Contents

Annex 1

Global Banking School Records Management and Retention Policy

1. **Purpose and Scope**

    1.1 Global Banking School (GBS) is committed to the efficient management of our records in compliance with legislative, regulatory, and best-practice requirements. The principles outlined in this policy have been developed to provide a consistent approach to managing records throughout their lifecycle and provides guidance on the retention and disposal of records held by GBS. Retaining records for the right length of time is necessary to support business requirements and to comply with legislation.

    1.2 Effective Records Management allows for fast, reliable, and secure access to records ensuring the timely destruction of redundant records as well as the secure identification and archiving of records considered worthy of permanent preservation. Records management is defined by International Standard (ISO BS 15489: 2016) as:[1]

2. Roles and Responsibilities

2.1. GBS has a corporate responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment. All records should have an identified owner responsible for their management whilst in regular use, and for appropriate retention and disposal. Individuals or roles must be identified within departments to take responsibility for records or record sets and fulfil the role of Information Asset Owner. There must be no ambiguity regarding responsibility for the maintenance and disposal of records.

2.2. It is vital that records management considerations are appropriately incorporated into project and planning processes and system design at the earliest possible stage of development. Where records contain personal data, there is a legislative requirement to do this to ensure that a data protection by design and default approach is followed. GBS recognises that there must be a clear allocation of responsibility within each department to assist with the management of records. Therefore, the roles and responsibilities include:

2.3. GBS Senior Management Team: Responsible for ensuring that systems are in place to {^^óæ|Á-ÑÕÓÙq̨^*æ|Áà|ã̃æ̧̨}•Ȩ̣̂&|̆ å̧̃*/ó@-Á•cæ̧̃æ|ã@̧^}óæ̧̧̃åÁ[}ã[¦ã̧̃*Á-Áˆc^{•Á of control and accountability. They must ensure staff are made aware of this policy and must develop and encourage good information handling practices within their areas of responsibility.

2.4. GBS Academic Registrar has overall responsibility for records management within GBS. This includes the implementation, oversight and management of information and records management and retention policy on a day-to-day basis.

2.5. Information Commissioner's Office ("ICO"): ICO is the independent regulatory office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act and advises businesses on how to comply with UK GDPR and therefore requires every data controller who is processing personal information to register with the ICO.

2.6. Line Managers: Responsible for ensuring that their staff are aware of this policy and

comply with its requirements. They should ensure that when a member of staff leaves, responsibility for their records is transferred to another person; if any of the information is redundant, it should be deleted by either the departing member of staff or their line manager.

2.7. All GBS Members: (including staff, academics, associates, contractors, temporary staff, and any students who are carrying out work on behalf of GBS) are responsible for ensuring that their work is documented appropriately, that the records which they create or receive are accurate and managed correctly and are maintained and disposed of in accordance with ÕÓÙq guidelines and any legislative, statutory, and contractual requirements.

2.8. GBS Academic Standards and Quality Office (ASQO)[2]: Responsible for monitoring, and review of this policy. They must ensure that this policy is kept up-to-date and that it is relevant to the needs and obligations of GBS. and can be contacted on asqo@globalbanking.ac.uk.

2.9. In relation to the wider responsibility for the management of information (including records), the relevant section of GBS ICT 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.

2.10. Everyone is responsible for p¦[c^&c} * ÁÕÓÙq information assets, systems, and IT infrastructure, and will protect those belonging to third parties. Failure to adhere to the mandatory requirements of the policy could result in disciplinary action.

3. Legislation and Compliance Framework

3.1. The public has a right to access our records under legislation such as the Data Protection Act 2018 and UK GDPR, The Limitation Act 1980, The Freedom of Information Act 2000, and the Environment Information Regulations 2004. Effective records management is therefore needed to enable us to meet our statutory obligations.

