All Computers Are Brilliant, Inc.

User Data Disclosure Policy

Version 1.1

Revision History

Version	Date	Comments
1.1	6 June 2025	Revisions to Section 6 to clarify intentional harm and threats to safety
1.0	25 April 2025	Initial version approved by Board

Section 1. Purpose.

The purpose of this policy is to define the circumstances under which the company may disclose users' personal data.

Section 2. Definition of personal data.

For the purposes of this policy, personal data includes users' names, email addresses, physical addresses, telephone numbers, approximate or exact geographic locations, Internet Protocol addresses, client machine details (e.g. user-agent strings), or any similarly personally identifiable information the company may possess about a user.

Section 3. General prohibition of data disclosure.

The company will not disclose users' personal data in its possession, except as specifically provided in this policy.

Section 4. Disclosure as required by 18 USC §2258A, and related voluntary disclosure.

If the company finds that a user registered for its services has posted or uploaded actual Child Sexual Abuse Material, as defined in the Child Content Safety Policy, the company will disclose all personal data about that user in its possession to the National Center for Missing and Exploited Children's CyberTipline, or its successor. This may include voluntary disclosure of information beyond the requirements of 18 USC §2258A.

Section 5. Disclosure in response to legal process.

The company will disclose users' personal data if legally compelled to do so, e.g. by court order.

Section 6. Disclosure in response to evidence of intentional harm or imminent threat to safety.

If any Director of the company becomes aware that a user of the company's services has intentionally inflicted significant harm on another person, the Director will attempt to obtain the unanimous consent of the Board of Directors to make a report to law enforcement including disclosure of some or all of the user's personal data, in accordance with Article V, Section 14 of the bylaws. If the Director is unable to obtain a vote from one or more Board members within 24 hours, the Director may make the report at their discretion and without further authorization. They must then notify the Board of the action.

If any Director of the company has a good-faith belief that a user of the company's services poses an immediate threat to the safety of one or more persons, that Director will immediately report the threat to law enforcement and notify the Board after the fact. The Director making the law enforcement report may disclose the subject user's personal information as part of the report, at the Director's discretion.

Section 7. Transparency in disclosure.

Unless legally prohibited from doing so, the company will update its publicly-available User Information Disclosure Report with the dates, times and nature of personal data disclosed for any disclosures made in accordance with sections 4, 5 and 6.

Section 8. Warrant canary.

The company will maintain a warrant canary consisting of a PGP-signed text statement that the company has not been compelled to disclose user data apart from the incidents listed in the User Information Disclosure Report, that the company has not been the subject of warrants or searches it cannot disclose, and that the company’s servers and cryptographic keys are under its sole control.