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

Document title	GBS Data Management and Classification Policy
Version	V5.1
Approved by	Information Management Group (Audit and Risk Committee)
Policy lead (Staff member accountable)	Data Protection Officer
Date of original approval	7th June 2024
Date of last review	Dec 2024
Changes made at the last review	Merger of the GBS Data Classification and Handling Policy with the GBS Records Management and Retention Policy (June 2024) Minor editorial changes (Dec 2024)
Date effective from	Dec 2024
Date of next review	June 2026

Related policies
▪ GBS Data Protection Policy ▪ GBS Data Breach Policy ▪ GBS Privacy Policy ▪ GBS Data Subject Access Request Policy ▪ GBS Access Control Policy ▪ GBS Email Usage Policy ▪ GBS CCTV Policy and Procedure
External Reference
1. Information Commissioner's Office, Accessed online at: https://ico.org.uk/ 2. UK Public General Acts, *Data Protection Act 2018*, Accessed online at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted 3. The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

Contents

Global Banking School Data Management and Classification Policy

1. Purpose and Scope

1.1 Global Banking School (GBS) needs to collect, store and process personal data about its staff, students, and other individuals it has dealings with, to carry out its functions and activities. GBS is a controller for most of the personal data it processes and is committed to full compliance with the applicable data protection legislation, including the Data Protection Act 2018 and the United Kingdom General Data Protection Regulation (UK GDPR).

1.2 GBS must retain data in the form of records, physical or digital, as part of its obligation to statutory and regulatory authorities, and for the delivery of services to GBS customers/students. Data in this context refers to all forms of records. For GBS, most records are in digital form, but physical records, whether stored physically or scanned, are also covered by this Policy. (Definitions for Data, Information, and Records can be found in Section 2).

1.3 This policy outlines types of data processed at GBS, types of records held, provides instruction on the classification to be applied, and how it may be handled. Without appropriate classification and labelling, data may be inconsistently managed. This may lead to sensitive data being processed in inappropriate ways.

1.4 GBS records are a vital corporate asset and GBS is committed to the efficient management of our records in compliance with legislative, regulatory, and best-practice requirements. GBS shall retain ownership of all records, documents, and materials created or obtained in the course of providing educational services, except for records held on behalf of other parties or loaned to GBS.[1] 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.

1.5 Effective records management allows for fast, reliable, and secure access to records

[1] *Further information can be found on our GBS Intellectual Property and Commercialisation Policy*

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 reviewed and confirmed 2021) as encompassing the following:[2]

a) creating and capturing records to meet requirements for evidence of business activity;

b) taking appropriate action to protect their authenticity, reliability, integrity and useability as their business context and requirements for their management change over time.

1.6 A key aim of this policy is to make clear the entire 'lifecycle' of record retention, from the point of creation, receipt, through the period of its active use, then into a period of inactive retention (such as archive files which may still be referred to occasionally) and finally either disposal or permanent preservation. This includes records relating to teaching and research activities, as well as commercial and administrative support functions. (Please refer to Annex 1 to view our Lifecycle of a record flow chart).

2. Definitions

2.1. "**Data**" are unorganised, collected facts and figures that have little meaning alone without appropriate filtering and processing.

2.2. **"Information**" is a processed and interpreted form of data that is comprehensible and meaningful to the observer, this can then be used to make informed decisions.

2.3. "**Records**" make up any practical information, digital or physical, that supports the organisation. These include documents, files, and communications that evidence an activity or retained information.

2.3.1. As an example of the distinction between data, information, and records: Measuring the population of a town over time would be data, determining if the population has changed over time would make it information, logging this in a central repository and updating it over time would make it a record.

2.4. "**Information Asset**" is a body of information, defined and managed as a single unit so it can be understood, shared, protected, and utilised effectively. Information assets have recognisable and manageable value, risk, content, and life cycles.

2.5. **"Information Asset Owners (IAOs)"** are named senior individuals responsible for each identified information asset, including physical repositories, databases, and IT systems within their remit. Defined IAOs should be at the appropriate business level within their respective departments. IAOs make up the division, sub-division, or other high-level area of GBS that owns a record and is responsible for its retention and disposal. They are responsible for the implementation of their section of the Retention Schedule, although operational practice may rest within other areas, requiring close collaboration, including ensuring that all Information Asset Owners are aware of their requirements of the Retention Schedule and apply accordingly. This may include auditing compliance.

