GALWAY BUSINESS SCHOOL

Information & Data Management Policy

QA May 2020

Information & Data Management Policy

8.1 Purpose

GBS operates in a complex, data-oriented environment. Data generated and held by the school are key assets that must be managed correctly in order to ensure that the school functions effectively. The aim of this policy is, therefore, to provide a comprehensive information and data management framework that covers data collection, storage, security, maintenance, and dissemination. In addition, the policy ensures that GBS complies with the requirements of the relevant Irish legislation such as GDPR 2018.

Document Name: Information & Data Management Policy	 GALWAY BUSINESS SCHOOL
Owner: Registrar	
Approved by: Governing Body	
Review frequency: Every 2 years	

Version	Description of Amendments	Approval Date	Implementation Date
V1.0	Approval in full of the policy by the Governing Body	July 2018	September 2018
V2.0	Extended by Section 9.7 Records Maintenance and Retention	July 2019	September 2019
V3.0	Policy reviewed to reflect GDPR 2018	March 2020	March 2020

8.2 Scope

The policy covers both personal and sensitive data including but not limited to:

- Learners' data and records
- Staff data
- Financial data
- Commercial data
- Intellectual property
- Academic data

GBS is committed to ensuring that all data is clearly identified and storage of all data is effectively maintained. The data storage includes data held on all IT resources and application types including Schoolworks and Microsoft Excel spreadsheets (and other such end-user applications) stored on the intranet.

8.3 Information Systems

The data availability is crucial for further organisational development and improvements of the operation of GBS. Therefore, GBS ensures the effective collection of information about its operations to help inform its decision-making process. Central to this are the GBS's CRM system Schoolworks and the VLE system Moodle, where all information that GBS collects is initially recorded and stored. In addition, certain information is exported from these into Microsoft Excel spreadsheets and other applications and stored on the intranet.

With regards to information systems, GBS will:

- Ensure that both Schoolworks and Moodle are maintained securely, kept up-to-date and remain fit for purpose.
- Ensure that Schoolworks and Moodle generate appropriate statistical data that can be easily accessed and analysed
- Produce annual data-driven reports that will serve as a basis for decision making and improvement of quality assurance policies and procedures. These reports will include data on:
    - Learner satisfaction rates

- Learner attendance/attrition/progression/dropout rates
- Learner completion rates
- Learner graduation/certificate rates
- Grade analysis of learner performance
- Career paths of graduates
- Learner individual traits

8.4 Management Information Systems

The Schoolwork and Moodle systems must be reviewed annually and their usability must be evaluated with regards to statistics generation. These statistics serve as a basis for various data- driven reports on which GBS bases its strategic planning. The Managing Director, Quality Assurance Committee and Risk Management Committee consider the reports listed below when crafting future plans for GBS's operations:

- Annual Monitoring Reports for each programme
- Module Reports for each module
- Overall attendance statistics
- Overall learner results

8.5 Data Classification

The purpose of this policy is to support the classification of data to allow for the protection of GBS's data, or data held by GBS, in terms of confidentiality, integrity, and availability. This policy covers all data captured, processed or stored by GBS. It applies to all members of GBS' community including, academic staff, administration and support staff, learners and other organisations or individuals handling data on behalf of GBS.

8.5.1 Responsibilities

- All information owners are responsible for ensuring that this policy is adopted within their area of responsibility.
- The classification of information will be the responsibility of the head of individual departments.
- Individual staff members are responsible for ensuring that sensitive information they produce is appropriately protected and marked with the appropriate classification.

8.5.2 Policy Requirements for Information Assets

All existing GBS information belongs to one of the classifications below. Unless otherwise classified, the information should be treated as 'GBS Controlled'.

8.5.2.1 Information Classification Guide

The guide provides a framework for classifying and protecting GBS's information resources. It outlines the security objectives in the left column and assesses the potential impact GBS should certain events occur which jeopardise the information and information systems needed by the school to accomplish its mission, protect its assets, fulfil its legal responsibilities, maintain its day-to- day functions, and protect individuals.

The three levels of potential impact on GBS or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) are as follows:

The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on GBS's operations, assets, or on individuals.

The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on GBS's operations, assets, or on individuals.

