Global Banking School
+44 (0) 207 539 3548
info@globalbanking.ac.uk
www.globalbanking.ac.uk
891 Greenford Road, London
UB6 0HE

GBS Data Management and Classification Policy

Contents

3.3.6. Line Managers: Responsible for ensuring that their staff are aware of this policy and comply with its requirements. Ensuring that their staff have completed all required training in Data Protection. Ensuring that activities requiring a Data Protection Impact Assessments (DPIA) are referred to the DPO. Ensuring that requests made under data subject rights are referred to Human Resources/DPO ensuring that suspected or actual compromises of personal data are reported immediately. Managers can ensure accurate disposal or updating of records when a staff member leaves the business by:

Creating and maintaining accurate, authentic, and reliable records appropriate for their role

Implementing a comprehensive offboarding process that includes a checklist for record disposal or updating.

Ensuring these records are held on GBS systems and hardware.

Providing training and guidance to staff on proper record management procedures

Application of good practice, including naming conventions and version control and classification

Use of the GBS Records Retention Schedule so that records are only kept as long as they are required, and destroyed securely

Completion of mandatory training

Establishing a centralised system for records management, making it easier to track and update records.

Maintaining open communication channels with staff to ensure they report any changes or updates to their records

4. Classifying Information

4.1. Information classification is the process of analysing and labelling data and information (digital, paper or otherwise) according to the impact a compromise of its confidentiality, integrity and/or availability would have on GBS. The greater the impact, the higher the classification.

4.2. Classification enables efficient processing of data. If data is not explicitly classified, it should be classified as confidential pending classification by default to avoid data leakage. By accurately labelling data in combination with appropriate controls for sensitive data, greater compliance and security will be achieved, without creating excessive operational friction.

4.3. In the case of disagreement over the classification level to be used, the highest level should be adopted. This also applies where an integrated set of data comprises content of varying classifications.

4.4. Automatic technical controls may be implemented to assist staff with maintaining appropriate controls for sensitive data, but where these have not been, staff are responsible for complying with this policy.

5. Information Classifications

5.1. GBS has five information classifications to help staff identify the level of security the

It is possible for the sensitivity and value of one piece of data or information to change over time. The Information Asset Owner should review the data/information regularly to ensure that its classification remains valid.

6. Legislation and Compliance Framework

6.1. The public has a right to access our records under legislation such as the Data Protection Act 2018 and UK GDPR and the Limitation Act 1980. Although GBS, as a private company is not subject to the Freedom of Information Act 2000 and the Environment Information Regulations 2004, our academic partners are, and if requested we are contractually obligated to respond to any enquiries from them in a timely manner. Effective records management is therefore needed to enable us to meet our statutory obligations.

6.2. Data Protection Act 2018 ensures that GBS is a registered Data Controller and is required to process personal data in accordance with the principles set out in the Act. The A

6.6. In accordance with the ISO 15489, GBS will implement best practices for the creation, organisation, maintenance, and disposal of our records since compliance will help improve our efficiency, mitigate risks, and meet legal and regulatory requirements. The standards below also apply:

BS EN 15713:2009. This Standard provides the framework for securely collecting, handling, storing, and disposing of confidential waste.

BS 10008:2020. This standard details what users need to do to manage electronically stored information (ESI) in such a way that it retains its authenticity and integrity.

7. Record Management Standards

7.1. Records Management is the process of managing records, in any format or media type, from creation through to disposal. This policy applies to all records that are created, received, or held in any format (e.g., physical, digitised or born digital) within GBS system or within a physical store during their lifecycle.

7.2. Records 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, 5.56 si6(l)5(s))-3(,)6( )-101(s

8.2. **Quality**

8.2.1. The quality of the records must be sufficient to allow staff to carry out their work efficiently, demonstrate compliance with statutory requirements, and ensure accountability and transparency expectations are met. The integrity of the information contained in the records must be beyond doubt; it should be compiled at the time of the activities to which it relates, or as soon as possible afterwards, and be protected from unauthorised alteration or deletion.

8.3. **Templates**

8.3.1. Where appropriate, templates should be used, so that documents are produced consistently. In addition, version control procedures must be used for the drafting and revision of documents, so that staff can easily distinguish between different versions and readily identify the latest copy.

8.4. **Duplicates**

8.4.1. GBS strongly discourages the practice of maintaining duplicate records, -7(i)5(ci)5e0000088(ng)3( )-417(du)3(t4 r9)]TJ34(est)8( )-4(cop)h57 Tm0 g0 G[-7(i)5.04 Tf1 0 .5

8.10.1. 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. These include, but are not limited to, any records that would recreate GBS' 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).

8.10.2. 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

contents of each individual record to avoid the risk of records being destroyed or lost. Where it is necessary that the naming convention contains personal data or other sensitive information, particular attention should be given to its protected storage arrangements.

9. Classification, storage, and handling of records

9.1. To ensure that the core principles of records management are adhered to, all Data must be classified, stored, and handled in accordance with *GBS Information Classifications* (Please refer to Annex 2 and 3).

