Grey Street

Privacy Policy & A2P 10DLC Messaging Policy

Combined Privacy and Messaging Compliance Policy

This document combines the Grey Street Privacy Policy (Part I) with the A2P 10DLC Messaging Compliance Policy (Part II), prepared for The Campaign Registry brand and campaign registration and for carrier review under the CTIA Messaging Principles and Best Practices.

Field	Detail
Entity	Grey Street
Business	Managed technology services provider (MSP) and business consulting
Jurisdiction	State of Georgia, United States
Contents	Part I: Privacy Policy · Part II: A2P 10DLC Messaging Policy
Policy version	1.0
Effective date	July 1, 2026
Published at	thegreystreet.com/privacy
Review cadence	Annual, or upon regulatory or carrier change

PART I

Privacy Policy

Effective Date: June 6, 2026 **Last Updated:** June 15, 2026

Grey Street ("we," "us," or "our") is a business consulting and managed technology services provider (MSP) serving small and mid-sized businesses in the Atlanta metropolitan area. In the course of delivering our services, we design, deploy, monitor, and manage our clients' information technology environments — including servers, networks, infrastructure devices, and end-user systems — and we are entrusted with access to systems and information that are often sensitive and, in many cases, subject to industry-specific regulation.

This Privacy Policy explains the information we collect, how we access and handle client systems and data, how we manage credentials and access, and the safeguards and choices that apply. It covers our website visitors, our clients and prospective clients, and the systems and information we access while providing managed services.

> **A note on regulated data.** Our clients operate across many industries — including healthcare and dental practices, financial services, and businesses that process card payments — each with its own regulatory obligations such as HIPAA, PCI DSS, and applicable state privacy laws. Grey Street accesses client information only as needed to provide services, and we follow the security and confidentiality protocols that apply to each client's industry. Where required, we enter into written agreements, such as Business Associate Agreements (BAAs) or data processing terms, that govern our handling of regulated information.

1. Information We Collect

The information we collect depends on your relationship with us and the services we provide.

Website visitors

- **Information you provide —** details submitted through contact or quote-request forms, such as your name, business name, email address, phone number, and the contents of your message.
- **Automatically collected information —** standard technical data such as IP address, browser and device type, pages visited, and the dates and times of visits, collected through cookies and similar technologies.

Clients and prospective clients

- **Business and contact information —** company name, points of contact, email addresses, phone numbers, service addresses, and billing and payment details.
- **Engagement records —** service agreements, support tickets, project documentation, asset inventories, and records of work performed.

Information accessed while delivering services

To manage our clients' technology environments, we access and maintain a range of information and systems on their behalf. Depending on the engagement, this may include:

- **System and configuration data —** server, network, and device configurations; network topology; software inventories; logs; and monitoring and performance data.
- **Account and identity data —** user accounts, group memberships, permissions, and directory information used to provision and manage access.
- **Credentials —** administrative and service credentials, passwords, keys, and other authentication secrets required to manage client systems.
- **Client business data —** data residing on systems we manage, which may include sensitive or regulated information belonging to our clients and their customers, patients, or employees.

2. Access to Client Systems and Devices

Managed services require us to access, configure, and control client systems. We do so under the authority of our service agreements and according to the practices below.

Server and infrastructure access

We access servers, network equipment, firewalls, wireless infrastructure, and other devices to deploy, configure, patch, monitor, troubleshoot, and maintain them. Access is limited to authorized Grey Street personnel and to the scope necessary to deliver the agreed services.

Account creation, management, and termination

On our clients' behalf, we create, modify, disable, and remove user and administrative accounts; assign and adjust permissions and group memberships; and manage the full lifecycle of access. When a client requests account termination — for example, when an employee departs — we disable or remove access and revoke associated credentials in accordance with the client's instructions and policies.

Remote access and control

We use remote monitoring and management (RMM), remote-access, and similar tools to connect to and control end-user devices and infrastructure. This allows us to provide support, apply updates, resolve issues, and respond to alerts without requiring an on-site visit. Remote sessions are conducted by authorized personnel and may be logged. Where our tools support it, we seek user awareness or consent for interactive remote-control sessions on end-user devices.

