INFORMATION TECHNOLOGY POLICY AND GUIDELINES

**LOYOLA INSTITUTE OF BUSINESS ADMINISTRATION
CHENNAI**

December 2018

TABLE OF CONTENTS

1. Introduction and policy statement

1.1 This document sets out the Information Technology (IT) Policy for LIBA for the protection of its IT equipment's systems and defining baseline responsibilities for IT equipment's security, equipment and file storage. "IT equipment's" refers to the LIBA IT network, hardware including portable media, system and application software, systems, documentation, physical environment and other information assets. It does not include IT systems not owned by the LIBA IT network.

1.2 This Policy covers the IT networks for LIBA staff across all sites and the separate network provided for Evidence & Practice Information Management and Technology in order to manage LIBA websites and publishing systems.

1.3 The equipment covered by this policy includes:

Network Infrastructure – The equipment housed internally to provide the LIBA IT network, including servers, enclosures, racks, cabling, switches/hubs, Routers, wireless access points, firewalls, proxies, authentication systems and devices, media converters.

- ❖ Desktops – Personal Computers provided to faculties, staff and students in the course of carrying out their duties
- ❖ Laptops/Netbooks - Portable Personal Computers issued to faculties and staff in the course of carrying out their duties
- ❖ Mobile Phones - Digital communication devices issued or provided to staff in the course of carrying out their duties
- ❖ Desk/Conference Phones – Telephones/Voice Communication devices connected to the Network Infrastructure including desk telephones, conference telephones (star phones), analogue telephony adaptors, DECT telephones (cordless)
- ❖ Media/Portable Media – Electronic Storage Devices such as DVDs, CDs, memory sticks and hard drives issued or provided to staff in the course of carrying out their duties
- ❖ External Communications Infrastructure – Equipment used to connect LIBA to the external world including the Wide Area Network, analogue telephone lines, digital telephone lines, leased lines, LES/WES/Ethernet first mile circuits, ADSL circuits, SDSL circuits and all related equipment and services.
- ❖ All related Facilities& Estates controlled IT media used in LIBA's meeting rooms

1.4 The objective of this policy is to ensure: The confidentiality of data and information assets are protected against unauthorised disclosure and incidents are promptly reported the integrity of data and information assets so that they are protected from unauthorised or accidental modification the availability and accessibility of IT systems as and when required by staff.

1.5 This policy sets out the principles of IT security including the maintenance, storage and disposal of data and explains how they will be implemented at LIBA to ensure there is a centralised and consistent approach to IT security.

1.6 One of the aims of the policy aims to raise awareness of the importance of IT security in the day to day business of LIBA.

1.7 The policy supports the LIBA business objectives of ensuring that the security, integrity and availability of IT systems are balanced against the need for staff to access systems and services that are necessary for their job, within the limits imposed by this policy. It will also help to protect data from misuse and to minimize the impact of service disruption by setting standards and procedures to manage and enforce appropriate IT security.

1.8 The policy supports the legal obligations of LIBA to maintain the security and confidentially of its information, notably under the Data Protection Act 1998, the Copyright Patents and Designs Act 1988 and the Computer Misuse Act 1990, and also supports adherence to information governance standards set by the Department of Health (DH).

2. Scope

2.1 This policy applies to all LIBA IT systems and those working at or for LIBA (Users): All LIBA employees (including LIBA staff on secondment to other organisations)

- Agency workers
- Contractors, where they are directly using LIBA's network.
- Secondees (those who are seconded to LIBA from other organisations) with authorised access to the IT network.

3. Responsibilities

3.1 Defining responsibilities ensures that all users of LIBA IT systems are aware of their responsibilities to minimize the risks to IT security and operations.

3.2 The Business Planning and Resources Director is responsible for ensuring that:

- Electronic filing systems and documentation are well maintained for all critical job functions to ensure continuity;
- No unauthorised staff are allowed to access any LIBA IT systems in any location, as such access could compromise data integrity confidentiality;
- Named individuals are given authority to administrate specific computer systems according to their job function and role following the principle of least privilege;
- Robust disaster recovery and business continuity procedures are in place;
- All current and new users are instructed in their security responsibilities;
- Procedures are implemented to minimise LIBA's exposure to fraud, theft or disruption of its systems; these include segregation of duties, dual control and staff rotation in critical susceptible areas.