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

10. Digitisation

10.1. In instances where digitisation is considered by GBS then all processes associated with this activity must adhere to this policy and related policies and consideration given to the provisions of BS 10008: 2014 Evidential weight and legal admissibility of electronic information specification.

10.2. If the original physical record is to be destroyed post-digitisation, then the digitised rendering needs to be managed as the authoritative record throughout its lifecycle and disposed of, or preserved, in line with the provisions of Annex 5 GBS Records Retention Schedule.

10.3.

records must ensure that adequate controls are in place to protect records from unauthorised access, disclosure, and alteration.

12. Retention

12.1. Retention periods are based on the requirements of the Data Protection Act 2018 and UK General Data Protection Regulation. GBS manages the lifecycle of its records in line with our GBS Records Retention Schedule and IT Security Policy. The Retention Schedule is a tool that helps us to uphold our UK data protection obligations by making provision for the time periods for which common types of records are retained by GBS.

12.2. The Retention Schedule is a live document and is subject to ongoing review and development. If the schedule does not make provision for a type of record, then this must be brought to the attention of Academic Registrar's Office to consider its potential inclusion in the Retention Schedule.

associated with retaining records beyond their required retention period.

12.6. Information Asset Owners must agree retention periods for the information assets which they are responsible for, using the Retention Schedule, and these must be set out in the Information Asset Register. The Retention Schedule includes the following information:

12.7. *Record function, activity, and record group*

12.8. *Retention period* - The recommended length of time for which records should be kept by GBS. The retention period is often expressed as a starting point plus number of additional years to be kept, though permanent retention may be advised for some records.

13. Review

13.1. All records must be reviewed before a decision is taken about their disposal. A check must be made using the appropriate records management system to establish the status of the information prior to disposal.

14. Disposal of Records

14.1. Records will be disposed of in accordance with agreed Retention Schedules. They will set out the minimum period for which a record should be retained and will be reviewed regularly and amended, as necessary. Retention periods will be agreed by Information Asset Owners. When the currency of the records and their need to be retained expires, the records will either be destroyed, or if they have lasting historical value, added to the archive.

14.2. The act of disposing of a record must be carried out in line with the provisions of GBS ICT 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 could lead to reputational damage and significant fines to GBS.

15. Security and Access

15.1. Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. Records must be stored in a safe and secure physical and digital environment taking account of the need to preserve important information in a usable format enabling access commensurate with frequency of use.

15.2. GBS Access Control Policy outlines the rules relating to authorising, monitoring, and controlling access to GBS information systems and assets.

16. Audit and Compliance

16.1. GBS Records Management and Retention Policy may be amended by GBS at any time. This policy is reviewed by Information Management Group (IMG) and approved by the Board of Directors.

17. Alternative Format

17.1. This policy can be provided in alternative formats (including large print, audio and electronic) upon request. For further information, or to make a request, please contact the Academic Standards and Quality Office at asqo@globalbanking.ac.uk.

Annex 3 - GBS Information Handling Requirements

Below are handling requirements based on assigned classifications (annex 2 above), including storage, access, exchange, and disposal.

	Duplicates and digital hard copies should be avoided where possible in favour of links to digital repositories with managed access. Physical (hard copy) information should not be brought or stored at home or away from GBS

Annex 4 - GBS Records Disposal Form

RECORDS DISPOSAL FORM						
Department:						
Information Asset Owner *(name and role):*			**Email:** **Telephone:**			
Record title/description:						
Record format:						
Classification: *(tick as appropriate)*	**Public:**		**Private:**		**Confidential:**	
	Restricted:		**Internal:**			
Reason for disposal:						
Method of disposal: *(tick as appropriate)*						

NB: Records must not be destroyed if any Freedom of Information or Data Protection request, litigation, claim, negotiation, audit, administrative review, or other action involving the relevant information is initiated before the expiration of the retention period.

They must be retained until completion of the action and the resolution of all issues that arise from it, or until the expiration of the retention period, whichever is later. Once completed, a copy of this form must be retained by the relevant Information Asset Owner.

Annex 5 - GBS Records Retention Schedule

Examples of Information Assets from the GBS Records Retention Schedule.

Student Administration and Progress	Student Administration and Support	The core academic record of a student.	This is the minimal record kept to provide references for former students and may be retained for the lifetime of the student (80 years). A core (minimal) transcript may be retained indefinitely after this time and transferred to the archive if the institution has one. This depends on the requirements of the individual institution and their archival facilities/policies. The core record may vary according to the policy of each institution but is likely to contain name and dates of study, modules studied, and the qualifications conferred.	Sector norms/Institutional business requirements/Institutional charter/Institutional memory and archival requirements.
Planning and Operation	Corporate Planning & Performance Management and Strategy	Records documenting the development and establishment of the institution's corporate planning and performance management policies and strategy documents.	Superseded + 10 years	Institutional business requirements.
Legal and		Legal records documenting the		

Health and Safety