

Fundraising University Privacy Policy

KFRM LLC d/b/a Fundraising University

Effective date: August 4, 2026

Last updated: August 4, 2026

Contents

1. Introduction and scope
2. How our platform works
3. Information we collect
4. How we use your information
5. FERPA compliance
6. COPPA compliance statement
7. Student data privacy and state law compliance
8. For donors: how your information is used
9. Data retention and deletion
10. Third-party service providers and data sharing
11. Cookies and tracking technologies
12. Security of information
13. Your rights
14. Breach response plan
15. Contact information

Section 1: Introduction and Scope

1.1 KFRM LLC d/b/a Fundraising University ("Company," "Fundraising University," "FRU," "we," "us," or "our") is committed to safeguarding the privacy of all individuals who interact with our platform and services. This Privacy Policy describes how we collect, use, disclose, retain, and protect personal information.

1.2 This Privacy Policy applies to all users of the Fundraising University platform, including:

- Students participating in fundraising campaigns
- Coaches and school staff who oversee student fundraising
- Donors who receive fundraising messages and make contributions

- Franchise owners and sales representatives who operate within the Fundraising University system
- Visitors to the Fundraising University website (fundraisingu.net)

1.3 This Privacy Policy covers the following Fundraising University systems and surfaces:

- The Student Fundraising Portal (student-facing web application)
- The donor-facing fundraising pages and checkout experience
- The coach dashboard
- The franchise management ERP system (internal use)
- The Fundraising University public website

1.4 Terms of Service. Use of the Fundraising University platform is subject to our Terms of Service, which are incorporated into and made part of this Privacy Policy by reference. By using the platform, you agree to be bound by our Terms of Service.

1.5 We may modify this Privacy Policy from time to time to reflect changes in our practices or applicable law. We will notify you of material changes by posting the updated policy on our website and updating the "Last updated" date above. We encourage you to review this Privacy Policy periodically.

1.6 By accessing or using the Fundraising University platform, you acknowledge that you have read, understand, and agree to be bound by this Privacy Policy and our Terms of Service. If you do not agree, do not access or use the platform.

Section 2: How Our Platform Works

This section explains, in plain language, how the Fundraising University platform operates and how data flows through the system. Understanding this context is essential to understanding the privacy practices described in subsequent sections.

2.1 The fundraising process

Fundraising University provides a web-based platform that enables high school students to conduct fundraising campaigns for their school programs (athletics, music, band, and other activities). The typical process works as follows:

1. A school partners with a Fundraising University franchise owner to set up a fundraising campaign.
2. Students receive login credentials to the Student Fundraising Portal.
3. Each student enters up to 30 donor contacts (friends and family members the student personally knows).
4. For each contact, the student clicks a button that opens the student's own native SMS (text messaging) application with a pre-composed fundraising message.
5. The student sends the message from their own phone, using their own phone number and their own cellular carrier.
6. Donors who wish to contribute can make a donation or purchase products through the platform.

7. Students and coaches track fundraising progress through the platform.

2.2 Text messaging architecture

Fundraising University does not send text messages. This is a critical distinction for understanding our platform and its compliance posture.

When a student uses our platform to reach out to potential donors:

- The platform composes a personalized message and opens the student's native SMS application (for example, iMessage or Android Messages) with the message pre-populated.
- The student reviews the message and sends it from their own phone, using their own phone number.
- The message is transmitted through the student's own cellular carrier, not through Fundraising University's systems.
- Donors receive the message from the student's personal phone number — a number that approximately 95% of donors already have saved in their contacts, because donors are friends and family of the student.
- There are no corporate shortcodes, no mass marketing systems, and no automated follow-up messages sent without direct student action.
- Donors can reply directly to the student or opt out by replying STOP to the student's personal number.

The complete technical and legal analysis is published in our [TCPA Compliance Statement](#).

2.3 Who sees what

- **Students** see their own donor contacts, their own fundraising progress, and their own messages.
- **Coaches** see aggregate team and individual student fundraising progress and can identify students who may need additional support. Coaches can view student contact lists through the coach dashboard.
- **Donors** see the student's fundraising page when they choose to donate or purchase products.
- **Franchise owners** see territory-level and school-level performance data through the franchise management ERP system.