3.3 The LIBA IT department has the following responsibilities:

- Day to day responsibility for the management and security of the systems, equipment and services laid out in section 1.3, with specific technical responsibilities being allocated across the team and to outsourced service providers.

- To make all users aware of this policy and to ensure that users understand and are able to abide by them when carrying out work on LIBA's behalf.
- Monitoring and reporting on the state of IT security within LIBA and across all LIBA systems.
- Developing and enforcing detailed procedures to maintain security access to all LIBA systems.
- Ensuring compliance with relevant legislation, policies and good practice for all internal systems.
- Monitoring for actual or potential IT security breaches for all internal systems. And reporting to the appropriate people as need be.
- Maintaining an IT asset register (see section 5.1).
- The allocation/disposal/reallocation of all computer hardware and software to ensure best practice usage, value for money and that all data storage devices, including portable electronic media, are purged of sensitive data (such as confidential or personal information) before disposal or reallocation.
- Determining whether or not there is evidence of negligence in use of IT equipment, and reporting any such evidence in accordance with the Incident Reporting procedure.
- Purchasing all computer equipment and software/license to ensure value for money, consistency and compliance.

3.4 LIBA Evidence and Practice department has the following responsibilities:

- Day to day responsibility for the management and security of the Evidence and Practice Infrastructure and systems, along with any externally hosted or supplied systems and services. Specific technical responsibilities will be allocated across the IT Operations team and to outsourced service providers.
- To ensure all Users and Systems comply with this policy and further directions that comply with this policy as issued by the CIO for Evidence and Practice from time to time
- Monitoring and reporting on the state of IT security within the LIBA IT systems for which they are responsible.
- Providing information on a timely basis to the LIBA IT team to maintain a single asset register for LIBA
- Ensuring compliance with relevant legislation.
- Monitoring for actual or potential IT security breaches within the LIBA IT systems for which they are responsible. And reporting to the appropriate people as need be.
- Determining whether or not there is evidence of negligence in use of IT equipment, and reporting any such evidence in accordance with the Incident Reporting procedure.
- Ensure any and all information as reasonably required by the Business Planning and Resources Director is provided to fulfil its compliance roles.

3.5 The Human Resources department is responsible for ensuring that:

- All LIBA staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment, and any contactors, temporary staff (including agency staff) and secondees sign LIBA's standard confidentiality undertaking before they are permitted to use LIBA systems.

- The LIBA IT and Evidence and Practice department are both notified immediately via the Starters / Leavers / Changers process about changes to user permissions so that access to the IT network can be amended as appropriate. This may include any instance where a member of staff is temporarily suspended from their duties.
- New staff are given basic user training in IT Security as part of their induction.

3.6 Users who **do not** have administration rights over their issued equipment are responsible for ensuring that:

- No breaches of computer security arise or result from their negligence.
- Users are specifically reminded to keep all passwords and remote log- in data secure (except where necessary to disclose them to the IT department for administrative purposes) and to deny unauthorised third party access to LIBA systems. This is particularly important for home workers and when using wireless networks.
- All reasonable care is taken to protect the security of IT equipment they are issued together with confidential data stored on it when taken outside secure offices.
- All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the LIBA IT department regardless of the working state of the equipment.
- Contractors engaged by LIBA are provided with and are to comply with this policy.
- Sensitive data stored on portable IT equipment is kept to the minimum required for business use and encrypted in order to minimise the risks and impacts should a security breach or loss of that equipment occur.
- Actual or suspected security breaches are reported as soon as they arise.
- Only staff explicitly authorised by the LIBA IT dismantle, repair or alter LIBA supplied equipment.

Further advice is contained in Appendix A.

3.7 Users who **do** have administration rights over their issued equipment are responsibility for ensuring that:

- No breaches of computer security arise or result from their negligence.
- Users are specifically reminded to keep all passwords and remote log- in data secure (except where necessary to disclose them to the LIBA IT or Evidence and Practice department for administrative purposes) and to deny unauthorised third party access to LIBA systems. This is particularly important for home workers and when using wireless networks.
- All reasonable care is taken to protect the security of IM&T equipment they are issued with together with confidential data stored on it when taken outside secure offices
- All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the LIBA IT department regardless of the

working state of the equipment.