Monitoring, logging, and alerting

We monitor the systems we manage for availability, security, and performance, and we collect logs and alerts to detect and respond to issues. Monitoring is directed at the operation and security of client systems, not at the personal activity of individual users beyond what is necessary to maintain and secure those systems.

3. Credential and Password Management

Managing access responsibly is central to our work. Our practices for handling credentials and passwords include:

- **Secure storage and retention —** credentials and passwords are stored in an encrypted, access-controlled password-management system and retained only as long as needed to service the client relationship.
- **Least privilege —** access to credentials is restricted to personnel who require it for their role and the task at hand.
- **Password creation and changes —** we set, rotate, and change passwords as part of routine maintenance, in response to staffing changes, after suspected or confirmed security incidents, and at our clients' request.
- **Multi-factor authentication —** where available, we use and recommend multi-factor authentication to protect administrative and sensitive access.
- **Revocation —** credentials are revoked or rotated promptly when access is no longer required, when personnel change, or at the conclusion of an engagement.

4. Sensitive and Regulated Information

Because we serve clients in regulated industries, we may have access to sensitive and regulated information held within the systems we manage — such as protected health information, payment card data, financial records, and personal information. We treat this information as confidential and access it only as necessary to provide our services.

Grey Street follows the security and compliance protocols that apply to each client's industry and to each area of their business. Where our role brings us within the scope of a regulatory framework — for example, acting as a business associate under HIPAA or as a service provider subject to PCI DSS — we enter into the appropriate agreements and handle information in accordance with those obligations. We do not use client business data for any purpose other than delivering and supporting the contracted services, unless the client directs otherwise or the law requires it.

5. How We Use Information

We use the information we collect to:

- Provide, maintain, monitor, secure, and support our clients' technology environments.
- Provision and manage accounts, access, and credentials on our clients' behalf.
- Diagnose and resolve issues, respond to alerts, and perform maintenance and projects.
- Communicate with clients and respond to inquiries from prospective clients.
- Prepare proposals, perform billing, and administer our agreements.
- Operate, maintain, and improve our website and our services.
- Meet our legal, regulatory, and contractual obligations.

6. How We Share Information

We do not sell personal information. We share information only as necessary to deliver our services and operate our business, and as permitted or required by law. This may include sharing with:

- **Technology vendors and subprocessors —** providers of the RMM, monitoring, backup, security, password-management, ticketing, and cloud platforms we use to deliver services, under agreements that require them to protect the information they handle.
- **Client-authorized third parties —** manufacturers, carriers, or other providers engaged at a client's direction or with their authorization.
- **Professional advisors —** our own accountants, attorneys, and insurers, as needed to run our business.
- **Legal and regulatory authorities —** when required by law, subpoena, court order, or to protect our rights, our clients, or the security of the systems we manage.

7. How We Protect Information

We maintain administrative, technical, and physical safeguards designed to protect the information and systems entrusted to us. These include access controls and least-privilege practices, encryption of stored credentials, multi-factor authentication, logging and monitoring, staff training, and policies governing the handling of sensitive information. No safeguard is perfect, and we cannot guarantee absolute security; in the event of a security incident affecting client or personal information, we will respond and provide notification in accordance with our agreements and applicable law.

8. Data Retention

We retain information for as long as necessary to provide our services, support and document our engagements, meet legal, regulatory, and contractual obligations, and resolve disputes. Credentials and access are retained only for the duration of the relationship and are revoked or securely destroyed when no longer required. Upon the conclusion of an engagement, we handle the return or disposal of client information as set out in the applicable agreement.

9. Confidentiality

All Grey Street personnel are bound by obligations of confidentiality. Access to client systems and information is granted on a need-to-know basis, and we expect our staff and subprocessors to handle client information with the same care described in this policy and in our service agreements.

10. Cookies and Website Analytics

Our website may use cookies and similar technologies to operate the site, remember preferences, and understand how visitors use our pages. Most browsers allow you to refuse or delete cookies through their settings; doing so may affect how parts of the website function.

11. Third-Party Links

Our website may link to sites operated by others. We are not responsible for the privacy practices or content of those sites, and we encourage you to review their policies.