2.6. **"Senior Information Risk Owner (SIRO)"** is an appropriately senior individual, typically at the executive level, accountable for ensuring that information is handled appropriately within the organisation and for taking ownership of information risk policy. The SIRO acts as an advocate for information risks to the Board of Directors and is expected to understand how corporate and academic strategic goals may impact information risks and vice versa.

2.7. **"Data Protection Officer (DPO)**" under UK GDPR, if an organisation's core activities involve large scale processing of special categories of data, or regular and systematic monitoring of individuals, a DPO must be appointed.[3] The DPO monitors internal compliance with UK GDPR and other data protection laws, guides data protection policies, informs and advises the organisation on its obligations, and acts as a point of contact for the Information Commissioner's Office (ICO).

2.8. *"***Information Commissioner's Office ("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.

[3] *Data protection officers | ICO*

2.9. **''Data Protection by Design and Default''**, also known as 'Privacy by Design', refers to Articles 25(1) and 25(2) of the UK General Data Protection Regulation (UK GDPR)[4]. These articles outline the obligations for GBS to effectively implement data protection principles and safeguard the rights of individual data subjects for all processing activities and business practices, with consideration made from the design stage through to the end of the lifecycle.

2.9.1. **Design** in this instance refers to considerations of data protection principles made for the design, development, or implementation of any system, service, product, or process and then throughout their lifecycle through to decommission.

2.9.2. **Default** refers to the principles of 'data minimisation' and 'purpose limitation', ensuring that only the necessary data is processed to achieve a specific and defined purpose.

3. Roles and Responsibilities

3.1. 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 use, and for appropriate retention and disposal. Each department must name senior individuals responsible for records or record sets (identified Information Assets) to fulfil the role of Information Asset Owner to ensure accountability. This helps in maintaining compliance with data protection regulations and ensuring proper management of records throughout their lifecycle.

3.2. GBS is registered with the Information Commissioner's Officer as a Data Controller. Details of registration are published on the Information Commissioner's website. GBS as a Data Controller shall implement appropriate technical and organisational measures to ensure that processing of personal information is performed in accordance with the UK GDPR and DPA (2018).

3.3. Records management considerations must be 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

[4] https://www.legislation.gov.uk/eur/2016/679/article/25

to do this to ensure that a data protection by design and default[5] approach is followed. The roles and responsibilities include:

3.3.1. GBS Senior Management Team: Responsible for ensuring that systems are in place to meet all of GBS' legal obligations, including the establishment and monitoring of systems of control and accountability. They must ensure staff are made aware of this policy and must develop and maintain good information handling practices within their areas of responsibility, along with appropriate management of breaches to classified data.

3.3.2. The Senior Information Risk Owner (SIRO) is responsible for ensuring that all IAOs are identified and is accountable for ensuring that information risk, policy, awareness, and understanding is maintained across the organisation. The SIRO position is to be filled by the Deputy Chief Executive Officer or assigned by them to a suitably experienced senior executive.

3.3.3. Information Asset Owners are responsible for classification and records management of their information assets.

3.3.3.1. GBS SMT and faculties are commonly considered Information Asset Owners. It is their responsibility to discover and label information according to its sensitivity. However, owners can be more broadly defined as those that create or manage data e.g., researchers collecting data in the field. Regardless all owners must classify and appropriately label data according to this policy.

3.3.3.2. IAOs must undertake and pass information management training on appointment and again at times determined by the Information Management Group based on risk and changes to legislation or practice.

3.3.3.3. IAOs must know what information the asset holds, and what enters and leaves it and why.

[5] *Data protection by design and default | ICO*

3.3.3.4. IAOs must formally review the risks to the confidentiality, integrity, and availability of their information assets, including those in their delivery chain, and repeat this review if there is a change or as guided by the Information Management Group.[6]

3.3.3.5. IAOs must Provide an annual written assessment to the Senior Information Risk Owner about the security and use of the asset.