2.4 Data lifecycle overview

Personal data collected through the platform follows this general lifecycle:

1. **Collection:** Data is collected when students set up their accounts, enter donor contacts, and when donors make contributions.
2. **Active use:** Data is available and actively used during the fundraising campaign.
3. **Retention:** Data is retained after the campaign concludes. See [Section 9](#) for specific retention periods.
4. **Deletion:** Data is deleted upon request or in accordance with the retention schedule described in [Section 9](#).

Section 3: Information We Collect

3.1 Student information

When students use the Student Fundraising Portal, we collect the following information:

- Phone number (used for login and device identification)
- First name and last name
- Opt-in preference for fundraising reminders
- Coach group assignment
- Engagement metrics (share clicks, page visits)

We do **not** collect email addresses from students through the Student Fundraising Portal. We do **not** collect grade level, date of birth, Social Security numbers, photographs, or biometric data from students.

A student's school association is determined through the fundraiser the student is linked to, not through a field the student provides directly.

3.2 Donor contact information entered by students

Students enter information about their personal contacts (friends and family) to facilitate fundraising outreach. For each contact, the following information is stored:

- Contact name
- Phone number
- Relationship designation (for example, "uncle" or "family friend")
- Message text fields (initial share message, follow-up message, second follow-up message)

This information is entered by the student, not by the donor. It is used to facilitate the student's fundraising outreach as described in [Section 2](#).

3.3 Donor information collected at checkout

When a donor chooses to make a donation or purchase products, the following information is collected during the checkout process:

- First name and last name
- Phone number
- Email address
- Shipping address (street address, city, state, ZIP code)
- Payment token (a tokenized reference to the donor's payment method, generated by our payment processor — not the full card number, CVV, or expiration date)
- Geographic coordinates (latitude and longitude, derived from address)

Important: Fundraising University does not collect, store, or have access to full credit card numbers, CVV codes, or card expiration dates. When a donor enters payment information during checkout, the card details are sent directly from the donor's browser to our payment processor (Priority) for tokenization. Only the resulting payment token is stored by Fundraising University. See [Section 10.1](#) for more detail.

3.4 Coach and school staff information

Coaches and school staff who use the platform are represented as users within the Fundraising University CRM system. Information collected includes:

- First name and last name
- Email address
- Phone number(s)
- Title or role designation

Coach groups (used for organizing students into teams) store only a group name and fundraising goal — no personal contact information.

3.5 Franchise owner and sales representative information

Franchise owners and sales representatives use the Fundraising University ERP system. As business operators, the following information is collected and stored:

- Contact information (name, email, phone numbers, office phone, mobile phone)
- Billing information (billing address, card brand and last four digits, billing plan)
- Integration credentials (QuickBooks tokens, Google OAuth tokens, Stripe identifiers) for business operations
- Territory and legal entity association
- Profile photo URL

3.6 Automatically collected information

We automatically collect certain technical information when you use our platform:

- **On the public-facing fundraising pages and checkout:** We use Google Analytics 4 to collect usage data including IP address, browser type, device information, referral source, page views, and session data. Google Analytics uses first-party measurement cookies.
- **On the Student Fundraising Portal:** We do NOT use Google Analytics or any third-party analytics tracking. The Student Portal uses only technical CDN requests (for loading interface assets such as icons and fonts) and stores authentication tokens in the browser's local storage.
- **On the franchise management ERP (internal):** The ERP uses cookie-based authentication and Google OAuth for login. No Google Analytics is present in the shared layout. Some pages load embedded analytics dashboards for internal business intelligence.

Section 4: How We Use Your Information

4.1 Platform operation and service delivery. We use personal information to operate the Fundraising University platform, authenticate users, display fundraising progress, and enable the core fundraising workflow described in [Section 2](#).

4.2 Processing donations and purchases. We use donor information to process donations and product purchases, issue receipts, fulfill orders, and handle refunds or disputes. Payment processing is handled by our payment processor, Priority (see [Section 10.1](#)).