- Contractors engaged by LIBA are provide with and comply with this policy.
- Sensitive data stored on portable IT equipment is kept to the minimum required for business use and encrypted in order to minimise the risks and impacts should a security breach or loss of that equipment occur.
- Actual or suspected security breaches are reported as soon as they arise.
- Only licensed or in house developed software, specifically required for their job within LIBA, is installed upon the equipment for which they are responsible
- The equipment for which they are responsible for is only used for work purposes (no private use) and specifically their own job.
- All due skill, care and attention is taken to ensure that no virus, Trojan spyware or other malware is introduced to their equipment or LIBA systems
- All due skill, care and attention is taken to ensure that no configuration, mis-configuration or alteration to systems, software, equipment or
- infrastructure has a detrimental effect on the normal running, availability or stability of the LIBA IT Infrastructure as detailed in section 1.3
- Only staff explicitly authorised by the IT Director for Operations can dismantle, repair or alter LIBA supplied equipment.

Further advice is contained in Appendix A.

4. Security

4.1 Technical security measures will be put in place to protect LIBA systems from viruses and other malicious software, and all IT systems will be monitored for potential security breaches.

4.2 Contact will be maintained with the appropriate organisations to ensure that LIBA IT systems comply with National standards and best practice regarding IT security management

4.3 Email and internet use will be governed in accordance with the Email and Internet policy.

4.4 Allocation of accounts to temporary workers using a generic username that cannot be mapped back to the user will not be allowed.

4.5 All relevant contracts with third parties will include standard Office of Government Commerce clauses on information security. All central processing equipment, including file servers, will be covered by third party maintenance agreements.

4.6 All connections to external computer networks and systems including privately owned IT equipment of all kinds must be approved by the LIBA IT department and Evidence and Practice Operations department.

4.7 All IT equipment, including virtual systems, will be uniquely identified and recorded.

4.8 Environmental controls will be maintained in the server/communications rooms of all premises to protect key equipment. Smoking, drinking and eating is not permitted in these areas.

4.9 Records of all faults and suspected faults will be maintained.

4.10 All LIBA laptops must be encrypted with access to LIBA IT networks via using a strong authentication method.

4.11 Access to premise server/communications rooms will only be with the express permission of the LIBA IT Department and accompanied by the appropriate representative.

4.12 Memory sticks and other portable media must be encrypted or have password protection when sensitive data is being transported outside secure offices.

5. Software protection

5.1 Only licensed copies of commercial software or in house developed software are used by LIBA. The LIBA IT department will maintain a register of all commercial software, including all software licenses, to ensure that LIBA complies with licence conditions and relevant law. Users must not install ANY externally developed software on LIBA IT equipment without prior approval of the IT department or where delegated, the Evidence and Practice department

5.2 All users are reminded it is a criminal offence to make or use unauthorised copies of commercial software and that offenders may be liable to disciplinary action.

5.3 Software products required by any department should be approved by the LIBA IT Department or Evidence and Practice Operations prior to purchase. Unless otherwise directed all software purchasing and licensing will be carried out by the LIBA Procurement department, and users must follow any instructions issued with regard to specific software or applications.

5.4 LIBA will minimise the risks of computer viruses through education, good practice and procedures, and application of robust anti-virus software and ensuring firewall policies follow appropriate national guidelines. Users must report any detected or suspected viruses, Trojan, spyware or malware on their computers immediately to the LIBA IT Department or Evidence and Practice Operations as appropriate.

6. Physical access controls

6.1 Physical access controls to secure areas will minimise the threat to the LIBA IT systems through damage or interference. The LIBA IT department will be responsible for access to all IT systems located in secure areas, with access being restricted using the principle of **least privilege**. An entry restriction system to the server/communications rooms at all premises will be implemented.

6.2 The server/communications rooms and store rooms for IT equipment will be locked at all times and the keys/codes held securely by the LIBA IT department.

6.3 Authenticated representatives of third party support agencies or other parties will be given access through specific authorisation from the Procurement and IT Manager and will be supervised by LIBA IT department representatives while on site.

6.4 No remote access to LIBA IT systems will be given to third parties at any time unless specific authorisation is received from the Procurement and IT Manager or the Director of Evidence and Practice Operations. Such access if granted must be supervised at all times.

7. User access control to the IT network drives

7.1 User access to the IT network drives will be granted where access is necessary to perform the person's job following the principle of least privilege. Access will be modified or removed as appropriate when a person changes job or leaves LIBA. It will be the responsibility of the HR department to notify the LIBA IT department and the Evidence and Practice Operations department immediately of any changes required to access controls, and procedures will be established between the three teams to ensure this happens.

