable documentation
* support business efficiency and continuity by ensuring information can be quickly located and retrieved and protecting information that is vital to the continued functioning of BESA
* provide evidence in litigation
* prevent unauthorised or unlawful disclosure of information by ensuring records are held securely and access is controlled and managed
* maintain the corporate memory by preserving records of historical significance.

To measure performance and improvement, BESA will use the international standard for records management, ISO 15489, and the Lord Chancellor’s Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (2009).

**2) Responsibilities**

Each department must have in place adequate systems for documenting its principal activities and ensuring that it creates and maintains records possessing ‘authenticity, reliability, integrity and usability’ (ISO 15489).

BESA’s Directors have overall responsibility for records management. Operational responsibility is delegated to the Communications and Website Manager, who is responsible for developing records management procedures, advising on good practice and promoting compliance with this Policy.

Line managers are responsible for ensuring that their 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) Record management systems**

Each department must have in place adequate systems for documenting its principal activities and ensuring that it creates and maintains records possessing ‘authenticity, reliability, integrity and usability’ (ISO 15489).

There must be a clear allocation of responsibility within each department for all aspects of record-keeping, including classifying documents and secure disposal. The ownership of information must also be clarified, so that there is no ambiguity regarding responsibility for its maintenance and disposal. Shared drives, mailing lists and role accounts should be used as a default.

Line managers should ensure that when a member of staff leaves, responsibility for records held on personal drives or other areas not accessible to colleagues is transferred to another member of staff; and out of date information deleted.

Records systems must be adequately documented, so that their effective operation does not depend on the memory of individual members of staff. They should also be periodically reviewed, and modified where necessary, to ensure that they continue to support local needs.

In particular, electronic systems storing data that may be required for evidential purposes should be regularly monitored and audited: it must be possible to demonstrate the reliability of the system, so that the integrity of the data cannot be questioned.

**4) Creating records**

Records must be accurate and complete, so that it is possible to establish what decisions and actions have been taken, and why. The quality of the records must allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met.

Information should be compiled at the time of the event or transaction to which it relates, or as soon as possible afterwards, and protected from unauthorised alteration or deletion. Where relevant, templates should be used, so that documents are produced consistently and quickly.

Standardised referencing and titling are essential, so that information can be promptly identified and retrieved. Naming conventions and glossaries should be used to ensure the consistent use of terms. Version control is also required for the drafting and revision of documents, so that different versions can be distinguished and the latest version readily identified.

**5) Classification**

All records – whether paper or electronic – must be organised logically, so that they can be easily and speedily retrieved. A classification scheme or filing structure should be devised, based on an analysis of a department’s functions and activities, to ensure that documents are organised appropriately and consistently. Similar records should be grouped together: if the contents of folders are too diverse, it will be difficult to locate material and assign appropriate retention periods.

**6) Access and security**

It must be possible for staff to retrieve the information they need to carry out their work. Paper records that are consulted frequently should be kept close at hand within the immediate office space.

Records must be made available as widely as possible. Information that other staff use or may require must be stored on a shared drive or within a centralised filing system, so that departments can operate efficiently when individuals are absent. Where appropriate, data should also be shared across BESA in order to avoid wasting resources recreating information that already exists and storing duplicate data unnecessarily. Information that is only accessible to a single person should therefore be kept to a minimum.

Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. Paper records containing confidential information must be stored in locked cabinets or rooms when not in use, and access only provided to authorised staff. Screens should be locked when computers are unattended Restricted electronic data should be protected through the use of access controls and, where appropriate, encryption.

Information held in digital systems must be also protected from accidental or unauthorised alteration, copying, movement or deletion: if possible, the systems should maintain audit trails allowing all actions to be to be traced to specific people, dates and times. It is essential that any data held on portable storage devices, such as laptops, USB flash drives, portable hard drives, CDs, DVDs, and any computer not owned by BESA, is kept secure and protected from theft.

The integrity of electronic data is of paramount importance, if it is considered the primary, definitive record of a transaction. Departments that are responsible for storing documents required for evidential purposes should aim to comply with the British Standards Code of practice for legal admissibility and evidential weight of information stored electronically.

**7) Preserving records**

All BESA’s departments should develop procedures to ensure that records of continuing value remain accessible, usually on a network drive or central server, so that they are backed up and safeguarded from hardware and software failure.

Records must be stored in conditions appropriate to their medium and format, taking into account operational needs, retention periods and costs. They should be protected in storage from potential hazards, such as fire and flood, and environmental conditions within storage areas must be maintained at stable levels to minimise the risk of the records deteriorating.

Records should be reviewed at regular intervals, usually annually. Where necessary, electronic records should be converted to newer formats and migrated to other systems, so that they are always accessible and usable. Processes should also be in place to protect documents from being inadvertently overwritten, for example, by using templates when creating new versions of documents.

**8) Disposal**

Records should be reviewed regularly and working copies, trivial emails, out-of-date reference material and unnecessary duplicates destroyed to prevent ephemeral material taking up space required by declared records.

Disposal of records, both paper and electronic, is controlled by the retention schedule, and carried out by authorised staff. When the retention period expires, all copies should be destroyed, wherever they are held. Destruction should also be documented, to provide evidence that retention schedules have been followed and to prevent searching for material that no longer exists.

Restricted or sensitive records must be destroyed confidentially and kept secure whilst awaiting destruction. Electronic data must be deleted so that it is completely erased and

Records must not be destroyed if they are required in connection with an on-going or pending investigation, grievance, complaint or legal dispute.

**9) Email**

Emails record actions and decisions, and must be managed as effectively as paper and other electronic records. Messages should be arranged in a record-keeping system to allow information to be easily located and retrieved, and regularly reviewed and deleted according to the retention schedule.

Email is merely a format and messages cannot be treated as a uniform series with a single retention period. Retention should be determined by the subject matter or business purpose, as for any other record.

**10) Vital records**

Records that would be vital to the continued functioning of BESA in the event of a disaster (e.g. fire, flood, virus attack) must be identified and protected. These include records that would recreate BESA’s legal and financial status, preserve its rights, and ensure that it continues to fulfil its obligations to its stakeholders (e.g. current financial information, contracts, proof of title and ownership, research data).

Vital records must be stored on central servers, so that they are protected by appropriate back-up and disaster recovery procedures. Vital records that are only available in paper format should be duplicated, and the originals and copies stored in separate locations. If, however, duplication is impracticable or legally unacceptable, fire protection safes must be used to protect the documents.

This policy has been adopted as part of BESA’s participation in the EDUCATE programme, and developed to ensure alignment with UCL’s policy on the matter.

**Last updated: May 2018**