4.3 Facilitating student fundraising campaigns. We use student and donor contact information to enable students to conduct their fundraising outreach, track progress toward goals, and organize students into teams.

4.4 Enabling coach oversight. We use student fundraising data to enable coaches to monitor individual and team progress, identify students who may need additional support, and manage the overall campaign.

4.5 Analytics and platform improvement. We use automatically collected information (as described in [Section 3.6](#)) to analyze platform usage, identify technical issues, and improve our services. Google Analytics 4 is used on the public-facing fundraising pages and checkout only — not on the Student Portal.

4.6 Communications. For students who opt in to fundraising reminders, we may send SMS reminders through our communications infrastructure (see [Section 10.2](#)). We may also send transactional communications related to donations, orders, or account activity.

4.7 Legal compliance and security. We may use personal information as necessary to comply with applicable laws, respond to legal process, enforce our Terms of Service, protect against fraud, and ensure the security of our platform.

4.8 What we do NOT use your information for.

- We do NOT display targeted advertisements to students.
- We do NOT sell personal information to third parties.
- We do NOT use student data to create behavioral profiles for commercial purposes.
- We do NOT use donor contact information for Fundraising University marketing purposes.
- We do NOT share student data with third parties for marketing or advertising.

Section 5: FERPA Compliance

Family Educational Rights and Privacy Act

5.1 FRU's role under FERPA. When Fundraising University provides services to schools and school districts, we function as a "school official" with a "legitimate educational interest" in student information, as those terms are used under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g. We access and use student information solely to provide our fundraising services to the school.

5.2 School as data owner. The school or school district that partners with Fundraising University maintains ownership of all student data. Fundraising University acts solely as a service provider. We do not claim ownership of student educational records and do not use student data for any purpose other than providing the fundraising service to the school.

5.3 Purpose limitation. Student data collected through our platform is used solely for:

- Facilitating the student's fundraising campaign
- Enabling coach oversight and support of student fundraising efforts
- Providing platform functionality, technical support, and security
- Complying with applicable law

5.4 Parent and eligible student rights under FERPA. Parents and guardians of students (and eligible students who are 18 years of age or older) have the following rights with respect to student education records:

- The right to inspect and review student education records maintained by the school
- The right to request correction of records believed to be inaccurate or misleading
- The right to provide written consent before the school discloses personally identifiable information from education records, except as permitted by FERPA
- The right to file a complaint with the U.S. Department of Education if they believe their FERPA rights have been violated

To exercise these rights with respect to data held by Fundraising University, parents may contact their child's school or contact us directly at support@fundraisingu.net.

5.5 Prohibition on commercial use. We do not use student educational records for any non-educational commercial purpose. We do not use student data to advertise, market products or services, or create commercial profiles of students.

5.6 Data return and deletion. Upon termination of services with a school, all student data associated with that school's campaigns will be returned to the school or securely deleted in accordance with the school's instructions and applicable law. See [Section 9](#) for our general data retention practices.

Section 6: COPPA Compliance Statement

Children's Online Privacy Protection Act

This section constitutes Fundraising University's COPPA Compliance Statement. It is also published as a standalone document for schools, groups and organizations that need to distribute it separately.

6.1 Applicability. The Fundraising University platform may be used by students under the age of 13 as part of fundraising programs supervised by schools, groups, or organizations. We recognize our obligations under

the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506, and the FTC's implementing regulations at 16 C.F.R. Part 312.

6.2 School and organization consent mechanism. When students under 13 use the Fundraising University platform as part of a program authorized by a school, group, or organization, we rely on the partnering school, group, or organization to act as the intermediary for obtaining verifiable parental consent on our behalf. This approach is consistent with FTC guidance permitting schools to consent on behalf of parents when an online service is used solely for an educational purpose.

