

## **Women Leaders in Technology (WLIT)**

### **Information and Communication and Technology Policy, 2022**

**Jan, 2022**

Prepared by:  
Sonika Baniya

---

## **Table of contents**

i. Preamble

ii. Objectives

iii. WLIT's ICT Policy

1. Data and its storage

1.1 What data do we collect?

- Fellows, programme participants, mentors
- Donors and Partners
- Newsletter subscriptions, event attendees
- General member intakes, staffs, volunteers

1.2 How data is used?

1.3 How to view and access data?

1.4 How to remove the data?

1.5 Data Breach response

1.6 Data security

- Password policy
- Digital Signature
- Email Security

1.7 Data Storage

2. Purchase and use of office resource policy

2.1 Software and Hardware purchase

2.2 Internet reimbursement

2.3 physical device procured under WLiT

3. Accessibility and Inclusivity

4. Ownership

iv. Exceptions to this policy

## Preamble

WLiT's mission is to build gender equal technical leadership with required mentorship and education. For this community to stand, we collect information so that we can provide you service. There is a need to ensure that all ICT resources are put to optimum use for the achievement of WLiT's overall objectives and goals. In doing so, it is imperative to have an ICT Policy that gives guidance on how the utilization of the various resources within WLiT and also how various procedures that affect the day-to-day interactions of the ICT management process shall be handled. This policy has been designed to ensure that there is an alignment of the ICT resources towards WLiT's overall goal.

This policy shall come into force after its approval by the board members of WLiT. In case of any dispute arising from the interpretation of the personnel policies, the board members will be consulted for the final decision. This policy shall be subjected to review at least once every two years. Any updates, reviews, or changes on any part or whole of this policy shall be approved by the board members prior to implementation. In such cases, all the people associated with WLiT, at that time, will be fully informed of the changes made.

## Objectives

- To understand and follow procedures to ensure the appropriate use of ICT at the organization, including maintaining secure storage of information
- To take responsibility to protect and maintain WLiT's data security and privacy

## WLiT's ICT Policy

We collect information from concerned individuals to provide service and communicate on community updates. WLiT always makes sure to protect individuals privacy and handle this responsibly.

In our continuous effort of handling the information we have, we have curated this ICT policy and tried to break down our information usage as much as we can. **This policy is also a written promise that WLiT do not share information with third parties in the information we have of our fellows, alumni and concerned individuals and we will never do that.**

This ICT Policy will be passed with our board members in a board meeting that is happening on 26 March 2022 (Saturday). If you have any questions regarding this policy then feel free to contact our policy leads, Sonika Baniya ([sonika@wlit.org](mailto:sonika@wlit.org)) and Nhasala Joshi ([nhasala.joshi@wlit.org](mailto:nhasala.joshi@wlit.org))

Approved on: March 26th 2022  
Effective from: March 26th 2022

## **1. Data and its storage**

- Contact information of fellows, alumni, staff and board members will be stored in google paid plan or WLIT's internal database system.
- WLIT will only provide official email domain- wlit.org to its staff and board members as long as they are associated with the WLIT. WLIT will only disseminate official emails (email with wlit.org email domain) of staff and board members.

Dissemination rights of all personal information of fellows (and everyone working for the organization) by board members will be only given if the information is owned by WLIT. For example, if someone (in or outside of organization) wants to access data of the fellows, then data that is owned by WLIT (organization email, picture taken by organization) can only be taken into consideration. For all the personal data, consent should be taken first from the concerned individuals.

### **1.1 What data do we collect?**

#### **i) Fellows, programme participants, mentors**

For the individual to become a fellow, programme participants, or mentor, we must collect their personal information starting from the early phase of the application process. Throughout the engagement with WLIT, we will continue to track and monitor the progress through phone calls, surveys, email correspondence on the basis of this data we have. The information of the individual will include but not limited to academic achievements, employment status, graduation achievements and personal as well as professional goals.

