Information Transparency

Updated September 17, 2026

This page presents the administrator-maintained data inventory below. Empty fields are left undisclosed rather than guessed.

Account Information

Information: Name, email address, password (hashed), profile photo, phone number if provided, language preference.

Purpose: Authenticate login, personalize the experience, enable communication features.

Source: Provided directly by the account holder at registration or in Account Settings.

Storage: This installation's own database.

Who can see it: Name and profile photo may be visible to other members within a shared School/PTO community context; email and phone are private by default.

Roles with access: The account holder; School/PTO administrators only where the account has an active relationship with their organization; Super Admins for support and moderation.

Public / private: Private, with limited visibility fields noted above.

Retention: Retained while the account is active; a member may request deletion.

Deletion: Deleting an account removes personal profile data; some records may be retained where required by law or a legitimate business need.

User controls: Edit profile, change password/email, enable two-factor authentication or passkeys, request data export or deletion from Account Privacy.

Legal context: Privacy Policy; Terms & Conditions.

Child / Student Records

Information: First and/or last name, grade, school affiliation, and optional teacher/roster relationship.

Purpose: Associate the parent's own activity (volunteer sign-ups, team rosters, membership registration, shop orders) with the correct child.

Source: Entered directly by the parent/guardian in their own account, or begun as a teacher-entered roster entry the parent must explicitly claim — never auto-linked by name match alone.

Storage: This installation's own database, within the parent's own account.

Who can see it: Visible only to the parent/guardian who owns the record, and to School/PTO administrators for the specific context it appears in (e.g. a class roster).

Roles with access: Parent/guardian; the specific School/PTO administrators managing that context; Super Admins for support.

Public / private: Private — no public student directory or public student-name display exists on this platform.

Retention: Retained while the parent's account and the child record remain active.

Deletion: Deleted immediately by the parent's own action; no separate approval process is required.

User controls: A parent may edit or delete their own child's record directly, at any time, from their own account.

Legal context: See the Children & Student Data Privacy page and, where one has been executed, the Student Data Privacy Agreement between SchoolCircle and that School/School Network.

School / PTO / School Network Organizational Data

Information: Organization name, address, logo, description, and staff/officer contact information the organization chooses to publish; verification documents submitted to claim a page.

Purpose: Power the organization's public page and directory listing, and confirm the person managing it has a legitimate relationship to that organization.

Source: Entered by an authorized organization representative during the claim/verification process or ongoing management.

Storage: This installation's own database and protected file storage.

Who can see it: Organization profile content is generally public by design, since it is a directory listing; verification documents are private and reviewed only by Super Admins.

Roles with access: The organization's authorized administrators; Super Admins for verification review.

Public / private: Mixed — profile content public, verification evidence private.

Retention: Public content persists while the organization page is active; verification files are deleted once review is complete.

Deletion: Verification files are removed after their one-time review; public profile content is removed if the organization page is deactivated.

User controls: The organization's authorized manager can edit its own public profile content at any time.

Legal context: School & School Network Terms; institutional agreements, where executed.

Forms, Volunteer Sign-Ups & Submissions

Information: Whatever fields a School/PTO's own custom form or volunteer opportunity asks for — which may include adult and parent-selected child information.

Purpose: Fulfill that specific form's stated purpose — for example volunteer scheduling, supply requests, or event RSVPs.

Source: Submitted directly by the member filling out the form.

Storage: This installation's own database.

Who can see it: Visible to the submitter and to the organization's authorized reviewers for that specific form.

Roles with access: The submitter; the organization's authorized form reviewers; Super Admins for support.

Public / private: Private.

Retention: Administrator-configurable per organization; see this installation's Admin Settings for its specific retention period.

Deletion: Deleted per the organization's configured retention setting, or sooner on request.

User controls: A member can review or, where the form allows it, withdraw their own submission.

Legal context: Privacy Policy. A form that embeds a third-party widget is additionally subject to that destination's own practices once loaded.

Messages & Notifications

Information: Direct and group message content, reactions, and notification preferences and delivery history.

Purpose: Enable member-to-member and organization-to-community communication.

Source: Generated when a member sends a message or interacts with the notification system.

Storage: This installation's own database; end-to-end encrypted message content is unreadable to the server itself.

Who can see it: Message content is visible only to conversation participants; this installation's server stores ciphertext for end-to-end encrypted conversations, not readable content.

Roles with access: Conversation participants only, for message content; Super Admins can see delivery metadata but not encrypted message content.

Public / private: Private.

Providers: OneSignal (optional push delivery only, never message content).

Retention: Retained while the conversation/account is active, subject to the member's own deletion actions.

Deletion: A member may delete their own conversations at any time.

User controls: Delete a conversation, manage notification preferences, and optionally set up encrypted per-device key backup protected by a PIN the server never sees.