Schools, groups, or organizations that use the Fundraising University platform for students under 13 are responsible for:

- Notifying parents about the use of the Fundraising University platform before student participation
- Obtaining verifiable parental consent before allowing students under 13 to access the platform
- Providing parents with this Privacy Policy (or a link to it)
- Ensuring that parents understand how to exercise their rights under COPPA

Disclosure: The Fundraising University platform does not currently include a built-in automated age verification or parental consent collection mechanism. The responsibility for ensuring that appropriate parental consent has been obtained before a student under 13 accesses the platform rests with the school, group, or organization partnering with Fundraising University. Fundraising University is committed to working with its partners to develop enhanced consent tools and processes.

6.3 Information collected from children under 13. For students under 13 who use our platform, we collect the following information:

- Phone number (used for login and device identification)
- First name and last name
- Opt-in preference for fundraising reminders
- Coach group assignment
- Engagement metrics (share clicks, page visits)
- Donor contact information entered by the student (contact names, phone numbers, relationship designations, and message text)

6.4 Information NOT collected from children under 13.

- Email addresses are not collected through the Student Fundraising Portal
- Social Security numbers are not collected
- Precise geolocation data is not collected from students
- Photographs, video, or audio recordings are not collected
- Biometric data is not collected
- No information is collected for behavioral advertising purposes

6.5 How we use and share children's information. Information collected from children under 13 is used solely to enable the student to participate in their school's fundraising campaign, to allow the student to enter donor contacts and compose fundraising messages, to track progress toward their goal, to enable coach oversight and support, to send fundraising reminders to students who have opted in, and for platform functionality, technical support, and security.

We share children's information only with the student's school and coach (for oversight and support), the Fundraising University franchise owner managing the campaign in that territory (aggregate performance data), Twilio (our SMS provider, for opt-in reminders to students — phone number and message content only), and Amazon Web Services (our cloud host, US-East-1). We do not share children's information with advertising networks, data brokers, social media platforms, or any other third party for commercial purposes. **Student records are explicitly excluded from our Mailchimp email marketing synchronization.**

6.6 Parental rights. Parents of children under 13 have the right to:

- Review personal information that Fundraising University has collected from their child
- Request deletion of their child's personal information
- Refuse to allow further collection or use of their child's information, and request that their child's account be deactivated
- Have their child participate without disclosing more personal information than is reasonably necessary to participate

To exercise these rights, parents may contact their child's school — the school can coordinate with us on the parent's behalf — or contact Fundraising University directly at support@fundraisingu.net or (602) 529-8293. We will respond to verified requests within 30 days. To protect the child's privacy, we may require the parent to verify their identity and their relationship to the child before processing the request.

6.7 No behavioral advertising or commercial profiling. We do not use information collected from children under 13 for behavioral advertising, targeted marketing, creating commercial profiles, or any purpose other than providing the fundraising service as described in this Privacy Policy.

6.8 Data retention for children's data. Personal information collected from children under 13 is subject to the same retention practices described in [Section 9](#) of this Privacy Policy. We retain children's personal information only as long as reasonably necessary to fulfill the purpose for which it was collected. Parents may request deletion of their child's data at any time by contacting support@fundraisingu.net; upon a verified deletion request we will delete the child's personal information within 30 days, except where retention is required by law. Upon termination of services with a school, all student data associated with that school's campaigns — including data from students under 13 — will be returned to the school or securely deleted in accordance with the school's instructions.

6.9 Security of children's data. We protect children's personal information using the same security measures we apply to all platform data, including SSL/TLS encryption for data in transit, secure cloud hosting on Amazon Web Services (US-East-1, Virginia), server access restricted to authorized personnel, phone-based verification and JWT authentication for the Student Portal, and no Google Analytics or third-party analytics tracking on the Student Portal. See [Section 12](#).

6.10 Changes to this statement. We may update this COPPA Compliance Statement from time to time. If we make material changes to how we collect, use, or share information from children under 13, we will notify schools and request that they inform parents accordingly. The "Last updated" date at the top of this policy will be revised to reflect the most recent version.

