EMIT LINC Popi Act

Terminology

LINC-ED CONTACT

1. A person whom I have invited to appear in my personal list of contacts and who has accepted the invitation.
2. A person who has invited me to appear in their personal list of contacts and once I have accepted the invitation.

EMIT ADMINISTRATOR

Any EMIT staff or personnel who have been given an administrative role on the LINC portal or appointed to manage EMIT activities and initiatives.

PRIVATE CONTACTS LIST

An “address-book” of contacts that are non-LINC-users

Information Management

1. All the user’s personal information is required to be visible to EMIT appointed administrators.
2. No information will be made public (displayed or shared to non-LINC-users)
3. A user may completely delete their account and all their information (Except in the case of a user who has been registered for any course - archival study records and learner information will be kept but will only be visible to EMIT administrators)

Location Residential Address (as per profile)

WHY DO WE WANT THIS INFORMATION?

- So that EMIT appointed administrators can better manage group memberships and physical events
- For displaying training groups, projects and teams near you
- For displaying physical events near you
- For displaying in your profile

- For displaying map pins to other members of the same group, project or team
- For displaying map pins to EMIT administrators
- For displaying map pins to prospective donors

DEFAULT SETTING FOR ALL USERS

- By default the user's residential location will be displayed and shared to other users as a pin on a map with a random inaccuracy of at least 1km and up to 2km.
- By default the user's residential city/town/suburb will be displayed in their profile. The actual street address will not be displayed (Except to EMIT administrators).

PERMISSION PREFERENCES

- Users may adjust their shared pin coordinates manually within a 5km range of the address supplied in their profile
- Users may redact their actual physical address in their profile with a custom setting for LINC-ed contacts.
- Users may NOT select to hide their accurate residential location or pin from EMIT administrators

---

Location Current (HTML Geolocation API)

WHY DO WE WANT THIS INFORMATION?

- For automatic attendance reports of training events for which the user is registered

DEFAULT SETTING FOR ALL USERS

- We will ask for permission to access current location when a user first signs-up on the portal (as per the HTML Geolocation API)
- We will ask for permission to access current location at the start time of a physical event for which the user has been registered (as per the HTML Geolocation API)
- Current location will not be shared with any other users except for EMIT appointed administrators (Except in the case of a physical event - below)
- Current location will be shared with other people attending the same physical event

PERMISSION PREFERENCES

- Users may select to turn off current location sharing at any time

---

Profile Information (Name, Gender, Contact Details etc.)

WHY DO WE WANT THIS INFORMATION?

- For displaying your profile page to other users and admins
- For enabling other users to contact you
- For effective training and support to achieve the EMIT program goals

DEFAULT SETTING FOR ALL USERS

- Contact details (email and phone) will by default be hidden from other users except EMIT administrators.
- Non-sensitive personal Profile information will be visible on your profile page (e.g., marital-status, gender, language, etc.)

PERMISSION PREFERENCES

- A user may select to show their contact details to other users (with custom settings for LINC-ed contacts)
- A user may redact their profile page to hide any information from other users (with a custom setting for LINC-ed contacts)
- A user may NOT select to hide any profile information from EMIT administrators

---

Resume

WHY DO WE WANT THIS INFORMATION?

- For displaying your resume to other users and admins
- For consideration in the course application approval process
- For supporting networking and collaboration initiatives between LINC users

DEFAULT SETTING FOR ALL USERS

- A user may select to publish their resume
- A resume, once published, will by default be public to all other LINC users
- A user will be required to create a resume on application for entrance to a course

PERMISSION PREFERENCES

- A user may select to un-publish their resume (it will be hidden from all other users except administrators)
- A user may select to delete their resume except if they are registered to study for any course
- A user may NOT hide their resume from EMIT administrators and it will remain visible to administrators even once un-published

---

Study Records, History and Reports

WHY DO WE WANT THIS INFORMATION?

- For learning management and reporting
- For displaying to potential donors and sponsors
- For displaying non-sensitive completion reports in your public profile

DEFAULT SETTING FOR ALL USERS

- By default, a user's non-sensitive course completion reports and site-generated certificates will be visible to other users. No specific grades or attendance records will visible to other non-administrative users
- By default detailed course reports and learning activities will not be visible to other users except EMIT administrators.

PERMISSION PREFERENCES

- A user may agree to share their complete confidential learning records and reports with another user after receiving a request to view such information. (use-case: a prospective sponsor)
- A user may select to hide their non-sensitive completion reports and site-generated certificates from other users (with custom settings for LINC-ed contacts)
- A user who is registered for any course may NOT hide their learning records and reports from EMIT administrators

---

Private Contacts List

WHY DO WE WANT THIS INFORMATION?

