



Acceptable Use and Data Submission Policy

Incorporated into the Master Services Agreement

Effective July 31, 2026

This Acceptable Use and Data Submission Policy ("AUP") is part of the Master Services Agreement between Legacy X LLC, a Pennsylvania limited liability company, d/b/a Luminary Impact ("Provider") and Client. It exists to keep one promise structurally true: Provider never holds Client's participants' identifying information outside the vault only Client can read.

1. The Core Rule: Coded Data Only

Client agrees to submit participant information only in de identified, coded form. Participant identities, meaning names, contact information, and other direct identifiers, may enter the platform only through the platform's designated coded forms, which route identity to the participant vault, readable only by Client, and assign codes for all working data.

Client will not submit, into any request brief, uploaded file, note, or self serve AI feature:

- Participant names, addresses, phone numbers, or email addresses, individually or in lists or spreadsheets
- Social Security numbers or other government identifiers
- Dates of birth tied to individuals
- Protected health information, absent an executed Business Associate Agreement
- Identifying information about victims of domestic violence, dating violence, sexual assault, or stalking
- Records subject to 42 C.F.R. Part 2, governing substance use treatment, in identifiable form
- Any personal information Client lacks the legal right to share

2. What the Platform Does to Help

2.1 Intake screening. The platform screens submissions and uploads server side for identifier patterns, for example Social Security numbers, date of birth columns, and lists of names or contact details, and rejects flagged items before anything is stored. Nothing flagged is retained, even briefly. The rejection message explains the category detected and the two correct paths: collect through coded forms, or re upload a de identified version.

2.2 Files that cannot be screened. PDF and image files cannot be content screened. The platform requires Client's explicit confirmation, at upload, that such files contain no participant identifying information. That confirmation is a representation under this AUP.

2.3 Honest limits. Screening is pattern based and cannot catch everything. It is a safeguard, not a substitute for Client's obligation under Section 1.

3. General Acceptable Use

Client will not use the platform to violate law or third party rights; attempt to access another organization's data or circumvent access controls or screening; probe, scan, or disrupt the

service; resell access; or submit malicious code. Provider may suspend access immediately to address a security risk, with notice as soon as practicable.

4. Responsibility Allocation

4.1 If Client submits data in violation of Section 1, including by confirming a file as identity free when it was not, or by circumventing screening, Client is responsible for that submission and for claims arising from it, as set out in Section 10.2 of the Agreement, and Provider's handling of that data before discovery is not a breach by Provider.

4.2 On discovering a violating submission, Provider will delete the data from active systems promptly, notify Client of the deletion, and work with Client in good faith on any resulting obligations. Repeated or willful violations are a material breach of the Agreement.

5. Changes

Provider may update this AUP prospectively with thirty (30) days' notice. Changes that materially reduce Client's protections require Client's consent.