#### **li. Donors & Partners**

Donors and partners are the individuals or organizations who support WLIT's vision and mission. The support can be financial or collaborative work or resource providing. All the information related to donors and partners will strictly be for the purpose of showcasing the support and letting the community know about the support. The information mostly will be contact informations, digital logo, financial information (bank information if WLIT is receiving financial support). There will be provision for not disclosing the information of donors/partners as they wish.

### lii. Newsletter subscriptions, Event attendees

Those who subscribe to the general newsletter through our website or event sign up sheets and/or follow us on social media channels are agreeing to share with us general contact information (i.e. email addresses) and there will always be an option for unsubscription of the newsletter. As an appreciation of following our activities, we ensure to send content in limited amounts and frequencies to respect your digital space. This also applies to unsuccessful applicants to both our programme or organization, and includes any information collected throughout the application and selection process.

### lv. General member intake, staffs, volunteers

In the annual general meeting, WLIT intakes general members who later on can be part of the board. In this process, we intake information of national identity (citizenship card) for annual reporting. Additionally, we take information (citizenship number, pan number, emergency contacts, general identity information, bank information) from staff for the bookkeeping and financial reimbursement of their contribution to the organization.

## 1.2 How data is used?

The information from individual help us in the following ways:

- For reporting and analysis purposes along with monitoring and evaluation.
- To find the most relevant and appropriate leadership opportunities and determine one's eligibility for such opportunities.
- In house programs like mentor mentee match pair, community engagement and interaction program.
- Monitoring and evaluation of fellows, alumni in terms of leadership development experience.
- Official documents like citizenship, license, national identity, pan number will be strictly only used for government purposes and will never be disclosed with anyone else even with inhouse unconcerned individuals in the organization.
- The inhouse email addresses, social media handles will be used to flow different opportunities and information flow.

*Note: The data here doesn't necessarily mean fellowship data but can also mean data of participants of other events like workshops, safer i events, research activities*

WLIT never had, does not, and never will share or sell information to third parties for the purpose of financial benefits. In every case, data will be lawful for business use and protect individual's integrity and freedom.

## 1.3 How to view and access data?

Currently, all the data is being stored in google cloud services. Only the administrator will be allowed to view and access all data strictly following all above clauses. For everyone else, they have to ask the administrator and access will only be provided on need to know basis. To view one's personal information, if the administrator is skeptical about the means of request, purpose or anything then the administrator can ask for personal identity verification. In case of viewing third person information, requesting an individual must bring written consent from the third person.

In future if WLIT incorporates web portals to access the information, data apart from generic ones will only be accessible to personal individuals.

#### **1.4 How to remove the data?**

By simply asking. One will always have full authority over their data and information that is held by the organization. The organization will retain their information as long as they want to. They will have full right to unsubscribe all the communications and mails from the organization to exercise "Right to be forgotten".

Once you ask the organization for the removal of your information, the administrator will be fully in charge of the removal process. But please bear this in mind that by asking so, you will not get any kind of opportunity notifications and involvement in any future programs and events.

#### **1.5 Data Breach response**

As soon as theft or data breach action in WLIT is identified, the first step will be the process of distinguishing generic breached data and sensitive breached data. The removal of all access to the sensitive data will be applied.

The immediate breach response committee will be formed of minimum five people that will include members from:

- Board
- Tech team
- Finance and legal team
- Communications
- Human resources
- And other immediate active members according to the current working environment

In case of the absence of the mentioned personnel, someone from the relating team will take role in the response committee

The team will be led by the Executive Director of the organization. The response will be taken as follows:

- Cyber investigation will be started in leadership of tech team
- Develop a communication plan
- Legal team (in absence of a legal team, board to take this role) will look into violation of any individual's right and ways to compensate them.

If any inhouse person from WLIT is found in violation of this policy, they may be subjected to disciplinary actions and also termination of employment/ engagement from the organization.

