GBS GLOBAL APPLIED KNOWLEDGE

GBS Records Management Policy

Introduction

1. GBS recognises that efficient and effective management of its records is necessary to support its core functions and activities, to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution.

2. GBS Records Management Policy sets out the principles that support GBS in discharging its records management obligations. These legal obligations include, but are not limited to, the: Freedom of Information Act 2000, the Environmental Information Regulations 2004, the General Data Protection Regulation 2016, the Data Protection Act 2018 in addition to GBS's own regulations. The policy is supported by guidance and a list of legislation, standards and Codes of Practice (not exhaustive) in relation to the management of records at GBS which are displayed on its records management webpage.

3. This policy also makes provision for how records (and the data and information they contain) are managed at GBS . The terms data and information have a wide variety of uses and are defined in numerous different ways across society and it is therefore not within the scope of this policy to invent potentially limiting definitions for these areas.

4. In instances when data and information are captured in a tangible form (e.g. in an MS Word document or MS Excel spreadsheet) they can benefit from management throughout their lifecycles to ensure that best use is made of them as assets and to ensure that they meet the compliance requirements of the environment they exist within. The discipline of records management assists with the systematic control of the: creation, receipt, maintenance, use and disposition of data and information throughout its lifecycle in the form of records.

5. To aid with the management of data and information as records at GBS this policy provides a definition of a record and makes provision for its lifecycle management. The policy adheres to the definition of a record as set out in ISO BS 15489:1 2016 (Information and documentation – Records Management). This standard defines a record as: 'information created, received and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in the transaction of business'.

6. ISO BS 15489:1-2016 also sets out that 'Records, regardless of form or structure, should possess the characteristics of authenticity, reliability, integrity and useability to be considered authoritative evidence of business events or transactions and to fully meet the requirements of the business'. To these ends this policy sets out six principles that make provision for the management of records throughout their lifecycle with the aim of ensuring that a consistent approach is taken to their administration at GBS.

7. GBS ’s Records Management Policy contains two parts. Part 1 sets out the policy and Part 2 makes provision for its supporting principles and processes.

CONTENT CONSIDERATIONS

• The public has a general right of access to:

o the recorded information held by GBS under the Freedom of Information Act 2000;
o Environmental Information under the Environmental Information Regulations 2004;
o A data subject’s own personal data under the General Data Protection Regulations 2016 and the Data Protection Act 2018;
o access in line with the provisions of any other legislation that provides a right of access to information.

N.B. In each case access is granted unless an exemption applies under each of these access regimes.
• This means that: email correspondence, physical documents, electronic documents (digitised/ born digital), microfiche, sound and audio visual records (this list is not exhaustive) could be in scope of an information access regime (I.E. each access regime has specific requirements of what is in scope of its provisions).

• It is important that data, information and records created, or held at GBS are managed in line with the provisions of the Information Security Framework (of which the policy forms a part).

• The information you create is representing GBS and therefore its content should be in line with GBS’s vision and values.

Part 1 – The Policy

Scope of the Records Management Policy

8. This policy applies to all records that are created, received or held in any format (e.g. physical, digitised or born digital) within a GBS system or within a physical store during their lifecycle. This includes records relating to teaching and research activities, as well as commercial and administrative support functions.

9. Records exist in a wide variety of formats and can include, but are not limited to, paper-based documents and files, electronic documents (including e-mails), spreadsheets, presentations, databases, clinical data, medical records, photographs, microfiche; social-media, webpages, film, slides, video and in electronic (digital) or (physical) hard copy format.

10. GBS Records Management Policy is published on GBS's Records Management internet pages and demonstrates GBS's commitment to taking forward the good practice recommendations in the Code of Practice on Records Management issued under section 46 of the Freedom of Information Act 2000 which includes that 'Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy'. GBS Records Management policy forms part of GBS's Information Security Framework.

Roles and responsibilities

11. GBS's Executive Board is responsible for ensuring that systems are in place to meet all of GBS's legal obligations, including the establishment and monitoring of systems of control and accountability. The CEO and MD are the principal academic and administrative officers of GBS and hold a general responsibility to the Executive Board for maintaining and promoting the efficiency and good order of GBS.

