GBS HE Malta Limited
Malta Campus
International House
Mdina Road
Mriehel BKR3000
Malta

GBS Records Management and Retention Policy

Version Control

Document title: GBS Records Management and Retention Policy		**No of pages:** 19
Version Number: V1.0	**Date first published:** December 2019	
Approved by: Malta Further and Higher Education Authority (MFHEA)	**Last review date:** January 2022	
Date approved: May 2022	**Due for next review: January 2023**	

Related policies
▪ GBS Records Management and Retention Policy ▪ GBS Data Protection Policy ▪ GBS Privacy Policy ▪ GBS Data Subject Access Request Policy ▪ GBS Access Control Policy ▪ GBS IT Security Policy ▪ GBS Email Usage Policy ▪ GBS Data Classification and Handling Policy
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

Contents

GBS HE Malta Limited Records Management and Retention Policy

1. Purpose and Scope

1.1 GBS HE Malta Limited (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]

'Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'.

1.3 The Code of Practice on Records Management issued in July 2009 by the Lord Chancellor under section 46 of the Freedom of Information Act 2000 at paragraph 2 of Part 1 states:

'The code applies to all records irrespective of the technology used to create and store them or the type of information they contain. It includes, therefore, not only paper files series and digital records management systems but also business and information systems (for example case management, finance, and geographical information systems) and the contents of websites.'

1.4 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. 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 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 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 GBS' guidelines and any legislative, statutory, and contractual requirements.

2.8. GBS Academic Standards and Quality Office (ASQO)[2]: Responsible for implementation, 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 IT Security Policy sets out that everyone granted access to GBS information assets (e.g., email, teaching and learning materials, staff/student information, financial information, research information, and the systems used to process these) has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the policy.

2.10. Everyone is responsible for protecting GBS' 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 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.

3.3. 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.

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

3.5. Freedom of Information Act 2000 compliance relies on the ability of the business to identify and locate the information sought in an accurate and timely way. The correct use of registered files will assist in meeting this requirement of the act. A regular critical examination of information held is essential to avoid holding data longer than is required. GBS must respond to requests within 20 working days.

3.6. Section 46 of the Freedom of Information Act provides guidelines set down in the Lord Chancellor's Code of Practice on the management of records. The code requires that GBS has in place 'a records management policy, either as a separate policy or as part of a wider information or knowledge management policy'.

3.7. Environmental Information Regulations 2004 enables members of the public the right to access 'environmental information' and must respond to requests within 20 working days.

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

3.9. The ISO 15489 provides series of international standards on information, documentation and records management and establishes standards for the management of business records.

3.10. It is important that data, information, and records created and held at GBS are managed in line with the provisions of the IT Security Policy. The information you create is representing GBS and therefore its content should be in line with GBS' vision and values.

4. Record Management Standards

4.1. 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.

4.2. 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 and in electronic (digital) or (physical) hard copy format. 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 accessed*: information can be located 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, and its 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 GBS Records Retention schedule) despite changes of format.

- *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 versions of records held centrally, it should be avoided where possible and a system enabling use of a single central version implemented. Where practical, to reduce the need for duplication, documents should be stored in central folders that

are accessible by relevant staff.

5.5. **Metadata**

5.5.1. 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 management of the records, and to enable individual records to be identified and accessed efficiently. The metadata could include details of the structure of the records, dates of access, use, alterations, disposal etc.

5.6. **Digital data**

5.6.1. Digital information should be filed in shared space such as Share-point, share-drive wherever possible. File titles should be brief but comprehensible with a consistent format used. Digital records should be captured as soon as possible after creation so that they are readily available to support GBS´ business.[3] If digital records are taken out of recordkeeping systems (e.g., printed) they must be managed in accordance with GBS Data Classification and Handling Policy.

5.7. **Restoration**

5.7.1. 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.

5.8. **Physical records**

5.8.1. All physical records created or received must be maintained in accordance with GBS Data Classification and Handling Policy. Handling paper or other media and guidance on the storage of physical records.