6.11 Operator information. The operator collecting information from children through the Fundraising University platform is:

KFRM LLC d/b/a Fundraising University

Email: support@fundraisingu.net

Phone: (602) 529-8293

Section 7: Student Data Privacy and State Law Compliance

7.1 Commitment to student privacy. Fundraising University is committed to protecting student privacy and complying with all applicable federal and state student data privacy laws, including but not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- California Student Online Personal Information Protection Act (SOPIPA, Cal. Bus. & Prof. Code §§ 22584–22585)
- California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA)
- Illinois Student Online Personal Protection Act (SOPPA, 105 ILCS 85/)
- Colorado House Bill 21-1110 and the Colorado Privacy Act (C.R.S. §§ 6-1-1301 *et seq.*)
- New York Education Law § 2-d
- Other applicable state student data privacy laws in jurisdictions where Fundraising University operates

7.2 Prohibition on advertising and marketing to students. We do not display targeted advertisements to students on the Fundraising University platform. We do not use student data to market products or services to students. We do not disclose student information for marketing or advertising purposes.

7.3 Prohibition on sale of student information. We do not sell student personal information to any third party for any purpose. We do not share student information with third parties for those third parties' own commercial purposes.

7.4 Data minimization. We collect only the minimum student data necessary to provide our fundraising services. We do not collect student email addresses through the Student Portal. We do not collect student grade levels, dates of birth, or Social Security numbers.

7.5 Security measures for student data. Student data is protected by the security measures described in [Section 12](#) of this Privacy Policy, including encryption in transit via SSL/TLS, server access controls, and secure cloud hosting on Amazon Web Services (AWS) in the US-East-1 (Virginia) region.

7.6 Third-party service provider obligations. Any third-party service provider that receives access to student data in connection with our services is bound by written agreements that require the provider to protect the confidentiality of student data, use student data only for the purposes specified by Fundraising University, comply with applicable student data privacy laws, and refrain from using student data for the provider's own commercial purposes.

7.7 California-specific rights

If you are a California resident, you have additional rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA):

- **Right to know:** You have the right to request that we disclose the categories and specific pieces of personal information we have collected about you, the categories of sources from which the information was collected, the business purpose for collecting the information, and the categories of third parties with whom we share the information.
- **Right to delete:** You have the right to request that we delete personal information we have collected from you, subject to certain exceptions.
- **Right to opt out of sale:** Fundraising University does not sell personal information. However, you have the right to direct us not to sell your personal information.
- **Right to non-discrimination:** We will not discriminate against you for exercising any of your CCPA/CPRA rights.

To exercise these rights, contact us at support@fundraisingu.net. We will respond to verified requests within 45 days as required by law.

7.8 Colorado-specific rights

If you are a Colorado resident, you have additional rights under the Colorado Privacy Act (CPA):

- **Right to opt out:** You have the right to opt out of the processing of your personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects. Fundraising University does not engage in any of these activities.
- **Right to access, correct, and delete:** You have the right to confirm whether we are processing your personal data, access your personal data, correct inaccuracies, and request deletion of your personal data.
- **Right to data portability:** You have the right to obtain your personal data in a portable and readily usable format.

To exercise these rights, contact us at support@fundraisingu.net.

7.9 Transparency and accountability. We maintain transparency about our data practices through this publicly available Privacy Policy, direct communication with schools and parents upon request, annual review and updates of our privacy practices, prompt notification of any data breaches in accordance with applicable law, and cooperation with schools regarding data access requests.

Section 8: For Donors — How Your Information Is Used

8.1 How you received a fundraising message. If you received a text message about a fundraising campaign, it was sent to you by a student you personally know — likely a friend or family member — from that student's own phone number. Fundraising University did not send the message. The student entered your name and phone number into our platform and used it to compose a message, which was then sent from the student's native SMS application on their personal device.

8.2 What information we collect about donors. Before you make a donation, the only information we have about you is what the student entered: your name, phone number, and relationship to the student. If you choose to make a donation or purchase products, we additionally collect your email address, shipping address, and a payment token generated by our payment processor (see Section 8.3).

8.3 Payment information. When you enter your payment information during checkout, your card details (card number, CVV, expiration date) are sent directly from your browser to our payment processor, Priority. Fundraising University does not receive, store, or have access to your full card number. We store only the payment token that Priority returns after successfully processing your card, along with transaction metadata (amount, date, status).