3.3.3.6. IAOs share responsibility for the protection of information held on ICT networks, systems, and hard copy information assets. IAOs must consider organisational culture and behaviours to ensure compliance with data protection law within their business area.

3.3.3.7. IAOs must maintain a log of access requests made and monitor as required with managers permissions granted to transfer personal information to removable media.

3.3.3.8. IAOs must report breaches to handling of information assets in accordance with their classification and the provisions of the GBS Data Breach Policy, all breaches must be reported to the Data Protection Officer.

3.3.4. The Data Protection Officer (DPO) is responsible for keeping this policy up to date, overseeing the implementation and compliance of data and records management policy. They will maintain a record of IAOs. They ensure that the policy aligns with data protection regulations and best practices, and they provide guidance and support to GBS in managing records and protecting sensitive information. More information on the DPO can be found in the GBS Data Protection Policy. The DPO can be contacted on dpa@globalbanking.ac.uk.

3.3.5. GBS Heads of Department are responsible for implementing records management practices and appointing Information Asset Owners within GBS, this could be the Head of Department, or an appropriately experienced member of staff. This includes the implementation, oversight and management of information, and this policy on a day-to-day basis.

[6] *Guidance: Information - Asset owner role (publishing.service.gov.uk)*

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

- Collaborating with the IT department and following GBS IT Policy to ensure proper access controls and permissions are in place for record management.

- Regularly reviewing and updating record management policies and procedures to align with industry best practices.

3.3.7. GBS Staff: Responsible for complying with Data Protection Policy. Completing all required data protection training including refresher training as and when required. They must ensure that they are processing data in line with GBS policies and requirements.

3.3.8. 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 any personal data that they supply about themselves to GBS are accurate and up to date. Ensuring that their work is documented appropriately, and that the records which they create or receive are accurate and managed correctly and are maintained and disposed of in accordance with any legislative, statutory, and contractual requirements.

3.3.9. GBS Academic Standards and Quality Office (ASQO)[7]: Responsible for ensuring that this policy is communicated and accessible to all relevant individuals or departments within GBS and ensure that the Policy Tracker is regularly updated. Contact ASQO on asqo@globalbanking.ac.uk.

3.3.10. In relation to the wider responsibility for the management of information (including records), everyone granted access to GBS information assets (e.g., email, teaching and learning materials, staff/student information, financial and the systems used to process these) has a personal accountability that they, and others who may be responsible to them, are aware of and comply with this policy.

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

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 information requires. The five classifications include: Public, Restricted, Private, Internal and Confidential.

5.2. **Public**

5.2.1. Information that is produced for publication and/or could be disclosed with no impact on GBS can be labelled as Public subject to applicable laws such as copyright. It is important to note that although the confidentiality of this category does not need to be maintained, the integrity and appropriate availability must be. For instance, a press release on an emerging infectious disease is designed to reach a wide audience and so the confidentiality does not need maintaining. However, the integrity of the message is vital to maintain to prevent reputational

damage. Availability in this instance is very important too, because if data is not available, the objective will fail.

5.3. **Internal**

5.3.1. Internal classified data can be characterised as non-sensitive, organisational data. If this level of data has any of its security properties violated it will have a low impact. Access is limited to GBS members and other authorised users. Disclosure may result in temporary inconvenience to individual(s) or organisation(s) or minor damage to reputation that can be recovered and has a small containment cost. Some common examples are project documentation, anonymised data (i.e. that cannot be re-identified), organisational data that is appropriate for GBS staff and students only, staff training materials, and non-sensitive committee minutes (this list is not exhaustive).

5.4. **Confidential**

5.4.1. Confidential data is the most common sensitive data processed. Access must be limited to specific named individuals. Disclosure may cause significant upset to individuals, reputational damage and/or financial penalty. Common examples may include interview notes, disciplinary correspondence, staff salaries, exam board minutes, datasets with sensitive personal data, student demographic details and assessments, staff appraisals, internal and external audit reports (this list is not exhaustive).

5.5. **Restricted**

5.5.1. The Restricted classification is reserved for the most sensitive data. Access must be limited to specific named individuals having to work in an appropriately secure manner. Compromise of this data may result in significant legal liability, severe distress/danger to individual(s), severe damage to organisational reputation and/or significant loss of asset value. Personal health data such as medical records about identifiable individuals are a common example of this highly sensitive category.

