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	

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 policv1G0 G[st)-2(ude)-3(nts)-4(,)]TJETQq0.000008881 0.000061035 595.98 848 842.0 1 25 U5.

and

2.4 and **Information Asset** 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.

2.9. **Protection by Design and** , also known as by refers to Articles 25(1) and 25(2) of the UK General Data Protection

[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

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*

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.

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*

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 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.

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 thBTD]13/ 519TQq0.000008881 0.000061035 595.98 842.52 reW*nBT/F3 10.98 Tf1 0 0 1 126.14

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

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.

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.

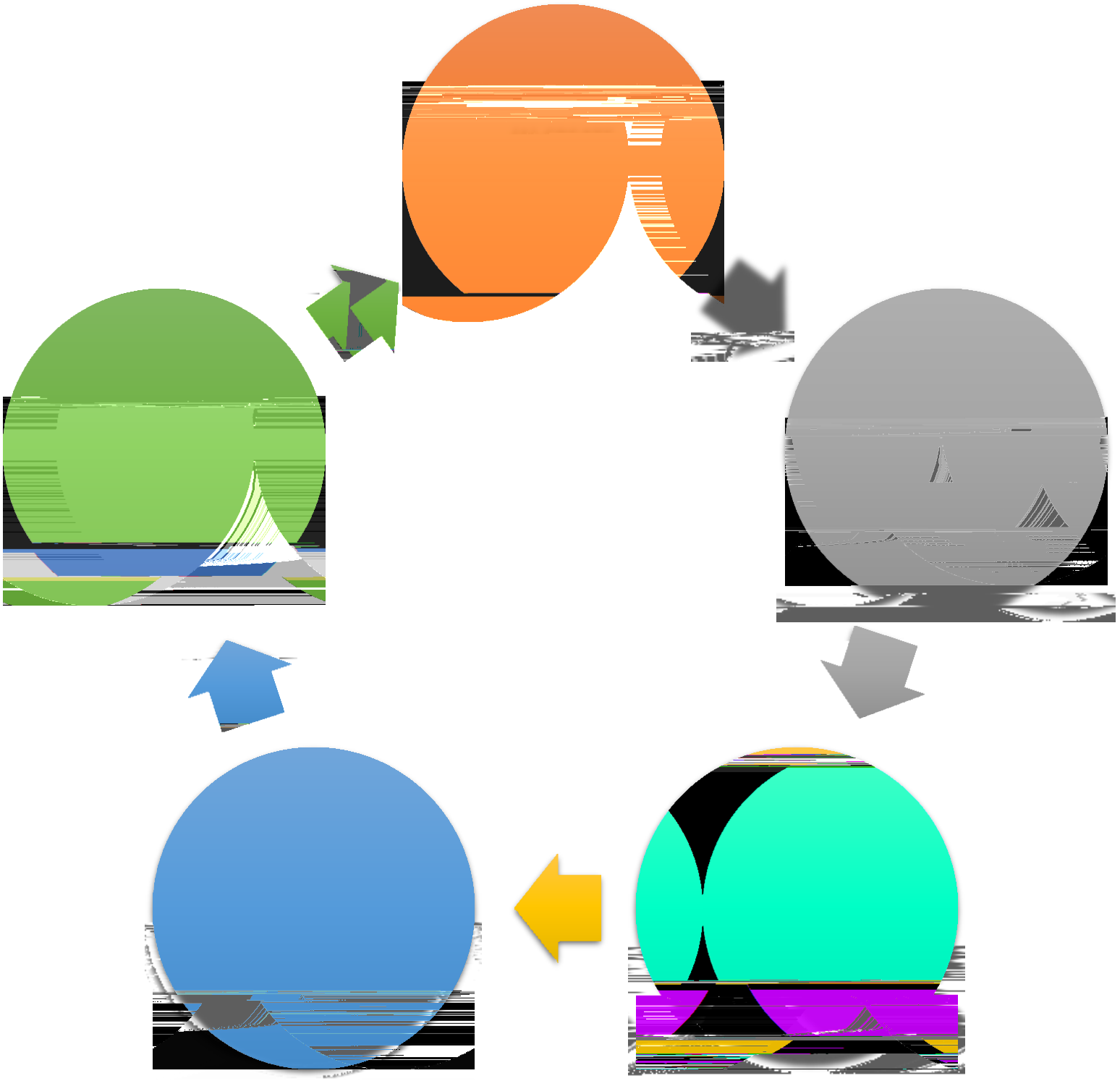
16. Audit and Compliance

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 **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

Annex 3 - GBS Information Handling Requirements

Annex 4 - GBS Records Disposal Form

RECORDS DISPOSAL FORM	
Department:	
Information Asset Owner *(name and*	

Health and Safety	Health & Safety Audit