---

[2] *Formerly known as GBS Quality Assurance Team*

3.2. Data Protection Act 2018 ensures that GBS is a registered data controller and is required to process data in accordance with the principles set out in the act. The act states that [¦*æ}ã ææ¦}•Á˘•oÁ[oÁ¦[&^••ÁÇ @&@Áã &¦ å^•Á‰ý¦cæä +DÁ^¦•[}æÁåæ}æÁ{¦Áæ}^Á[}*^¦Á c@æ}Áãaˆ˘ãˆˆã^å¦}Áˇ¦ãÁ˘•ã^••oÁ^^å•ÈÁIt also grants individuals the right to request personal data held about them by GBS and to object to how this data is being used.

3.3. In the event of a Subject Access Request (SAR) being made, we must search for, copy,

> *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.

4.3. Records must be maintained and stored in such a way that they can be easily identified and located to support business activities and that ensures appropriate accountability.

5. Record Processes and Procedures

5.1. Creating Records

5.1.1.   All digital records created or received must be maintained during their lifecycles. Each department must have in place adequate systems for documenting its principal activities. The records must be accurate and complete, so that it is possible to establish what has been done and why.

5.2. Quality

5.2.1.   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 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.

5.3. Templates

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

5.4. Duplicates

5.4.1.   The retention of duplicate records presents enhanced risks regarding their management, use and alteration. Whereas there may be a need to keep local

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. Th1o0 595.3(ce8 r-3(e)-5, s)-0.000008874 0 dn0.44 46.o/F3 10.98 Tf

Clear and well defined.

Convey an idea of the content that is understandable.

Identifiable . specifying the type of document, e.g., minutes, contract; draft; final, will assist access.

Concise - avoiding repeating information that can be gleaned from the name of the folder in which the file will be stored will assist access; and

Consistent naming - enabling ease of reference.

5.11.2. Without naming conventions, the context of the record becomes meaningless to anyone other than the creator, creating the unnecessary need to explore the 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.

7.3. 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.

8. Access to Records

8.1. The Legislation and Compliance Framework section of this policy sets out the main access regimes that apply to GBS records. In terms of internal access to records, it must be for a valid and authorised business reason. Those creating and/or storing records must ensure that adequate controls are in place to protect records from unauthorised access, disclosure, and alteration.

9. Retention

9.1. 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 its GBS Records Retention Schedule (RRS) and IT Security Policy. The RRS 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.

9.2. The RRS is a living document and is subject to ongoing review and development. If upon 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 Academic Quality Standards Office to consider its potential inclusion in the RRS. The Freedom of Inf(l)-2Inf(l)-2Ingnf(l)5(f)58ETQq0.0(

by subsequent legislation or organisational instructions.

9.5. Records that are no longer live (i.e., not in active use) are sometimes referred to as archive records. Retention periods apply to records in whatever format they are created/held. Retention and destruction of electronic records must be managed as well as those held on paper and follow the same rules.

9.6. It is recommended that academic and administrative departments and all other business departments 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 put in place processes to ensure that disposal actions are carried out in relation to specific records at the appropriate time.

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

9.8. *Record description* . The type of record or asset, applying to all formats of record.

9.9. *Retention period* - The recommended length of time for which the 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 it can permanent retention may be advised for some records.

9.10. *Record Owner* . The Division, sub-division, or other high-level area of GBS that owns the record and is ultimately responsible for its retention and disposal. The Record Owner is respon(thseib)5(lpn-4( )-30(for G[the)-2(im)10(pe3(araReten)-3(tio)-328)-105(or G[thi30(for sec)-3(a

13. Related Policies

13.1. Records management does not exist in isolation. It connects to functions such as management of personal information for compliance with the Data Protection Act, information security, and information assurance. This policy is accompanied by the Staff Handbook and must be followed to achieve GBS policy objectives. Reference should also be made to the

Annex 1

A circular records management lifecycle diagram with five stages:

- **(1) CREATE** — Create or receive information
- **(2) USE** — Use and handle in accordance with Data Protection Act
- **(3) RETENTION** — Maintain closed records in compliance with retention schedules
- **(4) REVIEW** — Determine whether records are worthy of permanent archival preservation.
- **(5) DISPOSAL** — Dipose appropriately, ensuring record of destruction is kept.