12. In relation to Records Management the Resources Committee is responsible for:

• Ensuring that Records Management policies, procedures and guidance align with GBS's IT Security Policy;

• Ensuring that GBS Records Management policy is kept up to date and that it is relevant to the needs and obligations of GBS;

• Developing appropriate Records Management guidance to underpin the policy;

• Communicating guidance on Records Management within GBS;

13. GBS's Head of Programme Management, and the team of Programme Managers, have delegated responsibility for taking forward the programme of records management work set out at paragraph 12. Likewise, Academics are responsible for implementing Records Management Practices and training and the sharing of this policy will be a mandatory part of all GBS staff induction.

14. In relation to wider responsibility for the management of information (including records) the relevant section of GBS's IT Security Policy sets out that:

• Everyone granted access to GBS information assets (e.g. email, teaching and learning materials, staff/student information, financial information, research information, and the systems used to process these) has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the Policy. Failure to adhere to the mandatory requirements of the Policy could result in disciplinary action.

• Everyone is responsible for protecting GBS's information assets, systems and IT infrastructure, and will protect likewise those belonging to third parties but used in the course of their work at GBS. Protection of GBS or third party information and assets could be required contractually, legally, ethically or out of respect for other individuals or organisations.

15. The complete provision with regard to responsibilities within the IT Security Policy can be found within the Policy and other associated policies.

Core principles of GBS Records Management

16. The management of records at GBS is based on six principles which adhere to the 'keeping records to meet corporate requirements' provisions set out in the Lord Chancellor's Code of Practice on the management of records and 'principles for managing records' specified in the British Standard BS ISO 15489-1:2016 'Information and documentation – Records management'.

17. The six principles for the management of records at GBS are:

1. The record is accurate: GBS has the information that is needed to form a reconstruction of activities or transactions that have taken place.

2. The record can be accessed: information can be located and accessed by those with the authority to do so and the authoritative version is identifiable where multiple versions exist.

3. The record can be interpreted: the context of the record can be established: who created the document and when, during which business process, and how the record is related to other records.

4. The record can be trusted: the record reliably represents the information that was actually used in or created by the business process, and its integrity and authenticity can be demonstrated.

5. The record can be maintained through time: the structural integrity of the record can be maintained for as long as the record is needed, perhaps permanently (and in line with the provisions of GBS Records Retention schedule) despite changes of format.

6. The record is valued: the record is understood to be an information asset and provision is made to ensure that the principles of accuracy, accessibility, interpretation, trustworthiness and (physical/digital) continuity are upheld throughout its lifecycle.

Part 2 - Processes and procedures

Capture and control of records

18. All digital records created or received during the course of GBS business must be maintained during their lifecycles at GBS within established GBS information systems. N.B. If there is uncertainty about the use of any information system then ensure this is clarified before its use with GBS IT Services.

19. Digital records should be captured within a GBS information system as soon as possible after creation so that they are readily available to support GBS´s business. ‘GBS business’ is defined as ‘any activity conducted either in the course of employment or as part of or related to a GBS course or other GBS activity that is not purely personal’. If digital records are taken out of recordkeeping systems (e.g. printed) they must be managed in accordance with GBS’s Information Classification and Handling Procedure.

20. All digital records systems must be designed and implemented to ensure that the six Records Management principles and the provisions of the IT Security Policy are adhered to for the entire lifecycle of the record. Where a records system is being replaced or superseded by another system the records management principles and the wider information security framework must be adhered to. Where a records system is to be decommissioned, provision must be made for maintenance or transfer of the records so that they remain accessible for the required retention period.

21. All physical records created or received during the course of GBS business must be maintained in accordance with GBS's Information Classification and Handling Procedure's – Handling Paper or other media and guidance on the storage of physical records as set out in GBS policy.

Email

22. Emails may contain actions and decisions and must be managed as effectively as other digital information. Email messages that need to be seen by others for business reasons should be stored in a shared GBS Information system with the appropriate access controls in place to ensure that only those who are authorised to see them have access. This process helps ensure that the information emails contain can be located and retrieved and regularly reviewed and deleted when that is the appropriate action.

23. Email is a format and messages cannot be treated as a uniform record series with a single retention period. Retention considerations should be determined by the subject matter the email contains and with reference to GBS Records Retention Schedule.