5.9. **Email**

5.9.1. Emails may contain actions and decisions and must be managed as effectively

[3] *'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'.*

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

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

5.10. **Vital Records**

5.10.1. 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).

5.10.2. 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 to protect the documents.

5.11. **Naming Records**

5.11.1. To ensure that records remain useable and can be located when required to fulfil GBS objectives they should be named consistently. Naming conventions help identify records and folders using common terms and titles. They also enable users to ascertain between similar records to determine a specific record when searching the electronic or physical file system. 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.

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 in line with GBS IT Security Policy.

6. Classification, storage, and handling of records

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

6.2. 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.

7. Digitisation

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

7.2. 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 GBS Records Retention Schedule.

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 Information Act Section 46 Code of Practice on the Management of Records states:

9.3. “As a general principle, records should be kept for as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. Destruction at the end of this period ensures that office and server space are not used, and costs are not incurred in maintaining records that are no longer required.”

9.4. Any retention period should be treated as a benchmark as there might be situations where the data should be held for a minimum or longer period than those recommended in the RRS any deviation should be documented fully. These periods may also be altered

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 responsible for the implementation of their section of the Records Retention Schedule, although operational practice may rest within other areas, requiring close collaboration, including ensuring that all relevant Information Asset Owners are fully appraised of their requirements of the Retention Schedule and apply accordingly. This may include auditing compliance.

10. Review

10.1. 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.

11. Disposal of Records

11.1. Records will be disposed of in accordance with agreed retention schedules. Retention schedules will set out the minimum period for which a record should be retained and will be reviewed regularly and amended, as necessary. Retention schedules will be agreed by the senior data owners for the relevant business function. 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 GBS Archive.

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

12. Security and Access

12.1. Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. All records in any format must be held in accordance with GBS IT Security Policy and Data Protection guidance. Records must be stored in a safe and secure physical and digital environment taking account of the need to preserve important information in a useable format enabling access commensurate with frequency of use.

12.2. GBS Access Control Policy outlines the rules relating to authorising, monitoring, and controlling access to GBS information systems. GBS recognises that information is a valuable asset and access to it must be managed with care to ensure that confidentiality, integrity, and availability are maintained.

12.3. GBS Data Classification and Handling Policy describes five information classifications to help staff identify the level of security the information requires. The five classifications include: Public, Restricted, Private, Internal and Confidential. (*Please refer to Annex 2 - Information Classifications* for a brief outline on these).

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, GBS Data Protection Policy, GBS Data Classification and Handling Policy, GBS Privacy Policy, GBS Data Subject Access Request Policy, GBS IT Security Policy, and GBS Access Control Policy. Information on other related policies is available from GBS Academic Standards and Quality Office (ASQO) and can be found under the GBS General Policies folder on SharePoint.