8.4 How to opt out. Because fundraising messages are sent from the student's personal phone, you can opt out by:

- Replying directly to the student who messaged you
- Contacting the student's parent or school
- Contacting Fundraising University at support@fundraisingu.net to request removal of your information

8.5 Donor rights. Donors have the right to:

- Know what information Fundraising University holds about them
- Request deletion of their information
- Opt out of future communications
- Contact us with privacy questions at support@fundraisingu.net

8.6 No marketing use. Fundraising University does not use donor contact information for its own marketing purposes. We do not sell, rent, or share donor information with third parties for marketing purposes.

Section 9: Data Retention and Deletion

9.1 Current practice. As of the effective date of this Privacy Policy, personal data collected through the Fundraising University platform is retained until a deletion request is received. We are actively developing formal retention schedules and automated deletion processes. Until those processes are implemented, the following retention guidelines apply.

9.2 Retention schedule.

Table 1: Data retention schedule by record type

Record type	Retention period
Student fundraising data (student profiles, contacts entered by students, engagement data)	Duration of the fundraising campaign plus 24 months, then deleted
Donor contact records (contact entries created by students)	Duration of the fundraising campaign plus 24 months, then deleted
Donor transaction and order records (donation history, purchase records, payment tokens)	7 years, to comply with tax and accounting requirements
Franchise owner and CRM data	Duration of the business relationship plus 24 months after termination
Analytics and log data	90 days, then deleted or anonymized

9.3 How to request deletion. You may request deletion of your personal data at any time by sending an email to support@fundraisingu.net. Please include your name and sufficient information for us to identify your records. We will respond to deletion requests within 30 days.

9.4 School data return or deletion. Upon termination of services with a school, we will return all student data associated with that school's campaigns to the school or securely delete it, in accordance with the school's instructions and applicable law.

9.5 Exceptions. We may retain personal data beyond the periods described above where retention is necessary for compliance with a legal obligation (such as tax reporting requirements), the establishment, exercise, or defense of legal claims, or the protection of vital interests.

Section 10: Third-Party Service Providers and Data Sharing

Fundraising University uses the following categories of third-party service providers in connection with our platform. We share personal data with these providers only to the extent necessary for them to perform their functions.

10.1 Payment processing: Priority. Priority is our primary payment processor for donor checkout. When a donor enters payment card information during checkout, the card details are sent directly from the donor's browser to Priority's gateway for tokenization. Fundraising University receives and stores only the resulting payment token and transaction metadata. Stripe identifiers are also stored on certain user and donor records for internal billing purposes.

10.2 SMS and communications: Twilio. We use Twilio's infrastructure for certain platform communications, including SMS reminders for students who have opted in. Twilio processes phone numbers and message content as necessary to deliver communications. Twilio is **not** used for student-to-donor fundraising outreach; those messages are sent by the student from the student's own device, as described in [Section 2.2](#).

10.3 Email marketing: Mailchimp. We use Mailchimp for email marketing communications to franchise staff and CRM contacts. **Student records are explicitly excluded from the Mailchimp synchronization process.** Student data is not shared with Mailchimp. CRM contact records and non-student user records (name, email, phone) may be synced to Mailchimp for franchise operational communications.

10.4 Cloud hosting: Amazon Web Services (AWS). The Fundraising University platform is hosted on Amazon Web Services infrastructure in the US-East-1 (Virginia) region. All platform data, including student data, donor data, and franchise operational data, is stored on AWS servers in the United States.

10.5 File storage: AWS S3. Uploaded files and documents are stored using Amazon S3 (Simple Storage Service).

10.6 Analytics: Google Analytics 4. Google Analytics 4 is used on the public-facing fundraising pages and checkout experience only. Google Analytics is **not** used on the Student Fundraising Portal. Google Analytics collects usage data as described in [Section 3.6](#).

10.7 Business intelligence: Apache Superset. The franchise management ERP embeds Apache Superset dashboards (hosted by our development partner) for internal business intelligence and analytics. This is used by franchise owners and internal staff only and does not collect data from students or donors.

10.8 Authentication: Google OAuth. CRM users (franchise owners, staff) may authenticate using Google OAuth. This is used for the internal ERP system only, not for the Student Portal or donor-facing pages.