Data may also be marked with a descriptor which identifies the reason the classification was applied. For example:

- Restricted – Personal information
- Restricted – Business information

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 Act states that organisations must not process (which includes “retain”) personal data for any longer than is required to fulfil business needs. It also grants individuals the ‘right to request personal data held about them by GBS and to object to how this data is being used.

6.3. In the event of a Subject Access Request (SAR) being made, we must search for, copy, and provide all personal data held even if it is no longer in use. For further information see the Data Subject Access Policy.

6.4. The Limitation Act 1980 provides timescales within which action may be taken (by issuing a claim form) for breaches of the law by former students after their departure from GBS and where GBS can use the files as evidence, if necessary.

6.5. In each case, access is granted unless an exemption applies under each of these access regimes. The scope of an information access regime can include a wide range of records, such as databases, cloud storage, social media content, and even text messages. It is important to consider any type of information that is created, received, or maintained by GBS as potentially falling within the scope of an access regime (this list is not exhaustive).

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, slides, video, including CCTV and in electronic (digital) or (physical) hard copy format.

7.3. Records must be maintained in a manner to ensure they have the following qualities:

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

- The record can be proved to be what it seems to be, and to have been created by the person who is supposed to have created them, and at the time claimed.

- Systems that control the creation and maintenance of records to ensure their creators are authorised and identified, and that the records are protected against unauthorised alteration and deletion.

- The record can be accessed: they can be located, retrieved, presented, and

interpreted by those with the authority to do so and the authoritative version is identifiable where multiple versions exist.

- 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.

- The record can be trusted: the record reliably represents the information that was used in or created by the business process. They are complete and protected against unauthorised alteration whilst authorised alterations, additions or deletions are indicated and traceable so their integrity and authenticity can be demonstrated.

- 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 Annex 5 GBS Records Retention schedule)[8] despite changes of format so it remains usable.

- 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.

7.4. 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.

8. Record Processes and Procedures

8.1. Creating Records

8.1.1. All records created or received must be maintained throughout their lifecycles. Each department must have in place adequate systems for documenting their Information Assets and Records of Processing Activities. The records must be accurate and complete, so that it is possible to establish what has been done and why.

[8] *Please note this has been adopted from JISC 'Records Retention Management' accessed online at: https://beta.jisc.ac.uk/guides/records-retention-management*

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, particularly when it involves downloading records from the central system and keeping local copies. Duplicates increase the risks associated with managing, using, and altering records but also lead to confusion and inefficiency. It is crucial for departments to understand the importance of relying on a single central version of records to ensure proper version control, records management, staff awareness, and compliance with this policy to maintain control over our information assets.

8.5. **Metadata**

8.5.1. Where possible, both paper and electronic records systems should contain metadata (information about the structure of the records system or series) to enable the system and the records to be understood and operated efficiently, providing an administrative context for effective identification and management of records. The metadata could include details of the structure of the records, dates of access, use, alterations, disposal etc.

8.6. **Digital records**

8.6.1. Digital records will be filed in a shared space such as Share-point, wherever

possible. File titles should be brief but comprehensible with a consistent format. Digital records must be captured as soon as possible after creation so that they are readily available to support GBS's business.[9] If digital records are taken out of recordkeeping systems (e.g., printed) they must be managed in accordance with this policy.

8.7. **Restoration**

8.7.1. Where a records system is being replaced or superseded by another system, the records management principles, and the wider information security policy 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.

8.8. **Physical records**

8.8.1. All physical records created or received must be maintained in accordance with this policy. Handling paper or other media and guidance on the storage of physical records.

8.9. **Digital Communications**

8.9.1. Digital communications such as emails may contain actions and decisions and must be managed as effectively as other digital information. Emails and 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, retrieved, regularly reviewed, and deleted when appropriate.

8.9.2. Email, for example, 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 Annex 5 GBS Records Retention Schedule.

8.10. **Vital Records**

[9] *'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'.*

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 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.