12. Your Choices and Rights

If you are a website visitor or prospective client, you may contact us to ask what information we hold about you, request corrections, or ask that we delete inquiry information we no longer need. For information that resides within systems we manage on a client's behalf, the client controls that data; requests from the client's own users, customers, or patients should be directed to the client, and we will support the client in responding as our agreements provide. Depending on your location, additional privacy rights may apply.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices or legal requirements. When we make changes, we will revise the "Last Updated" date above and post the current version on our website.

14. Contact Us

If you have questions about this Privacy Policy or our data-handling practices, please contact us:

Grey Street
Email: hello@thegreystreet.com

This document is a general template provided for convenience and does not constitute legal advice. Because Grey Street serves clients in regulated industries, this policy should be reviewed by a qualified attorney and aligned with your service agreements, Business Associate Agreements, and any client-specific compliance obligations before use.

PART II

A2P 10DLC Messaging Compliance Policy

SMS and MMS Consent, Opt-In, and Opt-Out Program

Prepared for The Campaign Registry brand and campaign registration and for carrier review under the CTIA Messaging Principles and Best Practices.

Field	Detail
Entity	Grey Street
Jurisdiction	State of Georgia, United States
Business	Managed technology services provider (MSP)
Policy version	1.0
Effective date	July 1, 2026
Review cadence	Annual, or upon regulatory or carrier change

1. Purpose and Scope

This policy governs how Grey Street sends application-to-person (A2P) text messages to mobile phones in the United States over 10-digit long code (10DLC) numbers. It documents the consent, opt-in, opt-out, content, and record keeping practices that Grey Street follows so that its messaging is lawful, is honest with recipients, and is approvable by The Campaign Registry (TCR) and the mobile carriers.

The policy applies to every text message Grey Street or any platform acting on its behalf sends to clients, client contacts, prospective clients, and staff, and to every person who authors, schedules, or reviews those messages. It covers messages sent through the company website, through contact and quote-request forms, through a customer relationship, ticketing, or scheduling system, and through any campaign service provider (CSP) such as Twilio.

2. Company and Messaging Overview

Grey Street is a business consulting and managed technology services provider (MSP) serving small and mid-sized businesses in the Atlanta metropolitan area. Its messaging exists to support the client service relationship. Grey Street texts clients and their authorized contacts to schedule and confirm service appointments and maintenance windows, to send support-ticket updates and system, outage, or security alerts for the environments it manages, and to deliver account and billing notices. Where a person has separately asked to hear from Grey Street about its services, the company may also send limited follow-up to that inquiry.

Grey Street does not buy phone number lists, does not send messages to numbers it did not collect directly, and does not send content outside the use cases it registers. Every registered campaign

describes a real program that a recipient has agreed to receive.

3. Regulatory Framework

Grey Street builds its messaging program on the strictest standard that applies to a given recipient. The following authorities govern the program.

3.1 Telephone Consumer Protection Act (TCPA)

The TCPA is the federal law, enforced by the FCC and through private litigation, that requires consent before a business sends automated texts. It requires prior express written consent for marketing or promotional messages and prior express consent for transactional or informational messages. Statutory damages run from 500 dollars to 1,500 dollars per message, so consent records matter.

3.2 CTIA Messaging Principles and Best Practices

The CTIA guidelines are the industry standard that the carriers (AT&T, T-Mobile, and Verizon) enforce when they decide whether to deliver, filter, or block traffic. They set the expectations for consent, sender identity, opt-out handling, and prohibited content. Following the CTIA guidelines is the practical route to carrier approval and, in most cases, to TCPA compliance as well.

3.3 A2P 10DLC registration through The Campaign Registry

The carriers block unregistered 10DLC traffic outright. Grey Street must register a brand (its business identity, tied to its EIN) and one or more campaigns (each messaging use case) with The Campaign Registry through its CSP. This policy is the source document for the answers Grey Street provides during that registration, including the consent question addressed in Section 6.

3.4 CAN-SPAM and messaging honesty

Grey Street does not use deceptive sender identity or misleading content, identifies itself in its messages, and honors opt-out requests promptly, consistent with the honesty principles that carry over from CAN-SPAM into messaging.