- To display on a user's personal impact page
- As a requirement for the EMIT Mi-10 initiative - as evidence of learners registration agreement to share their learning experience and material with at least another ten non-LINC users
- As a requirement for users to list their team members when creating a community impact project
- To display on a community project page
- To display on a Mi-Ten page
- As a requirement for registered student to list their emergency contacts
- To facilitate the emailing of sign-up invitations to colleagues and team-members

DEFAULT SETTING FOR ALL USERS

- Private contacts (non LINC-users) will only be represented by their first names and their relationship to the user. No contact details, addresses or locations will be displayed
- EMIT will not directly contact any person in the user's private contacts list.

PERMISSION PREFERENCES

- A user may choose to invite any private contact to become a LINC user, in which case a sign-up email will be sent to their given email address

Activity Logs

WHY DO WE WANT THIS INFORMATION?

- To assist with improvements and bug-fixing for the LINC portal
- To better manage EMIT initiatives and activities for learners, donors and administrators
- To display on the ‘My Journal’ page
- As a record of learner course involvement and progress
- As a record of donor involvement

DEFAULT SETTING FOR ALL USERS

- By default, non-sensitive activity information will be displayed on the user’s public journal
- By default, EMIT administrators will be able to view all activity logs for a user

PERMISSION PREFERENCES

- Users can select to hide any specific activity from their journal with custom settings for LINC-ed contacts

Guidelines for POPI

Purpose of processing: must state the purpose for which we are collecting personal information from users. This could include providing access to the platform, providing customer support, or marketing products or services.
Type of personal information collected: must state the type of personal information we are collecting from users. This could include name, email address, contact information, and payment information.
How personal information is collected: must state how we are collecting personal information from users. This could include through registration forms, surveys, or cookies.
How personal information is used: must state we they are using personal information. This could include to provide access to the platform, provide customer support, or market products or services.
How long personal information is kept: must state how long we will keep personal information. This could be until the user deletes their account, or for a longer period of time if required by law.
Who has access to personal information: must state who has access to personal information. This could include employees, contractors, or third-party service providers.
How users can access and correct their personal information: must state how users can access and correct their personal information. This could be done through the platform's settings page, or by contacting us directly.
How users can withdraw their consent: must state how users can withdraw their consent for the processing of their personal information. This could be done by contacting us directly, or by unsubscribing from marketing emails.
How users can complain about a breach of privacy: must state how users can complain about a breach of privacy. Could be done by contacting us directly, or by filing a complaint with the Information Regulator.
Opt-In
By clicking on the "I agree" button below, you are giving your consent to [name of platform or website] to collect, use, and share your personal information for the following purposes:

- To provide you with access to the platform or website
- To provide you with customer support
- To market products or services to you

You understand that you have the right to access, correct, and delete your personal information at any time. You also understand that you can withdraw your consent for the processing of your personal information at any time by contacting [name of platform or website].
I agree to the above.

4. POPI exists to protect and enforce the right to privacy. Data subjects(natural and juristic persons) can contact the Information Regulator if this is violated
5. To comply with the POPI Act, the following must be implemented:
    - POPI Code of conduct

- Responsible party(RP) and Third Party(TP)provider contracts - privacy policy clauses.
- Staff training and awareness - compulsory - require a register.
- Consent - expressive and voluntary