8.11. **Naming Record Conventions**

8.11.1. To ensure that records remain useable and can be located when required to fulfil GBS objectives, they must be named consistently and logically. Naming conventions help identify records and folders using common terms and titles. They will enable users to browse files names more effectively and efficiently. Naming conventions need not be overly prescriptive or formalised but must be:

- 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.

8.11.2. 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.

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. 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 an authoritative record.

11. Access to Records

11.1. 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.

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.

12.3. Any retention period will be treated as a benchmark as there may be situations where the data should be held for a minimum or longer period than those recommended in the Retention Schedule, any deviation should be documented fully. These periods may also be altered by subsequent legislation or organisational instructions.

12.4. Records that are no longer live (i.e., not in active use) are sometimes referred to as archive records, which is a collection of historical records and documents that are preserved for research, reference, and historical purposes. These archives often contain materials such as manuscripts, administrative records, publications, and other significant documents that provide insights into GBS history and development. Retention periods apply to records in whatever format they are created or held. Retention and destruction of electronic records must be managed as well as those held on paper and follow the same rules.

12.5. It is recommended that all departments regularly review (e.g., at minimum on an annual basis) their entries in the Retention Schedule to ensure they reflect the records that they work with and put in place processes to ensure that disposal actions are carried out at the appropriate time. The DPO alongside the Registry team will conduct regular audits to ensure compliance with the Retention Schedule and avoid keeping records longer than necessary. This helps maintain data privacy and minimise potential risks

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 1 – “Lifecycle” of a record

Annex 2 – GBS Information Classifications

GBS has four Information classifications to help staff identify the level of security required. The four classifications include: Public, Internal, Confidential, and Restricted.

GBS Information Classifications		
Sensitivity Level	**Classification**	**Description & Examples**
1	**Public**	Low sensitivity, data intended to be available to the public, with few security requirements as disclosure would not breach compliance with external requirements or GBS procedures.
		***Examples**:* *GBS contact information, public policies, prospectus, programme/course information, marketing materials, job descriptions, publications, published statistics and annual accounts.*
2	**Internal**	Low-Medium sensitivity, data available to any authenticated GBS staff member. Disclosure outside of the organisation would not cause meaningful financial or reputational damage. However, leakage of some data may be inappropriate or poorly timed.
		***Examples**:* *Internal communications (email, memos), market research, academic handbooks, intellectual property, and internal policies/procedures.*
3	**Confidential**	Medium-High sensitivity, internal data that has additional security requirements including access controls and clearance in order to access. Clearance should only be assigned to specific staff members, teams, partners, and third parties involved in creating, processing, or retaining the data. Disclosure outside of approved channels would breach confidentiality and could compromise activity within the organisation. Public disclosure may result in reputational or financial damage to the organisation if accessed by malicious parties.

		***Examples**:* *Personnel data, sensitive operational data, unpublished research data and other publications, timesheets, expenses, exam scripts, marks, examiners comments on student performance, documents that may be damaged by uncontrolled modifications, leakage of documents that may cause damage to projects, sponsors, or the organisation.*
4	**Restricted**	High sensitivity, data only accessible to specific and relevant senior staff members, with high security requirements including appropriate access controls that are reviewed regularly. Disclosure of restricted data could place GBS in serious financial or legal risk, resulting in damage to corporate revenue, reputation, and operation. **Personal Information**: protected characteristics and special categories of data under the GDPR. **What is special category data? | ICO** **Business Information**: disclosure of this sensitive information could cause severe harm to the organisation, its stakeholders, students, or staff.
		***Personal Information Examples**:* *Race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sexual orientation.* ***Business Information Examples**:* *Key financial information, bank account details, debt information, draft research/reports of controversial or financially significant subjects, passwords, system access credentials, administrative credentials, future marketing materials or financial information not approved to be made public, legal advice relating to legal proceedings for or against the organisation.*

