DOCUMENTATION RETENTION AND SECURE STORAGE POLICY

Table of Contents

INTRODUCTION

The objective of this policy is to lay down rules about the proper storage of important and sensitive documents to the nature of company ownership and functions and those that relate to the academic operations of Britts Imperial University College. Through the implementation of this policy Britts Imperial University College will maintain a complete and accurate record of documents in physical or electronic form as the need may demand.

For the purpose of retention, records will be categorized into two major categories:

a. Documents which must be preserved permanently
b. Documents which must preserved for a specific period, as per differing regulations

Record of documents in the second category will be made until the period of their immediate use or for a longer period to serve the purpose of contractual, legal, or academic requirement for purposes which will be mentioned in detail in this policy. Records which have outlived their purpose, or the stipulated timeline will be destroyed and log of this will be maintained as also mentioned in detail in the policy.

No staff of Britts Imperial University College, irrespective of any position of authority will knowingly destroy or permit them to be destroyed before the required time is completed.

SCOPE

The policy covers all the documents and records of Britts Imperial University College to the nature of administrative and academic in nature.

This will include the records stored in either physical form or digital form or in a combination of both or as CCTV recordings. For records maintained in digital form, it will include database maintained at in-house servers or as secondary storages (eg. hard disks or digital tapes) or data maintained on external cloud server on contract for the purpose. This policy will cover physical records maintained in the premises of Britts Imperial University College or in a separate location as specified for this purpose. This policy will also cover all records maintained in either form before the creation and implementation of this policy.

A record may be defined either in the form of a physical document, contracts memorandum, an appointment book or an expense record. It will also include an e-mail on the official maid ID of the employees, data maintained on Google drives created or shared by employees or maintained on external hard drives or any other format that may be included in future due to advancement of technology, not covered in the scope section of this policy.

ROLES AND RESPONSIBILITIES

- The Board of Directors will have the ultimate ownership of all the records of the institution, irrespective of their nature or the way they have been maintained, as covered in the scope of this policy. The functional leaders in academic and administrative domains will be responsible for the day-to-day record keeping and maintain the timelines of records under this policy or the decisions of the Directors.
- All other staff, stakeholders and students are bounded by the responsibility to read and understand the content of this policy

AIMS AND OBJECTIVES OF THE POLICY:

1. As per corporate laws the legal entity that owns Britts Imperial University College will have to maintain original records pertaining to creation and ownership of the organization.
2. Under partnership with different universities the assessment proofs of the students will have to be maintained for a specified amount of time.
3. The policy will also guide relationship with outsourced partners who have been assigned the task to maintain records in physical or digital formats.
4. It should be noted that failure to maintain records as per stipulated norms of the legal, tax or accounting authorities may result in penalties, fines or even loss of rights to operate the organization legally. It may also impact submission of evidence in

statutory audit enquiry or in legal cases. Any such possibilities will lead to serious disadvantages to the organization and may even result in extended litigations.

5. Failure to maintain records as per stipulated norms as specified by universities or other academic partners may result in delay of student results or appeals on results.
6. Maintaining secrecy of personal information of staff and students will of supreme importance in the process of storage and disposal of personal information. No staff will ever share or disclose any personal information to any external individual or agency.
7. Britts Imperial University College expects all that staff will fully comply with this Policy.

POLICY DETAILS:

Types of documents:

a. Documents which must be preserved permanently (Retained)

i. This will include all documents and records related to the formation of the company that owns Britts Imperial University College at the time of drafting of this policy or any other later. It will include the following: Company incorporation certificate, GST / Corporate Tax number Certificate, Memorandum and Articles Association, Directors DIN Certificates, Share certificates

ii. Other legal and accounts documents Digital signature dongles, Trademark certificates, Statutory Audit reports, legal correspondences, Documents that deal with maintenance of bank accounts

iii. HR related: Employee appointment, termination increment letters

iv. Administrative in nature: Asset register, purchase and disposal records of assets, record of disposal of temporary records.