6. If a data subject is not identifiable - POPI does not apply. A name or a photo is not enough to identify a Data subject. To use special information of a Data subject(photo's included), the Responsible party will need permission unless the Data subject has deliberately made this public.
7. You may not hold onto Personal Information(PI) that has no purpose. It must be 'legitimate purpose', then 7 years - otherwise destroy all old PI that you do not need - CD backups.
8. PI processing refers to the life cycle - distinguish between destroyed(irretrievable), deleted(can be retrieved) as well as automated(computer) versus non-automated(paper and file)
9. Define: Responsible party(RP) - data controller. Operator(O) - employed by a Responsible party - almost no responsibility - includes 3rd party Operators- HR Companies or cloud providers. There needs to be contractual clauses between (RP) and (O) to safeguard PI and RP. "I am aware of my responsibility as per the Act. I undertake to ……"
10. Action causes harm - DS must prove No intent or negligence and provide only the information involved to the Information Regulator.
11. Statistical information - defined as 'de-identified' PI, and can never be identified information again.
12. Must appoint information officer, "CEO" (default information officer) of a Responsible Party can appoint an information officer by way of a data protection appointment letter. Must keep a POPI compliance register.
13. Where PI is entered into a system where it can be recovered again, it must be justified and there must be a signed consent form by the DS.
14. Notice requirements define the purpose and comparable purposes for which PI can be used
15. PI must always be accurate and up to date. So in the consent form, the DS warrants to inform the RP should any changes to PI occur, and indemnifies the RP from any claims for failing to do so.
16. The DS may, through use of required access policy and form ask the Responsible Party to reveal what information they hold – this must be provided free of charge by the information officer.
17. A DS may request that their information be corrected or deleted – by providing reasons in a form or written consent to this effect. this can be addressed in the data access policy.
18. The POPI Act requires IT and automated system security is of utmost importance, a "reasonable" test in this regard which implies that data/laptops must be (triple) encrypted with the required password protection.
19. Direct Marketing, section 69, could be one of the most contentious areas. While the definition of telemarketing excludes marketing by electronic means, it includes marketing by any other means. It also includes selling of products, services, asking for donations, and electronic newsletters. With regards to telemarketing, the Act stipulates that there must always be an

"opt out" and that how and where the PI was obtained must be disclosed. The current position is that clients may be contacted until they say no – "opt out".

DM by electronic mail is prohibited unless:

- The Data Subject consents by way of "opt in" in the prescribed manner and in terms of Form 4 of the POPI Act. This authorised signature/consent requires an "advanced signature". Furthermore, Data Subjects may only be asked once. Non-compliance can result in a server/domain being blacklisted, resulting in all mail being spammed.
- The DM goes to an existing client/customer. A client/customer is, amongst others, someone who pays.

20. Section 69 prohibits cross-selling in a group of companies. Each entity in the group becomes a separate Responsible Party, making it important to ring-fence a clean database. The Information Regulator has declared that a contravention will only be penalised if the contravening party in question receives a warning letter and fails to stop their activity. If the letter is complied with, no action will be taken. If an enforcement notice is received, the party may appeal or comply.
21. The Act demands that there is a contract between the Data Subject and Responsible Party wherein they agree to comply with legislation that governs PI in a foreign country. If the foreign country does not have PI protection legislation, there must be a contract to the effect that the Data Subject and Responsible Party agree to be bound by the principles of PI protection. In such instances, the GDPR of the EU will be the benchmark. Clouds are typically hosted in countries with adequate data protection laws. The issue that must be clarified by Responsible Parties.

22. There must be a POPI section in the organisations PAIA (Promotion of Access to Information Act) manual.

Guidelines for Terms and conditions

1. Introduction: This section provides an overview of the agreement and may include information about the parties involved, the purpose of the agreement, and any additional legal disclaimers.
2. Acceptance of Terms: This section outlines the user's acceptance of the terms and conditions, often by clicking a checkbox or button during the signup or registration process.
3. Definitions: Here, key terms used throughout the agreement are defined to ensure clarity and understanding.
4. User Obligations: This section outlines the responsibilities and obligations of the user when using the web app. It may cover topics such as account creation, usage restrictions, and compliance with applicable laws.
5. Intellectual Property: This section addresses the ownership and protection of intellectual property rights, including copyrights, trademarks, and patents related to the web app.
6. User Content: This section explains the rights and restrictions associated with user-generated content, such as text, images, or videos uploaded to the web app.
7. Privacy and Data Protection: This section covers how user data is collected, stored, and processed by the web app, as well as any applicable privacy policies or procedures.
8. Payment Terms: If the web app offers paid services or products, this section details the payment terms, including pricing, billing, refunds, and cancellation policies.
9. Dispute Resolution: This section outlines the procedures for resolving any disputes or conflicts that may arise between the user and the web app, such as arbitration or mediation.
10. Limitation of Liability: Here, the web app owner limits their liability for any damages or losses incurred by the user while using the app.
11. Indemnification: This section explains that the user agrees to indemnify and hold harmless the web app owner from any claims or damages arising from the user's actions or misuse of the app.
12. Termination: This section details the circumstances under which the web app owner or the user can terminate the agreement and the consequences of termination.
13. Modifications: It clarifies that the web app owner reserves the right to modify or update the terms and conditions and how any changes will be communicated to the user.
14. Governing Law: This section specifies the jurisdiction or laws that govern the agreement and any disputes that may arise from it.
15. Miscellaneous: This section includes any additional provisions that are relevant but may not fit into the above categories, such as the entire agreement clause, severability, or waivers.