Annex 3 - GBS Information Handling Requirements

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

GBS Information Classification Handling Requirements					
Information Classification	**Description**	**Storage**	**Access**	**Exchange**	**Disposal**
Public	Published information intended to be viewable by the public.	Digital information should be stored using GBS approved IT facilities, systems, and shared drives to ensure appropriate records management, security controls, and backups. Published information should be presented and stored on GBS approved websites, repositories, and other relevant publications. Physical information such as marketing materials, programme info, published statistics, reports, and research documents should have a digital copy scanned for backup and review purposes.	No access controls required to view or disseminate Public information. Information can be accessed and shared via the internet without being an authenticated GBS staff member. Digital and physical information can be circulated without approval from the Information Asset Owner (subject to e.g. copyright, competition, consumer, or contractual laws applicable). Information can be accessed remotely, and via portable, mobile, and personal devices without encryption or enhanced security requirements.	Information can be shared via any digital medium, inclusive of all communications, file sharing, and collaboration platforms, without requiring encryption or approval.	No additional disposal requirements. Digital information should be deleted using the normal file deletion process (if deletion or archiving Is required e.g. by a retention schedule). Physical information such as paper documents can be disposed of using the normal waste disposal/recycling process. Superseded documents and information should be archived and marked appropriately as such.
Internal	Data intended to be available to any authenticated GBS staff member.	Digital information should be stored using GBS approved IT facilities, systems, and shared drives to ensure appropriate records management, security controls, and backups. Physical (hard copy) information should be stored within the relevant department's staff facilities, located on GBS premises. Information should not be stored on non-authenticated personal devices, portable drives, or discs without prior approval from the IAO.	Access should be limited to authenticated and current GBS staff members. Access can be limited only to staff members that require it (if the sensitivity is still not appropriate to be labelled Confidential). Information accessed via staff personal devices is restricted to 'Read Only' and should not be downloaded (mobile phones, portable devices, unauthenticated computers). Information can be accessed remotely via GBS provided portable and mobile devices, with appropriate disc encryption and security controls in place. Physical (hard copy) information can be accessed and disseminated freely within the organisation and its premises but should not be disseminated outside the organisation without prior approval from the Information Asset Owner.	Information can be shared via GBS authenticated internal communications systems and applications. Information should not be shared using non-authenticated or personal communications platforms. Information should not be sent to non-authenticated or personal communications accounts/addresses. Information should not be transferred to non-authenticated personal devices, drives, or discs without prior approval from the IAO.	Digital information should be deleted using the normal file deletion process (if deletion or archiving is required e.g. by a retention schedule). Physical (hard copy) information such as paper documents can be disposed of using the normal waste disposal/recycling process. Superseded documents and information should be archived and marked appropriately as such.
Confidential	Internal information that has additional security requirements including access controls and clearance in order to access. Intended to be accessible only to those with role-based permissions express	Data/Information must be held within GBS approved and authenticated systems, databases, and repositories as defined and documented in the GBS Information Asset Register and GBS Records Retention Schedule.	Access should be limited to the Information Asset Owner, relevant staff involved in processing, and executive leadership accountable for that information.	Exchanges of larger volumes of sensitive information should be assessed by the IAO for impacts of unintended/inappropriate disclosure – exchange methods used should reflect these risks.	Physical (hard copy) information should be disposed of by shredding, using GBS waste disposal facilities. Digital information stored on hard drives must be securely wiped (not just deleted from the device). Either by:

	permission from the Information Asset Owner.	Storage mediums should have appropriate encryption, firewall protection, and threat monitoring to mitigate risks associated with data breaches, malware attacks, and data leakage. Information should not be stored remotely, on personal devices, or portable drives (e.g. USB memory sticks). Physical (hard copy) information should not be left unattended anywhere on GBS premises and locked away securely in desk drawers or cabinets when not in use, regardless of student or staff accessibility. Physical (hard copy) information should not be brought or stored at home or away from GBS facilities and premises.	Role-based permissions should be used and managed by the Information Asset Owner, with reviews of access conducted regularly. Requests to access confidential information should be made to the Information Asset Owner, with valid reasoning given for requesting access. Access should be revoked once the need for access and processing has been fulfilled. Remote access must be done using a GBS provided portable and mobile devices, with appropriate disc encryption and security controls in place. Access via staff personal devices should be blocked (unauthenticated mobile phones, portable devices, computers) unless written approval is given by the Information Asset Owner. The IAO must review all requests for access promptly, with consideration for the information's sensitivity, confidentiality, integrity, and availability requirements. Physical (hard copy) information should be placed and presented in areas with restricted access (i.e. staff areas that require key card access).	Information must be sent using GBS authenticated internal communications systems, applications, network, and facilities. Information must only be sent to GBS authenticated addresses, accounts, and systems – Unless requested/approved by the IAO. Information must not be shared with external/3rd party addresses, accounts, or systems without written approval or request from the IAO. Information must not be downloaded to personal portable devices, mobiles, or computers. Digital hard-copy or duplicate versions of confidential information should be avoided, unless requested by the IAO. Paper and electronic copies must be clearly marked as confidential and distributed securely, with the intended recipients marked clearly. The reason for confidentiality may also be used when exchanging or disseminating confidential information.	- Removal of decryption code for encrypted drive - Secure drive wiping tool Digital information stored on systems and cloud storage should be disposed of using encrypted deletion/archiving. Archived information be stored in a secure folder with restricted access.
Restricted	Information only accessible to specific and relevant staff members, typically suitably experienced managers, trained administrators, and executive leadership accountable for the information. Disclosure of restricted information could place GBS in serious financial or legal risk, resulting in damage to corporate revenue, reputation, and operation: - Highly sensitive personal information about staff and students that could be used to identify them individually. - Highly sensitive business information, disclosure of which could cause serious harm to the organisation and its interests.	Data/Information must be held within GBS approved and authenticated systems, databases, and repositories as defined and documented in the GBS Information Asset Register and GBS Records Retention Schedule. Information must be stored in a highly restricted central repository. - Digital information must be stored in GBS authenticated secure repositories, with limited and controlled access. - Physical (hard copy) information must be stored in secure environments with appropriate barriers to access for non-staff (e.g. lockable drawer, filing cabinets, and safes). Physical (hard copy) information should not be left unattended anywhere on GBS premises and locked away securely when not in use (above). Information must not be stored remotely, on personal devices, or portable drives (e.g. USB memory sticks).	Information may only be accessed using GBS authenticated devices, with appropriate disc encryption and security controls in place. Access is limited to the Information Asset Owner, approved processors, and executive leadership accountable for that information. - IAOs must risk assess their restricted information in terms of access and review permissions regularly based on a 'Need to Know' basis. - Once the requirement to access for processing/analysis purposes has been fulfilled, access should be removed. - Requests for access should be made to the IAO, with valid reasons for required access provided and confirmation of completion given, for the IAO to remove access. - The IAO must review all requests for access promptly, with consideration for the information's sensitivity, confidentiality, integrity, and availability requirements.	Exchanges of large volumes of data should be avoided where possible, with consideration for 'data minimisation' and 'Need to Know' concepts (i.e. Does the recipient require the entire dataset to process, or can they receive an extraction or subset?). Exchanges of larger volumes of sensitive information should be assessed by the IAO for impacts of unintended/inappropriate disclosure – exchange methods used should reflect these risks. - Information must be sent using GBS authenticated internal communications systems, applications, network, and facilities. - Information must only be sent to GBS authenticated addresses, accounts, and systems – Unless requested/approved by the IAO. - Information must not be shared with external/3rd party addresses, accounts, or systems without written approval or request from the IAO.	Physical (hard copy) information must be disposed of securely via shredding and/or incineration, with storage of paper information avoided where possible in place of digital information (excluding original copies of legal documents, certifications, licences etc). Archived information should be anonymised, or pseudonymised if analysis is still required. (note: pseudonymisation could potentially still link the data to the data subject with additional information, archived information should still be stored securely). Digital information stored on hard drives must be securely wiped (not just deleted from the device). Either by: - Removal of decryption code for encrypted drive - Secure drive wiping tool GBS devices used to store restricted information must be sanitised/wiped (as above) prior to 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 facilities and premises, removal is only permissible if other options have been evaluated and approval is granted by the IAO. Personal information that relates to identifiable data subjects, considered 'at rest' or archived, should be anonymised if further analysis or processing is not required, or it has exceeded the defined retention period within the GBS Retention Schedule (GDPR no longer applies). If further analysis is required, or the subject is expected to need to be identified (e.g. DSARs), the information should be pseudonymised if 'at rest', allowing for further analysis with no direct link to the individual data subject. Subjects could still be identified indirectly via this method, but only with access to additional information (GDPR still applies).	Remote access must be done using a GBS provided portable devices and computers, with appropriate disc encryption and security controls in place. Access via personal devices of any kind is prohibited, download and 'read only' access should be blocked for all restricted information. Physical (hard copy) information when in use must be placed and presented in areas with restricted access and visibility (i.e. staff areas and meeting rooms that require key card access).	Restricted data must not be extracted from GBS information systems and stored locally, in device drives, or on personal devices or information systems. Extractions of restricted information must be stored with GBS information systems, marked appropriately, with personal data de-identified (either by anonymisation or pseudonymisation, depending on analysis requirements defined by the IAO). Extractions of restricted information should be archived or deleted once the reason form processing has been fulfilled. Paper and electronic copies must be clearly marked as Restricted and distributed securely, with the intended recipients and reason for classification marked clearly (e.g. RESTRICTED Information – Sensitive Personal Data).	Digital information stored on systems and cloud storage must be disposed of using encrypted deletion/archiving. Archived information be stored in a secure folder with access restricted to the IAO and documented proxies.