7.2 For those with existing access to the IT network, requests to change access permissions should be made to IT. These will be authorised by the Procurement and IT Manager who will, if necessary, check the requirement with the relevant Director or line manager.

7.3 No individual will be given access to the IT network unless properly trained and made aware of his or her security responsibilities.

7.4 Each member of staff will be provided a storage space on their 'Z drive'. This storage space is free for the individual to use (subject to sections 7.5 & 7.6 below). If this storage limit is exceeded then the Z drive will be unable to save any additional data – it is individual's responsibility to manage this allocation.

7.5 'Z drives' remain part of the LIBA IT systems and LIBA has full rights of access to all data stored on its IT network. The content of Z drives is not routinely monitored but LIBA reserves the right to view content if there are reasonable grounds for doing so; for example to prevent fraud or suspected breach of LIBA policies. Further information is contained in the Email and Internet policy.

7.6 Users are not permitted to store entertainment files (including music, pictures, video, electronic games) upon the LIBA systems. Files which have the same nature but are for work purposes must be notified to and approved via the LIBA IT department

8. Disposal/reallocation of equipment

8.1 Equipment allocated to an individual user (including memory sticks) must not under any circumstances be reallocated within a department (or any other user) and must always be returned to LIBA IT for reallocation to ensure correct management of sensitive data

8.2 Where equipment is obsolete for LIBA's business purposes but is still in working order and is deemed to be of use to private individuals, that equipment may be offered for sale to LIBA staff without any guarantees or warranties. The Finance Department will be notified of any sums due from the buyer of the equipment.

8.3 Where the equipment is deemed to be of no use to private individuals, it will be either disposed of by the Disposal Service Agency (or successor organization) or returned to the manufacturer in accordance with the Waste Electrical and Electronic Equipment Directive ("WEEE"). Alternatively it may be passed on to a properly registered charity who will seek to reuse the equipment. As a last resort the equipment will be passed to a properly registered waste carrier for certified recycling.

9. Security incident investigation and reporting

9.1 The objective of security incident investigation is to identify detect, investigate and resolve any suspected or actual computer security breach.

9.2 A security incident is an event that may result in:

- degraded system integrity
- loss of system availability
- disclosure of confidential information
- disruption of activity
- financial loss
- legal action
- unauthorised access to applications, files and folders
- loss of data

9.3 Incidents should be notified to the Procurement and IT Manager or the Director of Operations as appropriate who will report incidents to the Business Planning and Resources Director and the Audit Committee, in accordance with Incident Reporting Procedure. All security incidents that may have an impact on connectivity will be reported immediately, by the Procurement and IT Manager, to the Helpdesk.

9.4 All users must report actual security breaches, or any concerns or suspicions about security breaches, as soon as they arise.

9.5 All actual security incidents will be formally logged, categorised by severity and actions recorded by the LIBA IT department, and reported to the Business Planning and Resources Director and the Audit Committee in accordance with Incident Reporting Procedures.

10. Disaster recovery and business continuity

10.1 All business critical data will be replicated between servers at relevant locations so that if the servers in one location become unavailable, access is automatically switched to the servers in another location.

10.2 All data will be backed up onto archive libraries at each site so that data exist in four places (server and tape library at each site). Critical computer equipment must be fitted with battery back-ups (UPS) to ensure that it does not fail during switchovers or emergency shutdowns.

10.3 To minimise the risk to LIBA IT systems, robust disaster recovery plans will be put in place to ensure:

- ❖ identification of critical computer systems
- ❖ identification of areas of greatest vulnerability and prioritisation of key users and user areas
- ❖ agreement with users to identify disaster scenarios and what levels of disaster recovery are required
- ❖ development, documentation and testing of disaster recovery plans, including identifying tasks, agreeing responsibilities and defining priorities
- ❖ recovery plans cater for different levels of incident, including loss of key user area within a building, loss of building(s), loss of a key part of the IT network, and loss of processing power
- ❖ the existence of emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery
- ❖ personnel) and actions to be taken to return to full normal service

11. Risk management

11.1 The objective of risk management is to identify, counter and report on actual and possible threats to IT systems.

11.2 Significant IT risks will be included in the LIBA risk register and will be made available to the Audit Committee.

12. Auditors

12.1 The implementation of LIBA’s IT policy and procedures may be subject to periodic review by both internal and external auditors and the subsequent recommendations will be agreed and action plans put in place and monitored.