3.5 Sensitive client data and industry protocols

Grey Street serves clients in regulated industries and may handle regulated data on their behalf, including as a business associate under HIPAA or as a service provider subject to PCI DSS. Its text messaging program is operational and is addressed to authorized client contacts. Grey Street does not transmit client end-user regulated data — such as protected health information or payment card data — or system credentials over SMS. Messages are limited to the minimum necessary, such as a contact name, a ticket or visit reference, or a request to call, and Grey Street follows the security and confidentiality protocols that apply to each client's industry. Standard SMS is not encrypted; Grey Street informs recipients of this and honors any request to receive communications by another method or at an alternative number or address.

3.6 Georgia and other state law

Several states impose SMS rules that are stricter than the federal TCPA, including tighter quiet hours and consent standards. Grey Street applies the strictest rule that applies based on the recipient's state of residence and follows Georgia law for its in-state operations.

> **Not legal advice.** This document reflects the CTIA guidelines, the TCPA, and carrier registration requirements as they stand in 2026. It is an operating policy, not a legal opinion. Grey Street should have counsel review it before submission, and should confirm current TCR field wording inside its CSP account, because carrier questions are periodically reworded.

4. Definitions

Term	Meaning
A2P	Application-to-person messaging, meaning texts sent by software or a platform rather than typed by one person on a phone.
10DLC	A standard 10-digit local phone number sanctioned by carriers for A2P messaging.
TCR	The Campaign Registry, the central database of registered brands and campaigns that carriers rely on.
CSP	Campaign Service Provider, the messaging platform (for example Twilio) that submits registration and sends traffic.
Brand	The registered legal identity of Grey Street, tied to its EIN.
Campaign	A registered messaging use case with its own description, sample messages, and consent method.
Express written consent	A recipient's clear, documented, written agreement to receive marketing texts before the first such message.
Express consent	A recipient's agreement to receive transactional or informational texts, typically by knowingly providing a mobile number for that purpose.
Opt-in	The action by which a recipient agrees to receive messages.
Opt-out	The action by which a recipient revokes consent, for example by replying STOP.

5. Registered Campaign Use Cases

Grey Street registers only the use cases below and sends only content consistent with them. Most of its messaging is transactional and tied to an existing service relationship. Any promotional follow-up is registered separately and held to the higher written consent standard.

Use case	Consent standard	What the recipient receives
Service scheduling and coordination	Express consent	Appointment scheduling, changes, technician assignment, and requests to call about service.
Maintenance and appointment reminders	Express consent	Reminders and confirmations of scheduled service visits and maintenance windows.
Support tickets and system alerts	Express consent	Support-ticket updates and monitoring, outage, or security alerts for managed systems.

Account and billing notices	Express consent	Operational notices such as invoices, payment reminders, and documentation requests.
Inquiry and sales follow-up (limited promotional)	Express written consent	Replies and follow-up to people who asked to hear from Grey Street, for example through a form.

6. Consent and Opt-In

Consent is the foundation of the program. Grey Street obtains consent before it sends messages, matches the type of consent to the type of message, keeps a record of every opt-in, and lets any recipient withdraw consent at any time. Consent is never a condition of purchasing or receiving any service, and Grey Street never uses pre-checked boxes to manufacture agreement.

6.1 Consent standard by message type

- **Transactional and service messages.** For scheduling, reminders, ticket and system alerts, and account notices, the recipient gives express consent by knowingly providing their mobile number to Grey Street for that purpose, in a context where the messaging use is disclosed.
- **Marketing and promotional messages.** For any follow-up that promotes Grey Street rather than serving an existing service relationship, the recipient must give prior express written consent through a clear, documented action such as checking an unchecked box or submitting a form that states what they are agreeing to.
- **Conversational messages.** When a person texts Grey Street first and the company simply replies with relevant information, that exchange is conversational and needs no separate opt-in, though opt-out support still applies.

6.2 How recipients opt in

- **Website contact or quote form.** A client or prospect enters their mobile number on the Grey Street website and agrees to SMS through an unchecked consent box placed next to the disclosure in Section 6.3. The submission is time stamped and stored.
- **Lead or landing-page form.** A person who responds to Grey Street outreach submits their number through a form that carries the same disclosure and an affirmative consent step before submission.
- **Verbal or in-person opt-in.** During a consultation, onboarding, or service call, a client contact provides a mobile number and agrees to receive service-related texts. Staff record the consent, including who agreed, the date, and the phone number.
- **Service agreement or paper form.** A client signs a service agreement or paper form that includes the SMS disclosure and provides a mobile number. The signed form is retained.