v. Original Partner deeds with universities, rental agreements, rental cancellation agreements.

vi. All such documents will be maintained in safe lockers to be owned by the Directors or the Chief Accounts Officer. Scanned copies of these will also be maintained on cloud servers with exclusive sharing rights owned by the above two members. Due to regular use of Digital signature dongles, they can be delegated to the responsibility of accounts staff to be retrieved only with the permission of the line manager.

vii. Student result sheets: to be maintained in digital form on cloud

viii. The retrieval of the above originals will only be with the permission of the Directors or any other staff who have been delegated with the responsibility to manage their storage.

ix. All such records when maintained in digital form will have editing rights of only:
Directors on records related to company formation, Accounts managers for accounts related, Dean for all student related and Admin In-charge for

asset related. All other staff may be given individual viewing or download rights for specific durations.

x. In case there is any change of Directors or staff in the category of ownership of the records, physical or digital, then a proper handover needs to be taken at the time of exit and a handing over to the new staff in charge.

xi. If the digital copies are maintained on an inhouse server, then an NDA has to be signed by the IT head and the staff involved in the maintenance that none of the data will be retrieved and shared, internal or external, without the permission of the appropriate authority.

xii. If the digital copies are maintained on an external cloud, then an undertaking is required from the vendor that none of the data will be visible to any external entity or individual engaged in the design, uploading or cloud maintenance of the data at any point of time.

xiii. The management reserves the right to change the category of any record for a temporary or permanent time.

b. Record retention schedule for all documents which have to be preserved for a specific period of time (Temporary):

Major category	Sub type	Form of storage	Ownership	Duration
Student records	Admission enquiry forms	Physical	Admission office	12 months from admission
	Admission forms	Physical and Digital	Admission office	5 years from admission on 3 years from exit of student, which is later
	Visa letters	Physical and Digital	Admission office	3 years from exit of student
Academic records	Annual academic plans for all programs	Digital	Academic Head	3 years from the end of the academic year
	Lesson plans	Digital	HODs	To be renewed annually, else 3 years from the end of the program
	Training content: ppts, videos, etc.	Digital	HODs	To be renewed annually, else 3 years from the end of the program
	Student reference material: handouts, class assignments	Digital	HODs	To be renewed annually, else 3 years from the end of the program
	Assignment briefs	Digital	HODs	3 years from the end of the batch
	Student work: *multiple submissions*	Digital	HODs	5 years from results
	Faculty assignment response sheets: *multiple responses*	Digital	HODs	5 years from results
	Student craft work as assignment for assessment	Physical and Digital	HODs	Physical craft work if not submitted to the University, will be returned after declaration of results. Digital copy: 5 years from results
	Result records	Digital	Academic Head	
Accounts records	Ledgers and schedule; *including student fee records*	Digital on accounts software	Accounts head	8 years from close to accounting year
	International remittance	Digital	Accounts head	8 years from close to accounting year
	Cheque book, empty	Physical	Accounts head	3 years from close of accounting year
HR records	Employee applications	Physical	HR Head	3 years
	Performance records	Digital	HR Head	3 years
	Payroll records	Digital	HR Head	8 years
	PF, Gratuity, ESIC	Digital	HR Head	8 years
	Student feedback of faculty	Digital	HR Head and Dean	3 years

	Staff development programs	Digital	HR Head / Line managers	3 years
Administrative records	AMC documents	Physical and Digital	Line managers	3 years from expiry of AMC
	Contract and leases - expired	Physical and Digital	Line managers	8 years from expiry of AMC
	Insurance policies – expired	Physical and Digital	Line managers	3 years from end of term
	Meeting minutes books	Digital	Line managers	3 years
	Images of functions and events	Digital	Marketing	3 years from the event

POLICY OF E-MAILS:

All exchange and storage of mails on the company mail IDs, is considered to the property of the organization. All mails sent by staff are also considered to represent the outlook of the company about mail communication. Therefore, staff should avoid using official mails for any personal communication.