10.9 Content delivery networks (CDNs). The platform loads interface assets (icons, fonts, scripts) from third-party CDNs including jsDelivr, unpkg, Google Fonts, Font Awesome, and cdnjs. These CDNs deliver static files and do not receive personal data from Fundraising University.

10.10 Contractual obligations. All third-party service providers that receive access to personal data are bound by written agreements requiring them to protect the confidentiality of personal data, use data only for the purposes specified by Fundraising University, comply with applicable privacy laws, and refrain from using data for their own commercial purposes.

10.11 No sale of personal information. Fundraising University does not sell personal information to any third party for any purpose.

Section 11: Cookies and Tracking Technologies

11.1 What are cookies. A cookie is a small file containing an identifier that is sent by a web server to a web browser and stored by the browser. Cookies may be "persistent" (stored until their expiry date or until deleted) or "session" cookies (expiring when the browser is closed).

11.2 Public-facing fundraising pages and checkout. The donor-facing fundraising pages and checkout experience use Google Analytics 4 measurement cookies and session cookies for authentication and basic functionality.

11.3 Student Fundraising Portal. The Student Fundraising Portal does **not** use Google Analytics cookies or any third-party analytics tracking cookies. Authentication is handled via JSON Web Tokens (JWT) stored in

the browser's localStorage, not cookies. The Portal loads interface assets from third-party CDNs (jsDelivr, unpkg), which may set their own cookies according to their respective privacy policies.

11.4 Franchise management ERP. The internal ERP system uses cookie-based authentication and Google OAuth session management. No Google Analytics is present in the shared layout of the ERP.

11.5 Safety & Compliance Center pages. The pages in this Safety & Compliance Center — this page and those linked in the navigation above — set no cookies at all and load no fonts, scripts, images, or analytics from any third party.

11.6 Managing cookies. Most browsers allow you to refuse or delete cookies. Methods for doing so vary by browser. You can find instructions for managing cookies in your browser's help documentation. Blocking all cookies may affect your ability to use certain features of the platform.

11.7 Do Not Track. Some browsers include a "Do Not Track" feature. The Fundraising University platform does not currently respond to Do Not Track signals. However, as noted above, the Student Fundraising Portal does not use analytics tracking.

Section 12: Security of Information

12.1 Encryption in transit. All data transmitted between your browser and the Fundraising University platform is encrypted using SSL/TLS (Secure Socket Layer / Transport Layer Security) technology.

12.2 Server access controls. The Fundraising University platform is hosted on Amazon Web Services (AWS) infrastructure with access restricted to authorized personnel. Application containers run in a managed Docker environment with controlled deployment access.

12.3 Payment security. Payment card data is handled through browser-to-gateway tokenization with our payment processor, Priority. Donor card numbers, CVV codes, and expiration dates are sent directly from the donor's browser to Priority's secure gateway and are never received or stored by Fundraising University's servers. Only payment tokens and transaction metadata are stored on our systems.

12.4 Authentication security. The Student Fundraising Portal uses phone-based verification and JWT (JSON Web Token) authentication. The franchise management ERP uses cookie-based authentication with optional Google OAuth. Passwords for CRM users are stored in hashed form.

12.5 Your responsibilities. You are responsible for maintaining the confidentiality of your login credentials and for controlling access to your devices. If you believe your account has been compromised, contact us immediately at support@fundraisingu.net.

12.6 No guarantee. While we implement reasonable security measures, no method of electronic transmission or storage is 100% secure. We cannot guarantee absolute security of your information.