13. Compliance

13.1 Breach of this policy may result in disciplinary action in accordance with the LIBA Disciplinary Policy and Procedure. Any breach of the law will be reported to the appropriate authorities.

14. Related Policies

14.1 This policy should be read in conjunction with the following LIBA policy and procedure documents:

- E Mail and Internet Policy
- Disciplinary Policy and Procedure Incorporating Suspension Guidelines
- Incident Reporting Procedure
- Data Protection Policy
- Counter Fraud Policy
- Disaster Recovery / Business Continuity Plan
- Risk Management Policy
- Home Working Policy

15. Internet usage policy

15.1 LIBA faculties, staff, students and agents of outsourced support services may use our internet service for the following reasons:

- To complete their job duties.
- To use as a study and research tool.
- To use as an online collaboration tools or interface.

15.2 LIBA internet services are not to be used for the following reasons;

- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Online gaming.
- Pornographic content.
- Inappropriate use of social media web sites.
- Download or upload obscene, offensive or illegal material, engage in illegal activities.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.

15.3 Any use of our network and connection must follow our security and data protection policy. Users should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.
- We also advise our users to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask [their systems administrator.]

LIBA's IT department may install anti-virus and disk encryption software on our organization's computers. Users may not deactivate, configure or re-configure application settings and firewalls settings without approval of the IT department personnel.

LIBA's IT department will not assume any responsibility if user's devices are infected by malicious software, or if their personal data are compromised as a result of inappropriate use.

16. Organization issued equipment

16.1 LIBA expects its users to respect and protect the organization’s equipment. “Organization’s equipment” in this computer usage policy for users includes organization’s-issued desktops, laptops, tablets, mobile phones and any other electronic equipment, and belongs to our organization.

We advise our users to lock their devices in their desks when they’re not using them. Our users are responsible for their equipment whenever they take it out of their offices.

17. Email

17.1 Our users can use their corporate email accounts for work-related purposes as long as they don’t violate policy.

Users shouldn’t use their corporate email to:

- Register to illegal, unsafe, suspicious websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorized advertisements or solicitation emails.
- Sign up for services unless authorized.

LIBA’s IT department reserves the right to monitor corporate emails. We also have the right to monitor websites users visit on our computers.

18. Corporate email usage policy

18.1 Policy brief & purpose

- LIBA corporate email usage policy helps users use their organization’s email addresses appropriately.
- Our priority is to protect our confidential data from breaches

19. Scope

19.1 This policy applies to all fulltime students, faculties, staff and collaborators. This email may be assigned to an individual who fits in the above said groups and allocation of email id’s to collaborators will be decided by the management. (e.g. firstname.secondname or surame@liba.edu.

20. Policy elements

20.1 Users should use their organization’s email for work-related purposes.

- The IT committee will define what constitutes inappropriate and appropriate use.
- Inappropriate use of organization’s email
- Our users represent our organization whenever they use their corporate email

address.

20.2 LIBA reserves the right to monitor and archive corporate emails.

- ❖ Appropriate use of corporate email
- ❖ Users are allowed to use their corporate email for work-related purposes without limitations.
- ❖ Users must adhere to this policy at all times, in addition to our confidentiality and data protection guidelines.

21. Email security

21.1 Email is a most preferred medium for phishing attacks, confidentiality breaches, viruses and other malware. This can compromise the security of the system. Users must:

- ❖ Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information.
- ❖ Remember passwords instead of writing them down and keep them secret.
- ❖ Change their email password every two months.

Also, users should always be vigilant to catch emails that carry malware or phishing attempts. We instruct users to:

- ❖ Open emails that you are expecting to arrive.
- ❖ Be very cautious in opening emails from unknown senders.
- ❖ Pay attention to the email domain that is specified after @ symbol, if suspicious do not open.
- ❖ Avoid opening attachments and clicking on links when content is not adequately explained.
- ❖ Be suspicious of clickbait titles.
- ❖ Check email and names of unknown senders to ensure they are legitimate.
- ❖ Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If a user isn’t sure that an email they received is safe, they can ask our [*systems administrator*.]

We remind our users to keep their anti-malware programs updated.