In addition, the exchange of e-mail communication cannot be related to privacy of the staff, the senior management has the right to access the official mails of any staff under circumstances of possible leak of sensitive data, collect evidence on the staff using official mails for personal benefits or making personal contacts. Such an access will not require any permission or prior notice to the concerned staff.

All e-mail communication should also be retained as per the schedule presented earlier for retaining temporary data. Mails related to permanent data should never be deleted. All staff should inform their Line managers about their mail ID's storage quote reaching the maximum limit well in advance. In such cases either a new mail ID will be created with an auto-forward from the original one or additional space will be purchased, as the case may demand.

In case any staff decides to exit from the organization, he / she will not resort to deleting any email before or after the formal handover.

PROVISION FOR USE OF EXTERNAL CLOUD FOR RECORDS:

In case the institute adopts the use to an external cloud base, the following need to be ensured in terms of data secrecy:

1. The credentials of the vendor should be confirmed through external feedback, especially past and current clients. If possible, feedback from cyber-crimes section should also be solicited.
2. Any cloud space taken for this purpose should be on non-sharing terms, at times vendors use artificial servers' partitions which makes data secrecy at risk.
3. The privacy of personal data of staff and students has to be maintained; therefore, all data entry work should always be done inhouse, this should never be outsourced.
4. The vendor needs to sign an NDA about not sharing any part of this data to its team of developers or maintenance staff or the company which owns the server space.
5. The cloud should have differing levels of access to staff who can make changes or just view records.
6. The cloud should have a feature to record all login, view and edit activities.
7. In case of cancellation of the vendor agreement or the vendor closing his services, all data should be returned to Britts Imperial University College in its latest and original form and all copies should be permanently deleted from the cloud under observation of authorised staff.

THIRD PARTY DATA SHARING

Where there will be a need to share a part of data with any third party, they will have to follow the policy on data retention as presented in this policy. This sharing will be bounded by a legally bounded NDA and all exchanges will need to be recorded on purpose of such an exchange, person who has authorised the exchange, the duration for which the data was in the possession of the third party, the state in which data was shared and the state in which it was returned. Any personal data will never be shared with any third party unless defined by contract

DISPOSAL OF RECORDS

All disposal of records will be recorded, and the record will be maintained as permanent, no portion of the disposal record will ever be deleted. All physical records in the temporary category will be cross shredded in the physical presence of the concerned Line manager and his/her consent will be recorded. In case of records being on digital format they will be removed from the internal server or the cloud under the supervision of the concerned line manager and a record of this deletion will be maintained. For such deletions the IT Department shall use the permanent delete command to permanently dispose of digital records.

CLOSED CIRCUIT TELEVISION (CCTV)

All CCTV recordings will be deleted after a period of 6 months unless there is an advance notice from the management or an external official authority for the purpose of evidence collection for an investigation. CCTV recordings will only be shared with third parties only under permission from the IT head and under legally binding situations.

IMPLEMENTATION OF THE POLICY

The implementation of the policy though owned by the Board will be functionally driven by the Functional and Line managers through delegation of work to identified team members. Failure to comply with this policy may result in disciplinary action which may be bounded by the cyber security laws of the land at the time of violation being committed.

TRAINING TO RAISE AWARENESS

The HR department will ensure a session in the staff induction program to read out the contents of the EDI policy to the new joiners. Similarly, the Dean / Academic head will guid the student support to ensure that all students have read and understood the contents of this policy.

POLICY REVIEW

The contents of this policy will be reviewed before the end of every academic year, by providing enough time to involve the feedback of the staff and students and make changes so the new policy document is ready well before the commencement of the new academic year.

FURTHER INFORMATION

Any further information or clarity about the content of the policy can be obtained from:

Mr. Gladwyn Victor
Contact: +971585046263