14. Audit and Compliance

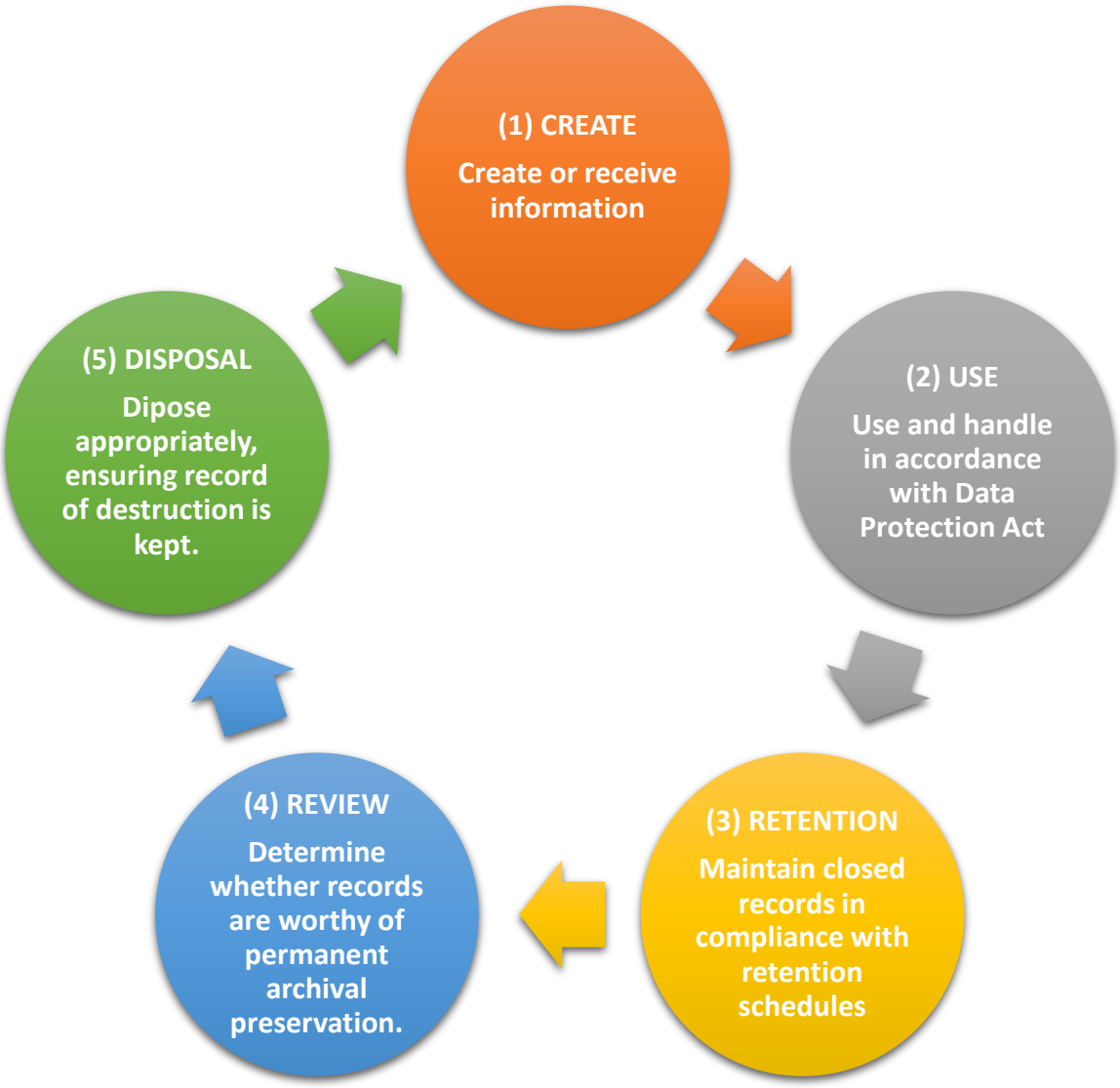
14.1. GBS Records Management and Retention Policy may be amended by GBS at any time.

15. Alternative Format

15.1. 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:

- **Name:** Welfare Management Team
- **Position:** Welfare Officer/Manager
- **Email:** welfare@globalbanking.ac.uk

Annex 1 – "Lifecycle" of a record



Annex 2 – GBS Information Classifications

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.

CLASSIFICATION	DEFINITION
Public	Data that can be freely disclosed to the public. Examples include GBS contact information, location, job descriptions and prospectus.
Restricted	Highly sensitive internal data. Disclosure could negatively affect operations and put GBS at financial or legal risk. Restricted data requires the highest level of security protection by everyone working at GBS from staff to students to partners etc. For example, Committee papers and documents marked for the attention of a specific reader.
Private	Private information is typically a classification of information that individuals use for themselves. It is a broad and general term that is more ambiguously used than other privacy terms. For example, emails to colleagues regarding work buffets or quizzes etc.
Internal	Data that has low security requirements, however, is not meant for public disclosure such as marketing research, academic handbooks.
Confidential	Confidential information is information shared with only a few people, for a designated purpose and can be shared with others within GBS. The person who is receiving the information from you, the receiver, generally cannot take advantage and use your information for their personal gain, such as giving the information out to unauthorised third parties. These can include documents prepared for publication or unpublished research data.

Annex 3 - 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.