Email signature
We encourage users to create an email signature that exudes professionalism and represents our organization. Salespeople and executives, who represent our organization to customers and stakeholders, should pay special attention to how they close emails. Here’s a template of an acceptable email signature:
[User Name]
[User Title], [Organization’s Name with link]
[Phone number] | [Organization’s Address]
[Disclaimer]
Users may also include professional images, organization’s logos and work-related

videos and links in email signatures. If they are unsure how to do so, they can ask for help from their supervisor.

22. Social media usage policy

22.1 “Social media” refers to a variety of online communities like blogs, social networks, chat rooms and forums. This policy covers all of them.

We consider two different elements: using personal social media at work and representing our organization through social media.

- Ensure others know that personal account or statements don’t represent our organization.
- Users should not state or imply that their personal opinions and content are authorised or endorsed by our organization.
- We advise using a disclaimer such as “opinions are my own” to avoid misunderstandings.

23. User confidentiality policy

23.1 Policy brief & purpose

LIBA’s **confidentiality policy** explains how we expect our users to treat confidential information. Users will unavoidably receive and handle personal and private information about students, faculties, staff and partners of our organization. We want to make sure that this information is well-protected.

We must protect this information for two reasons. It may:

- Be legally binding (e.g. sensitive personal data.)
- Constitute the backbone of our business, giving us a competitive advantage (e.g. business processes.)

23.2 Scope

This policy affects all users, who may have access to confidential information.

23.3 Policy elements

Confidential and proprietary information is secret, valuable, expensive and/or easily replicated. Common examples of confidential information are:

- Unpublished financial information.
- Data of Students/Faculties/Partners.
- Strategies, formulas or new technologies.
- Students data (existing and prospective)
- Data entrusted to our organization’s by external parties
- Marketing/ cost packaging and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives marked as confidential

Users may have various levels of authorised access to confidential information. What users should do:

- Lock or secure confidential information at all times
- Shred confidential documents when they're no longer needed
- Make sure they only view confidential information on secure devices
- Only disclose information to other users when it's necessary and authorized
- Keep confidential documents inside our organization's premises unless it's absolutely necessary to move them

What users shouldn't do:

- Use confidential information for any personal benefit or profit
- Disclose confidential information to anyone outside of our organization
- Replicate confidential documents and files and store them on insecure devices

When users stop working for our organization, they're obliged to return any confidential files and delete them from their personal devices.

23.4 Confidentiality Measures

We'll take measures to ensure that confidential information is well protected. We'll:

- Store and lock paper documents
- Encrypt electronic information and safeguard databases
- Ask users to sign non-disclosure agreements (NDAs)
- Ask for authorisation by senior management to allow users to access certain confidential information

23.5 Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons. Examples are:

- If a regulatory body requests it as part of an investigation or audit
- If our organization's examines a venture or partnership that requires disclosing some information (within legal boundaries)

In such cases, users involved should document their disclosure procedure and collect all needed authorisations. We're bound to avoid disclosing more information than needed.

23.6 Disciplinary Consequences

- Users who don't respect our confidentiality policy will face disciplinary and, possibly, legal action.
- We'll investigate every breach of this policy. We'll terminate any user who willfully or regularly breaches our confidentiality guidelines for personal profit. We may also have to punish any unintentional breach of this policy depending

on its frequency and seriousness. We'll terminate users who repeatedly disregard this policy, even when they do so unintentionally.

- This policy is binding even after separation of employment.

24. Organization's data protection policy

24.1 Policy brief & purpose

LIBA's **Data Protection Policy** refers to our commitment to treat information of users and stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

24.2 Scope

This policy refers to all parties (users, outsourced agents) who provide any amount of information to us.

Who is covered under the Data Protection Policy?

Users of our organization must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

24.3 Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our organisation collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

24.4 Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the organisation within its legal and moral boundaries
- Protected against any unauthorised or illegal access by internal or external parties

24.5 Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time

- Transferred to organisations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

24.6 In addition to ways of handling the data the organization's has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

24.7 Actions

To exercise data protection we are committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train users in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions will appear on our website.

24.8 Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

25. Review

25.1 This policy will be monitored by the IT department to ensure it is fit for purpose and reviewed every 3 years.

26. Signatories

Signed: ___________________________________ Date: _______________________ On behalf of the LIBA IT department

Signed: ___________________________________ Date: _______________________ On behalf of LIBA HR department

Signed: ___________________________________ Date: _______________________ On behalf of LIBA Administrative department

Signed: ___________________________________Date: _______________________ On behalf of LIBA Academic department

Appendix A

Good Practice Guide

Below is a summary of recommended Do’s and Don’ts for all users of LIBA systems. It is intended to complement approved LIBA policies and support new information governance standards set by the Department of Health.