The potential impact is **HIGH** if: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on GBS's operations, assets, or individuals.

Public Information, i.e. information that can be communicated without restrictions, and is intended for general public use, is not included in the framework below as this data will not cause harm to any individual, group, or to GBS if made public. Examples include Standard guidelines and policies, GBS' Strategy, Contact Details, maps, GBS's Marketing materials, Public Web site and advertisement.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorised disclosure of information could be expected to have a limited adverse effect on GBS's operations, assets, or on individuals.	The unauthorised disclosure of information could be expected to have a serious adverse effect on GBS's operations, assets, or on individuals.	The unauthorised disclosure of information could be expected to have a severe or catastrophic adverse effect on GBS's operations, assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorised modification or destruction of information could be expected to have a limited adverse effect on GBS's operations, assets, or on individuals.	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on GBS's operations, assets, or on individuals.	The unauthorised modification or destruction of information could be expected to have a severe or catastrophic adverse effect on GBS's operations, assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information could be expected to have a limited adverse effect on GBS's operations, assets, or on individuals.	The disruption of access to or use of information could be expected to have a serious adverse effect on GBS's operations, assets, or on individuals.	The disruption of access to or use of information could be expected to have a severe or catastrophic adverse effect on GBS's operations, assets, or on individuals.
Data Classification	**GBS Controlled** With this classification protection of information is at the discretion of the custodian and there is a low risk of embarrassment or reputational harm to GBS.	**GBS Restricted** GBS has legal, regulatory or contractual obligation to protect the information with this classification. Disclosure or loss of availability or integrity could cause harm to the reputation of GBS or may have short term financial impact on the school.	GBS Highly Restricted Protection of information is required by law or regulatory instrument. The information within this classification is subject to strictly limited distribution within and outside of GBS. Disclosure would cause exceptional or long term damage to the reputation of GBS, or risk to those whose information disclosed, or may have serious or long term negative financial impact on the GBS.
Examples	Meeting minutes, school working & draft documents.	Learner or employee records, grades, employee performance reviews, personally identifiable information.	PPS numbers, physical or mental health records relating to individuals, critical research data.

8.6 Data Privacy

This section provides details of the way in which GBS processes personal data in line with its obligations under Data Protection Law. The purpose of this Data Privacy Policy is to explain what Personal Data GBS processes exist and how and why GBS process it. In addition, this section outlines GBS's duties and responsibilities regarding the protection of such Personal Data. The manner in which GBS processes data will evolve over time and the policy will be updated from time to time to reflect changing practices. In addition, in order to meet transparency obligations under Data Protection Law, GBS will communicate this policy section by reference into notices used at various points of data capture when collecting personal data (e.g. application forms, website forms etc.).

8.6.1 GBS as a Data Controller

Data Controllers are defined in the GDPR as persons or organisations that, alone or with others, determine the purpose and means of processing personal data. When GBS determines the purposes and means of the processing of personal data it acts as a Data Controller. In relation to suchprocessing, Article 6(1)(e) of the GDPR provides an appropriate legal basis, which permits processing that is necessary for the performance of the task which is in the public interest, where such "public interest" is laid down in EU or Irish law. Section 34(1) of the Data Protection Act 2018 further makes it clear that GBS can rely on this public interest basis as a lawful basis for processing personal data where processing is 'necessary for the performance of a function of a Data Controller conferred byor under an enactment, or the administration by or on behalf of a Data Controller of any non- statutory scheme, programme or funds where the legal basis for such administration is a function of a controller conferred by or under an enactment'.

Where processing activities are not specifically supported by a particular statutory basis, GBS relies on other legal bases under Data Protection Law. These include: Article 6(1)(a) of the GDPR which permits processing where the data subject has given his or her consent; Article 6(1)(b) which permits processing where necessary for the performance of a contract to which the data subject is a party; Article 6(1)(c) which permits processing that is necessary for compliance with a legal obligation to which the Data Controller is subject; and Article 6(1)(d) which permits processing thatis necessary in order to protect the vital interests of the data subject or of another person.