Section 13: Your Rights

13.1 Depending on your jurisdiction and your relationship with the Fundraising University platform, you may have some or all of the following rights with respect to your personal data:

- **(a) Right to access:** You have the right to confirm whether we process your personal data and to access a copy of that data.
- **(b) Right to rectification:** You have the right to request correction of inaccurate or incomplete personal data.
- **(c) Right to erasure or deletion:** You have the right to request deletion of your personal data, subject to certain exceptions (such as legal retention obligations).
- **(d) Right to restrict processing:** In certain circumstances, you have the right to restrict our processing of your personal data.
- **(e) Right to data portability:** You have the right to receive your personal data in a structured, commonly used, and machine-readable format.
- **(f) Right to opt out of sale:** Fundraising University does not sell personal information. However, you have the right to direct us not to sell your personal information.
- **(g) Right to non-discrimination:** We will not discriminate against you for exercising your privacy rights.
- **(h) Right to withdraw consent:** Where our processing of your personal data is based on your consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

13.2 California-specific rights. California residents have additional rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), including the right to know the categories and specific pieces of personal information collected, the right to delete, and the right to opt out of the sale of personal information. See [Section 7.7](#) for details.

13.3 Colorado-specific rights. Colorado residents have additional rights under the Colorado Privacy Act, including the right to opt out of targeted advertising and profiling. See [Section 7.8](#) for details.

13.4 How to exercise your rights. To exercise any of the rights described above, please contact us at:

Email: support@fundraisingu.net

Phone: (602) 529-8293

We will respond to verified requests within 30 days (or within 45 days for CCPA/CPRA requests, as required by California law). We may require you to verify your identity before processing your request.

13.5 Right to lodge a complaint. If you believe that our processing of your personal information violates applicable law, you have the right to lodge a complaint with the appropriate regulatory authority. For FERPA complaints, contact the U.S. Department of Education, Student Privacy Policy Office. For COPPA complaints, contact the Federal Trade Commission. For state-specific privacy complaints, contact your state's attorney general.

Section 14: Breach Response Plan

14.1 Overview

Any individual who suspects that a theft, breach, or exposure of Fundraising University protected or sensitive information has occurred must immediately provide a description of what occurred via email to support@fundraisingu.net or by calling (602) 529-8293. This contact is monitored and communicated to the Fundraising University Principal Privacy Officer (PPO). The PPO will investigate all reported thefts, data breaches, and exposures to confirm whether a breach has occurred. If a breach is confirmed, the PPO will follow the appropriate response procedures.

14.2 Scope

This plan applies to all individuals who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle non-public information (NPI) or personally identifiable information (PII) of Fundraising University and its clients. Any agreements with third-party vendors will contain language referencing this plan.

14.3 Response procedures

Upon confirmation of a data breach:

1. All access to the affected resource will be removed immediately.
2. The PPO will convene an incident response team, which may include representatives from IT, legal, communications, client services, human resources, and other relevant departments.
3. IT and designated forensic resources will analyze the breach to determine the root cause.
4. A communication plan will be developed in coordination with legal and communications to determine how to notify affected individuals, internal staff, and the public as required by applicable law.
5. Notification of affected individuals will be made as required by applicable federal and state breach notification laws.

14.4 Third-party provider breaches

Any third-party provider engaged by Fundraising University that handles NPI or PII is required to notify the PPO of any theft, breach, or exposure. Fundraising University remains responsible for notifying affected individuals of breaches that involve their data, regardless of whether the breach occurred at Fundraising University or at a third-party provider.

14.5 Enforcement

Any Fundraising University personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner found in violation may have their relationship with Fundraising University terminated in accordance with the applicable agreement.

Section 15: Contact Information

For questions about this Privacy Policy, to request access to or deletion of your personal data, to report a privacy concern, or for any other privacy-related inquiry, please contact us at:

Fundraising University

KFRM LLC d/b/a Fundraising University

Email: support@fundraisingu.net

Phone: (602) 529-8293

We will respond to all privacy inquiries within 30 days. For CCPA/CPRA requests from California residents, we will respond within 45 days as required by law.

[Accessibility Statement and Conformance Report \(ACR/VPAT\)](#)

[TCPA Compliance Statement](#)

[Return to the Safety & Compliance Center](#)

Effective August 4, 2026. Last updated August 4, 2026. Published by KFRM LLC d/b/a Fundraising University.

KFRM LLC d/b/a Fundraising University

support@fundraisingu.net · (602) 529-8293

Published at <https://fundraisingu.net/safety/privacy-policy/>. That page is the authoritative version of this document; where this PDF and the page differ, the page governs.