## **1.6 Data Security**

### **i) Password policy:**

All the individual passwords/ organizational passwords will be shared personally. Users will be encouraged to change their personal passwords upon first login. The social media passwords will be shared with the communications team, social media team and admin only. The gmail and drive access will be given to administrator, Safer I leads and communication team only. Everytime administrator or any communications team or social media team changes, all the shared passwords must be changed. This is also applicable if any employee is no longer working for the organization. All the passwords created in a digital platform must be strong and no same password strictly in all digital platforms.

Everytime new employee joins the organization's communications team, Safer I leads and WLIT administrator can share the organizational email passwords and social media passwords if their job description needs access to the organization account.

### **ii) Digital Signature:**

The concerned authority from WLIT for most official document signatures will be Executive Director and President of the Board. All the concerned authority including Executive Director and President of board must use disclaimer in email footers that signatures can not be forged.

### **iii) Email Security:**

All the full time staffs, board members, leads of Safer I and necessary core team members (for example: communications team, social media team) will be given organizational email. Emails cannot be forwarded to any unconcerned authority. Also, only personal organization email can be integrated with personal emails (for example: [sonika@wliit.org](mailto:sonika@wliit.org) can be integrated with



[sonika@gmail.com](mailto:sonika@gmail.com) but [info@wlit.org](mailto:info@wlit.org) cannot be integrated with [sonika@gmail.com](mailto:sonika@gmail.com) ). Important donor emails must be kept in pdf format in our cloud.

*Note: For the server space, email attachment size can't be more than 500 MB, this can be changed in future but at the time of writing this policy, our server space can't take more than 500 MB.*

## **1.7 Data Storage**

WLIT is currently storing all the data in OneDrive, a microsoft service, and the files will be stored under yearly folders. The files stored are pictures, videos, documents of the program and proposals the organization is currently working on. The organization will take consent from participants, fellows, alumni, staff and every concerned authority at the time of taking pictures and videos. A verbal group consent will be taken and everyone will have the right for objection.

## **2. Purchase and use of office resource policy**

### **2.1 Software and Hardware purchase**

All software and hardware purchases must be consulted with the administrator first. Also, free trial purchase of software where the organizational name is mentioned must be consulted with the administrator first.

All the necessary full time employees will be provided with a computer, repair allowance per month and use of hard drive if necessary. The devices to be used as advised by the executive team and board.

### **2.2 Internet reimbursement**

All working employees, volunteers, board members, fellows, alumni, Safer I leads, core team members and everyone involved while working for the organization will be reimbursed for the work-related internet usage in case of attending online meetings, attending online sessions, developing fellowship project, and project discussion.

### **2.3 Physical device procured under WLIT**

All physical devices procured under organization should be billed under the organization with the permission of administrator. The employees, alumni and board are allowed to use physical devices of the organization with proper information to the administrator in need basis.

### **3. Accessibility and Inclusivity**

WLIT has always been a big advocate of accessibility and inclusivity. To shed light on this advocacy, a campaign named Safer-I Nepal was started with five enthusiastic fellows of 2018 WLIT batch. All the digital content of WLIT will be accessible in terms of language, color used, contrast and captionated video contents. Website of WLIT will follow WCAG 2.1 standards and the same goes for the website of Safer-I.

WLIT in every case (be it data collection via form, in terms of salutation in communications, graphical content and many more) will be inclusive of all concerned people. This includes all gender, sexual orientation, ethnicity and geographical diversity.

### **4. Ownership**

WLIT shall retain overall responsibility and ownership for all Institution's information assets. But in the case of a product built by fellows in their respective fellowship, WLIT and the team of fellows will have 51:49 ownership in the product. WLIT will provide all the resources required for fellows to build the test prototype of the product. Please bear in mind that the test prototype will not include premium services of the software.

### **Exceptions to this policy**

In case of any exceptions to this policy, it shall be thoroughly documented and followed through a proper channel of authorization using the same board which approved this document.