In certain instances, GBS will act as a joint controller of personal data whereby GBS together with other entities (e.g. external HRM contractor) determines the means and purposes of the relevant processing. In such circumstances, the essence of the arrangement as between GBS and the other Joint Controllers will be made known to the relevant individuals in a transparent manner. Examples of such scenarios may include where GBS and other institutions engage in collaborative research projects or admission of learners.

8.6.2 GBS as a Data Processor

In some cases, GBS may act as a Data Processor, under the instructions of a Data Controller. Data Processors are persons or organisations that process personal data on behalf of a controller (e.g. payroll contractor). The GDPR defines data processing as any operation(s) performed on personal data, e.g. collecting, storing, distributing or destroying. Many controllers also process personal data and do not require a separate data processor.

When acting as a Data Processor, GBS complies with its relevant obligations under Data Protection Law. These include ensuring that the data that is processed by GBS on behalf of the relevant Data Controllers is subject to appropriate technical and organisational measures to ensure a level of security appropriate to the risk and ensuring that the processing is underpinned by a contract which includes the data protection provisions required by Data Protection Law.

8.6.3 Purposes of Data Processing

Much of the data Processing undertaken by GBS is for the purpose(s) of fulfilling GBS's statutory functions, and objects under the QQI Approved Quality Assurance Procedures. The following are illustrative and non-exhaustive examples of the types of public interest Processing undertaken by GBS:

(a) **Examinations and Academic Records:** One of GBS's core functions to provide courses of study and to conduct examinations for the purpose of QQI award degrees and other qualifications. Accordingly, the processing of Personal Data, including but not limited to student numbers, names, exam scripts, exam results, details of qualifications and degrees conferred is necessary in order for

GBS to perform these functions. To ensure the integrity of this system, it is also necessary and proportionate for GBS to maintain records of exam results, degrees conferred and other relevant details. GBS Processes such as Personal Data in accordance with this Privacy Policy and its other policies, regulations and procedures, including the Examination Appeals Procedure.

(b) **Registry:** In administering the GBS in such a manner as to enable GBS to provide courses of study in an efficient manner it is necessary for GBS to Process Personal Data, including the full student record. Academic Coordinator and Registry may also process personal data of a sensitive nature which is provided by the student to GBS, for example, health data to support a deferral of an academic year or postponement of an assessment. This is clearly both necessary and expedient to further the objectives and development of the school per QQI regulations.

(c) **Alumni Affairs:** Among GBS's functions are to collaborate with graduates, convocations of graduates and with associations representing graduates both within and outside the State. This function provides appropriate support for Processing activities undertaken by GBS when liaising with and contacting GBS graduates in relation to their alumni events and initiatives.

(d) **Other Universities/institutions:** In accordance with its objects and functions to promote and facilitate the highest standards in, and quality of teaching, and to collaborate with educational, business and other institutions both within and outside the State, GBS will engage in certain collaboration with such organisations. Such collaborations may involve the sharing of certain personal data as between GBS and its international educational partner institutions and other organisations. Personal Data of students and staff may be disclosed to such other institutions as necessary for the purposes of enrolling the students and marketing, and written agreements will be put in place.

8.6.4 Special Categories of Data

GBS processes Special Categories of Data (SCD) in certain circumstances, typically related to the ordinary course of employee and student administration, the provision of student support and development services and the processing of Garda vetting forms for students and employees, where required by law.

Section 41 of the Data Protection Act 2018 provides a general lawful basis for processing SCD where it is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the controller or the data subject in connection with employment or social welfare law. As required by Data Protection Law, GBS applies suitable and specific measures in respect of such Processing of SCD.

GBS Processes Garda vetting forms for students and employees as authorised by the NationalVetting Bureau (Children and Vulnerable Persons) Act 2012 (the "National Vetting Act") in respect of GBS students and staff that undertake placements or volunteering and studies which involves engagement with children and vulnerable persons. Garda vetting forms may contain Personal Data relating to criminal convictions/offences and because GBS is subject to a legal obligation to process such data, Art, 6(1)(c) of the GDPR provides the lawful basis for such processing.