Vital records

24. 'Vital records' are defined as any record that would be vital to ensure the continued functioning of GBS in the event of any incident that interrupts its normal operation. Such records should be identified by a Head of a Department. These include, but are not limited to, any records that would recreate GBS '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, HR).

25. Digital 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 physical format should be digitised (where possible) or duplicated and the originals and copies stored in separate locations. (The duplicates should be clearly marked as a copy of an original record.) If, however, duplication is impracticable or legally unacceptable, fire protection safes must be used to protect the documents.

Naming records

26. To ensure that records remain useable and can be located when required to fulfil business objectives they should be named consistently following: GBS guidance on naming conventions or if applicable the specialist naming conventions in use within a specific professional sector.

27. Where it is absolutely necessary that the naming convention contains personal data or other sensitive information particular attention should be given to its protected storage arrangements in line with GBS'sIT Security Policy.

Classification, storage and handling of records

28. To ensure that the core principles of records management are adhered to, all GBS information must be classified, stored and handled in accordance with GBS's information classification scheme.

29. Records require storage conditions and handling processes that take into account their specific properties. GBS will produce and maintain guidance on the storage of records on its records management internet pages.

Digitisation

30. In instances where digitisation is considered by GBS then all processes associated with this activity must adhere to this policy and GBS's IT Security Policy and consideration given to the provisions of: BS 10008: 2014 Evidential weight and legal admissibility of electronic information – Specification.

31. If the original physical record is to be destroyed post-digitisation then the digitised rendering needs to be able to be managed as the authoritative record throughout its lifecycle and disposed of, or preserved, in line with the provisions of GBS's Records Retention Schedule and IT Security Policy.

N.B. whilst in certain instances digitisation might help reduce physical storage space requirements through the disposal of the hard copy record, on other occasions it may not be appropriate to destroy the original post digitisation. An example of this might be where the record has intrinsic value (e.g. historical) in its original physical format or the digitised image is not able to be relied on as the authoritative record.

Access to records

32. The Content Considerations section of the introduction to this policy sets out the main access regimes that apply to GBS records. In terms of internal access to records then in each case it must be for a valid and authorised business reason.

33. Those creating and or storing records must ensure that adequate controls are in place to protect records from unauthorised access, disclosure, alteration and

Disposal of records

34. GBS manages the lifecycle of its records in line with its GBS's Records Retention Schedule (RRS) and IT Security Policy. The RRS is a tool that helps us to uphold our UK and EU data protection obligations by making provision for the time periods for which common types of records are retained by GBS.

35. It is recommended that academic and administrative departments and all other business units regularly review (e.g. at the minimum on an annual basis) their entries in the RRS to ensure they reflect the records that they work with and also put in place processes to ensure that disposal actions are carried out in relation to specific records at the appropriate time.

36. The disposal of information and records, as codified in GBS RRS, also adheres to the practices that the Lord Chancellor's Code of Practice on the management of records, issued under section 46 of the Freedom of Information Act 2000, sets out that it would be desirable for the relevant authorities to
follow in connection with the keeping, management and destruction of their records.

37. The RRS is a living document and is subject to ongoing review and development at GBS. If on accessing the RRS it is found that the schedule does not make provision for a type of record then this should be brought to the attention of GBS's Resource Committee Chair to consider its potential inclusion in the RRS.

38. The act of disposing of a record must be carried out in line with the provisions of GBS' IT Security Policy with special consideration given to records that contain sensitive information or personal data. Disposal of records without due care and attention to these procedures risks causing harm and distress to individuals and reputational damage and significant fines to GBS.

Preservation of records

39. The RRS also makes provision for the selection and preservation for certain categories of record created in any format at GBS to be transferred to any future records centre and therein preserved. These records form part of GBS's archive for historical research purposes and are the enduring record of its functions and activities.

Where to go for help

40. If you require any advice, training, team briefing or a presentation on any aspect of this policy, please contact GBS Resources Committee Chairman in the first instance. (info@globalbanking.ac.uk)

Maintenance

41. This policy will be reviewed by the GBS Resources Committee no less than every three years. Any amendments or additions will be submitted to GBS’s Resources Committee for approval. The next review is scheduled for 2022.

END