- **Do** ensure you keep security in mind when working – If you have been sent a file or a web link, are you sure you can trust the person it came from, is this the type of thing they would normally send, does it ‘feel right’? Remember, lots of spam and viruses sent impersonate the e-mail address of a real person, so the e-mail may not have been sent by the person you think. Lots of viruses move from machine to machine as hidden files on storage devices. Remember, only IT equipment issued, or approved, by the LIBA IT department should be used, except where personal PCs and laptops are used in accordance with the Home Working policy.
- **Do** report any errors or problems promptly – If you have an error or an issue, especially if it may be security related, please report it to the IT helpdesk quickly and with as much detail as possible. Reporting that you had a problem 3 days ago and you can’t remember the error message makes it almost impossible to track and correct the problem. Reporting promptly with details of which system (e.g. terminal server, e-mail) was affected, the date and time the problem occurred and the specific error message or event makes it much easier to find and fix the problem, and get you working again.
- **Do** think about what you are saving and copying onto the network and in e-mail. Does the file need to be there? How big is it? If you are saving an attachment out of an e-mail, remember to delete the copy in the e-mail to save using up double the space. If you are copying data from a DVD, why is this necessary? If it is only for your use, can it stay on the DVD?
- **Do** take care of the equipment you are issued with, either permanently or on loan. Most of it is expensive and it may contain sensitive or confidential data.
- **Do** remember to return the equipment before leaving LIBA. All data will be securely erased by the LIBA IT department. Please note that any personal data that has not been erased from returned equipment may be viewed by the IT department.
- **Do** keep passwords secure and never disclose them to anyone else. Passwords should ideally contain at least 8 characters with a mix of letters and symbols in upper and lower case.
- **Do** keep portable media, especially laptops, taken outside LIBA offices secure at all times. For example, do not leave them in boots of cars overnight, in overhead luggage racks or unattended in other insecure areas. Where possible carry IT equipment in anonymous cases without a manufacturer’s logo and avoid using laptops in public places where possible if confidential information may be visible to other people.
- **Don’t** connect any equipment (Laptops, USB devices including storage devices, networking equipment, 3G cards etc.) to LIBA IT systems unless it has been supplied or specifically authorised by the LIBA IT department. If in any doubt, *confirm* with the helpdesk *before* connecting anything.
- **Don’t** download any Software, Software updates, Installation Packages, or Executable files from the Internet or external storage devices (USB sticks, external hard drives, CD-ROM, DVD etc.) onto LIBA IT systems unless specifically authorised by the LIBA IT Department.
- **Don’t** install any software on any LIBA IT systems unless specifically authorised by the LIBA IT department. All software installs are normally carried out by the LIBA IT department and user installation of software is only authorised in special circumstances.
- **Don’t** download, upload, store, copy or distribute any materials, data or software of a pornographic, obscene, indecent, racist, defamatory, libellous, sexist, offensive or otherwise

unlawful nature (other than for properly authorised and lawful research, for which written notification must be given to the relevant Director).

- **Don't** attempt to circumvent the security and restrictions in place on the LIBA IT systems. These are in place to ensure a safe working environment for all staff and maintain the security and resilience of the LIBA network.
- **Don't** leave portable media unattended in public places where there is a potential for opportunist theft or compromise (i.e. installation of a virus).
- **Don't** connect any LIBA issued equipment or storage devices into another computer or network unless you are happy the network is correctly maintained and up to date Anti-Virus protection is in place. Viruses can be transferred using machines and storage devices connected to compromised computers or networks.
- **Don't** use the LIBA network, including U drives, for the storage of music files, as these may breach copyright permissions. Private photographic and or video files should not be stored on U drives as they use up large amounts of space.

For further information and advice please contact the LIBA IT department or log a call on the IT Helpdesk.

Appendix B

Version Control Sheet

Version	**Date**	**Author**	**Replaces**	**Comment**

Loyola Institute of Business Administration
LIBA
★ Loyola Campus, Chennai-34 ★

Fr. P. Maria Joseph Christie, S.J

Director

DIRECTOR
LOYOLA INSTITUTE OF
BUSINESS ADMINISTRATION
LOYOLA CAMPUS
CHENNAI - 600 034