8.7 Records Maintenance and Retention

As part of our record-keeping obligations under Article 30 of the GDPR, GBS retains a record of the processing activities under its responsibility. This Policy applies to GBS and all staff, employees, officers and contractors engaged by GBS. This section is concerned with the retention and destruction of Personal Data (e.g. documents, records, emails and correspondence, files, audio visual files and recordings and any other forms of information and records regardless of their format together referred to as 'data'). Having regard to the principles contained in Article 5(1) of the General Data Protection Regulation (EU No. 2016/679) ("GDPR"), it is the duty of GBS to:

- retain personal data in identifiable form only for such period as is necessary in relation to the purpose for which the data are processed
- ensure that personal data retained by GBS is adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed
- take all reasonable measures to ensure that personal data retained by GBS are accurate

This policy applies to any type of data created, received, transmitted and retained in the context of GBS's day to day activities and any other data processing undertaken by GBS, regardless of the format. Therefore, any data in paper or electronic form must be retained for the period indicated in Table 9.7 below. Data should not be retained beyond this period unless a valid operational reason (or a litigation hold or other exceptional situation) calls for its continued retention.

8.7.1 Data Ownership

All data, irrespective of format, generated, created, received and/or retained by GBS is the property of the school and subject to its overall control. GBS Personnel leaving GBS are not to remove any data.

8.7.2 Data Storage

GBS's records must be stored in a safe, secure and accessible manner to ensure the security and confidentiality of such data in accordance with GBS's Data Privacy Policy in Section 9.6. Special care

is to be taken to ensure that information of a sensitive nature, in particular, information that constitutes a special category of personal data under the GDPR, is stored in a secure manner which may include, for example, locked filing cabinets and offices for hard copy data and/or the use of password protection and encrypted files for data stored in electronic form. The table below presents the data retention periods implemented by GBS for various types of data:

Table 9.7: GBS's Data Retention Periods

HR Data	
Type of Personal Data	**Retention Period**
Annual Leave and Public Holiday records	6 years
Carer's Leave records	8 years
Parental Leave records and Force Majeure Leave records	8 years (Parental Leave Acts, section 27)
Hours Worked and related information such as annual leave	3 years (The Organisation of Working Time Act, Section 25)
Payslips	3 years (National Minimum Wage Act, Section 22)
Taxation records	6 years (Companies Acts and Taxes Consolidation Act)
Accidents	10 years (The Safety, Health and Welfare at Work Act, Section 60)
Employee contract	3 years from the date of termination of the employment
CV and interview notes of unsuccessful applicants	3 years (National Minimum Wage Act, Section 22)
Signed Documents	6 months
Learner Data	
Type of Personal Data	**Retention Period**
Records relating to summative assessment results	Permanently retained (Assessment and Standards, Section 4.5.2)
Records contributing towards module grade	One year after Graduation
Research Thesis	Permanently retained
Broadsheets	Permanently retained
Records of successful learner applicant	Duration of Studies + 3 years
External Examiners' reports	Permanently retained
Deferral, withdrawal and application for transfer	Duration of Studies + 1 year
Board of Examiners meeting records	Permanently retained
Module Reports	Permanently retained
Quality Assurance Data	
Type of Personal Data	**Retention Period**
Minutes of QA meetings	Permanently retained
Record of amendments to the QA system	Permanently retained

8.7.3 Data Destruction

Once Data have met their required retention period it should then be transferred to the GBSapproved archives or deleted or destroyed as follows:

- Hard copy files: to be destroyed by confidential shredding or by using the services of an approved confidential waste disposal firm.
- Electronic files: to be purged or deleted from all relevant systems on which such Data is stored and/or databases.
- Data stored in other media: to be deleted or destroyed in a safe and confidential manner to ensure the content is not disclosed.

It is the responsibility of each GBS department to ensure that personal data is retained by that department in compliance with this policy and to ensure that all GBS Personnel under their responsibility complies with it.

8.8 Data Protection

This document is the GBSs policy in response to the requirements of the Data Protection Acts. GBS is required by law to comply with the following Irish legislation relating to the processing of Personal Data:

- General Data Protection Rregulation (2018)
- The Data Protection Act 1988 (The Principle Act)
- The Data Protection (Amendment) Act 2003

8.8.1 Scope

In order to sustain competitive advantage, GBS needs to collect and process personal information relating to many categories of people, which include the students and staff of the school. GBS takes the confidentiality of all personal information particularly seriously and consequently takes all reasonable steps to comply with the principles of the Data Protection Acts. The school aims tocollect personal information only in order to meet specific legitimate purposes and to retain that information only for as long as those purposes remain valid. Ordinarily, the school will not pass personal information to any third party, except where required by law.