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)*	**Destruction:**				**Transferred to Archives:**	
Method of destruction: *(tick if applicable)*	**Non-confidential waste or recycling**				**Confidential shredding**	
	Digital deletion from GBS network (e.g., central locations, share-drive, database etc.)				**Digital deletion from other location**	
Approximate number of records:						
Date of disposal:						
Approved by: (Must be Senior Management Team)						
Date Approved:						

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.

Function	Activity	Record Group	Retention Period	Citations and Notes
Business function/ related area	*Activity carried out by business function*	*Record category/type held for this activity*	*Length of time this record should be retained for, after which deletion/archiving must be scheduled*	*Relevant legal basis for retaining a record, its retention period, regulatory, statutory, and any specific requirements for the record group referenced*
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. *For details on what may constitute the core student record see:* *The European Credit Transfer and Accumulation System (ECTS) User Guide 2015* *What Is a Student Record? A Case Study by King's College London, Appendix IV* *For more details on the HEAR, see the HEAR website and 'Beyond the Honours Degree – the Burgess Group Final Report' (October 2007)* *Guidelines for HE Progress Files, QAA (2001)* *Guide to the Diploma Supplement, UK HE Europe Unit (2006)*
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: key records.	Superseded + 10 years	Institutional business requirements.
Legal and Governance	Governance Framework Development	Records documenting the establishment and development institution's governance structure and rules.	Life of institution	Institutional business requirements. *The institution may wish to transfer these records to the archive once they are no longer in active use.*

Health and Safety	Health & Safety Audit	Records documenting the conduct and results of health and safety audits.	Completion of audit + 5 years	*Retaining previous versions provides evidence of compliance and effective management of health and safety over time.*
Strategy and Planning	Human Resources Strategy and Policy Development	Records documenting the development and establishment of the institution's human resources strategy, and policies: key records.	Superseded + 10 years	Institutional business requirements.
Payroll	Payroll Administration	Records documenting calculation and payment of employees' salaries and other payments.	Minimum: Current tax year + 3 years Recommended: Current tax year + 6 years	Minimum: The National Minimum Wage Regulations (SI 2015/621) Regulation 59(8) The Income Tax (Pay As You Earn) Regulations (SI 2003/2682) Regulation 97(8) Recommended: Taxes Management Act 1970 c. 9 s 34
Estates	Property Acquisition	Records documenting the negotiation of leases and original lease agreements.	Expiry of lease + 15 years	Limitation Act 1980 c. 58 s 14B
Information Communication Technology (ICT)	ICT Systems Development	Records documenting the initial development and post-implementation modification and maintenance of ICT systems.	Decommissioning of system + 5 years	Institutional business requirements.
Information Strategy and Data Protection	Information Compliance Strategy and Policy Development	Records documenting the development and establishment of the institution's information compliance strategy and policies: key records.	Superseded + 5 years	Institutional business requirements.
Marketing and Communications	Market Research	Market research data: aggregated data and analyses.	Completion of research + 5 years	Institutional business requirements. *The institution may wish to transfer these records to the archive once they are no longer in active use.*