Legal context: Privacy Policy; Cookie Policy for push-notification consent.

Payments & Transactions

Information: Transaction amount, date, payment method type (never full card numbers), billing name/email, and the associated order, membership, donation, or ticket record.

Purpose: Process payment, provide receipts, and support refunds and accounting.

Source: Generated when a member completes a paid transaction through Stripe or PayPal.

Storage: Full payment card details are handled directly by Stripe/PayPal and are never stored on this installation's own servers; only transaction metadata needed for its own records is stored here.

Who can see it: The payer; the organization that received the payment, for its own transactions only; Super Admins for support.

Roles with access: The payer; the receiving organization, for its own transactions; Super Admins for support.

Public / private: Private.

Providers: Stripe, PayPal.

Retention: Retained as required for accounting, tax, and dispute-resolution purposes.

Deletion: Financial records are retained per applicable accounting/tax requirements rather than deleted on request.

User controls: Review a member's own transaction history from their account.

Legal context: Terms & Conditions; Third-Party Service Providers registry.

Security & Audit Records

Information: Login timestamps, approximate device/location signals, admin and moderator action logs, session/CSRF tokens, and the IP address at the time of a security-relevant action.

Purpose: Detect and investigate unauthorized access, support account recovery and abuse investigation, and provide the audit trail behind administrative actions.

Source: Generated automatically by the platform's own authentication and administrative systems.

Storage: This installation's own database.

Who can see it: Not visible to other members; Super Admins review audit logs relevant to their responsibilities; a member can review their own recent login history.

Roles with access: Super Admins for audit review; the account holder, for their own login history.

Public / private: Private.

Retention: Retained per this installation's configured security/audit retention settings.

Deletion: Purged per this installation's configured retention window.

User controls: Review recent login history and manage trusted devices from Account Security.

Legal context: Privacy Policy; Security & Trust page.

First-Party Analytics

Information: Approximate page views, a random rotating visitor identifier never linked to a name or account, device class, and a normalized referrer source category — never full URLs, query strings, or fingerprinting.

Purpose: Understand approximate traffic and engagement to improve the platform, and provide Insights dashboards to organization administrators for their own pages.

Source: Generated automatically as visitors use the site.

Storage: This installation's own database only.

Who can see it: Aggregated statistics are visible to relevant organization administrators for their own pages; the raw visitor identifier is never exposed in any dashboard.

Roles with access: Super Admins; the relevant organization administrators, for aggregated statistics about their own pages only.

Public / private: Private, with aggregated views available to relevant organization administrators.

Providers: None — no third-party analytics service is used.

Retention: Raw events are pruned per this installation's configured retention window; the visitor-identifier cookie itself expires after 180 days.

Deletion: Purged automatically per this installation's configured retention window.

User controls: Decline the 'Analytics' cookie category at any time from Cookie Preferences — the identifier is then never stored.

Legal context: Cookie Policy.

Cookies & Client-Side Storage

Information: Session/CSRF tokens (strictly necessary), the optional analytics visitor identifier, PWA install-prompt state and accessibility preferences stored in the browser's local storage, and the cookie-consent choice itself.

Purpose: Necessary cookies keep the site functional and secure; optional categories are described in, and controlled from, the Cookie Policy.

Source: Set by this platform as the visitor uses it, per the categories described in the Cookie Policy.

Storage: The visitor's own browser.

Who can see it: Private to the visitor's own device.

Roles with access: The visitor only.

Public / private: Private to the visitor's own device.

Retention: Per-cookie expiration is documented in the Cookie Policy; a consent choice itself persists 365 days.

Deletion: Cleared by the visitor at any time through their own browser settings or the Manage Cookie Settings control.

User controls: Manage Cookie Settings, available from the footer of every page.

Legal context: Cookie Policy.

Uploaded Media

Information: Photos, logos, documents, and other files a member or organization uploads — for example a profile photo, organization logo, event photo, verification document, or a signature image used for an institutional agreement.

Purpose: Display the content the uploader chose to publish, or support a specific workflow — for example a signature image embedded only into that organization's own signed PDF, never a public URL.

Source: Uploaded directly by the member or organization.

Storage: This installation's own protected file storage; sensitive subdirectories deny all direct web access.

Who can see it: Varies by upload type: some are public by design (a published event photo), others are strictly protected (a signature image, a verification document).

Roles with access: Varies by upload type — see Visibility.

Public / private: Mixed, by upload type.

Retention: Retained while the associated content or record remains active.

Deletion: Removed when the uploader deletes the associated content, or automatically where a workflow defines a one-time use.

User controls: Replace or remove uploaded content the member directly controls.

Legal context: Privacy Policy.

Authoritative HTML source: https://schoolcircle.net/legal/information-transparency
Downloaded November 15, 2026