GBS is committed to ensuring that all employees, registered learners, agents, contractors and data processors comply with the Data Protection Acts regarding:

- the processing and confidentiality of any personal data held by the school
- the privacy rights of individuals under the legislation

8.8.2 Data Protection Principles

To comply with the law, information (as defined by the Data Protection Acts) must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the school must comply with the following Data Protection Principles or Obligations:

- The data must be obtained and processed fairly and lawfully
- The data can only be obtained for specified, lawful and clearly stated purposes

- Processing and Disclosure of personal data should not be incompatible with the specified purpose for which it was obtained.
- The data must be kept safe and secure. GBS is responsible for applying adequate security structures to prevent unlawful or inadvertent processing, alteration or loss of the data.
- The data must be kept accurate, complete and where necessary up-to-date.
- The data obtained should be adequate, relevant and not excessive
- The data should not be kept for longer than is necessary for the purpose or purposes for which it was obtained.
- The person to whom the information relates has a Right of Access. GBS must store and maintain the data in such a manner as to be able to respond to a Subject Access Request in a timely manner.

8.8.3 Disclosure of Personal Data

The legislation recognises two categories of Personal Data:

- Ordinary Personal Data such as name, address, mobile phone number, car registration, PPS Number.
- Sensitive Personal Data, which is more deeply personal to an individual, such as their racial or ethnic background, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, the (alleged) commission of any offence, subsequent proceedings or sentence.

Sensitive personal data should normally only be processed if the data subjects have given their explicit consent to this processing. The legislation applies equally to automated and manual data, i.e.data held or processed on a computer, or data held in 'hard copy', stored in an indexed or relevant filing system.

The security of personal information in the possession of GBS is of paramount importance. In addition to the principles contained within this policy, staff are also advised to read and adhere to GBS's Data Classification Policy. All staff and students have an individual responsibility to ensure that they adhere to this policy and the Data Protection Acts.

8.8.4 Summary of Responsibilities:

8.8.4.1 School / Department Responsibilities:

- All personal data is processed within the School/Unit complies with the Data Protection Acts and this policy.
- All contractors, agents and other non-permanent school's staff used by the school, are aware of and comply with, the Data Protection Acts and this policy.
- All personal data held within the School/Unit is kept securely and is disposed of in a safe and secure manner when no longer needed.

8.8.4.2 Staff Responsibilities

- Personal data which they provide in connection with their employment is accurate and up- to-date, and that they inform the school of any errors, corrections or changes, for example, change of address, marital status, etc.
- Personal data relating to living individuals which they hold or process is kept securely
- Personal data relating to living individuals is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

8.8.4.3 Learner Responsibilities

- Personal data which they provide in connection with their studies is accurate and up-to- date, and that they inform the school of any errors, corrections or changes, for example, change of address, marital status, etc.

8.8.5 Rights under the Acts (1988 & 2003)

The Data Subject is entitled to:

- Access to a copy of any data held by GBS which relates to them including:
    - A copy of their personal data
    - The purpose of processing data
    - The categories of personal data concerned
    - To whom the data has been or will be disclosed
    - Whether the data has been or will be transferred outside of the EU

    - The period for which the data will be stored, or the criteria to be used to determineretention periods
    - The right to make a complaint to the Data Protection Commissioner
- Require that any inaccurate data held by GBS is corrected or erased
- Prevent the processing of the data likely to cause them distress or damage
- Prevent the processing of their personal data for the purposes of Direct Marketing

8.8.6 Procedures to access personal data held by GBS

Formal written application is made to the Registrar via email. The Registrar will respond within 14days from the date it receives the request with the following information:

- A copy of the personal data requested
- The purpose of processing data
- The categories of personal data
- To whom the data has been or will be disclosed
- Whether the data has been or will be transferred outside of the EU
- The period for which the data will be stored, or the criteria to be used to determine theretention period
- The right to make a complaint to the Data Protection Commissioner
- The right to request rectification or deletion of the data

Whether the individual has been subject to automated decision makin