6.3 Disclosure shown at the point of opt-in

Every web and lead form opt-in presents the following disclosure beside the consent control. It names the sender, describes the messages, states that frequency varies, gives the help and stop instructions, states that message and data rates may apply, and confirms that consent is not a condition of service.

> By providing my mobile number and checking this box, I agree to receive text messages from Grey Street about service scheduling, appointment and maintenance reminders, support and system alerts, and account or billing notices. Message frequency varies. Message and data rates may apply. Reply HELP for help or STOP to unsubscribe at any time. Consent is not a condition of purchase or service. See our Privacy Policy and SMS Terms at thegreystreet.com/privacy

For any campaign that includes promotional follow-up, the disclosure names that purpose as well, and the consent control is separate from any general contact submission so that agreement to marketing is distinct and affirmative.

6.4 Opt-in confirmation message

For each recurring program, the first message Grey Street sends confirms the opt-in, identifies the sender, states the message frequency, and repeats the help and stop instructions. A sample confirmation appears in Section 12.

6.5 Proof of consent and record keeping

Grey Street keeps a record of each opt-in that captures, at a minimum, the phone number, the date and time of consent, the method of consent, and the exact disclosure text the person saw or heard. Screenshots of the web form, the lead form, and any paper form are hosted at a publicly reachable link so carrier reviewers can verify the opt-in flow during registration. Verbal opt-ins are supported by dated records. These records are retained for at least four years.

> **Consent data is never sold or shared.** Grey Street does not sell or share SMS opt-in or consent information with third parties for their own marketing. The only sharing is with service providers, such as the CSP, that help deliver the messages. The Grey Street Privacy Policy states this, because a privacy policy that permits sharing or selling opt-in data is treated as noncompliant by the carriers.

---

7. Answer to the Registration Question

How do SMS recipients consent to receive messages?

This is the exact question The Campaign Registry and the carriers ask during campaign registration. Grey Street provides the answer below. A short version fits the character-limited field, and the fuller version supports manual review. Both describe the same real flow, which the hosted screenshots verify.

Short version (paste into the TCR consent field)

> Recipients opt in by knowingly providing their mobile number to Grey Street and affirmatively agreeing to receive texts. On our website and lead forms, the person enters their number and checks an unchecked consent box next to this disclosure: “By providing my mobile number and checking this box, I agree to receive text messages from Grey Street about service scheduling, appointment and maintenance reminders, support and system alerts, and account or billing notices. Message frequency varies. Message and data rates may apply. Reply HELP for help or STOP to unsubscribe. Consent is not a condition of service. See our Privacy Policy and SMS Terms at thegreystreet.com/privacy.” We also collect verbal and written opt-ins and retain a dated record of each. We do not sell or share opt-in data. A screenshot of the opt-in form is hosted at thegreystreet.com/privacy

Fuller version (for the campaign description or manual review)

Grey Street is an Atlanta-area managed technology services provider. Recipients are our clients and their authorized contacts, and people who ask to hear from us. They consent in one of four ways, each of which discloses the program and creates a record:

- **Web contact or quote form:** the person enters a mobile number and checks an unchecked consent box beside the SMS disclosure before submitting. The submission is time stamped and stored.
- **Lead or landing-page form:** a person responding to our outreach submits a mobile number through a form carrying the same disclosure and an affirmative consent step.
- **Verbal or in-person opt-in:** a client contact provides a number and agrees to service-related texts, which staff record with the name, date, and number.
- **Signed service agreement or paper form:** a client signs a form that includes the disclosure and provides a number, and the form is retained.

In every case the disclosure names Grey Street as the sender, describes the message types, states that frequency varies and that message and data rates may apply, provides HELP and STOP instructions, and confirms that consent is not a condition of service. We keep proof of each opt-in (number, date, method, and the disclosure shown), host screenshots of the forms at a publicly reachable link for verification, and never sell or share opt-in or consent data with third parties for their own purposes.

---

8. Opt-Out and Revocation of Consent

A recipient may withdraw consent at any time, and Grey Street honors it immediately. The program supports the standard opt-out keywords and treats any reasonable expression of a wish to stop as a valid opt-out, whether it arrives by text, phone call, email, or in person.

Keyword	Effect	
STOP, UNSUBSCRIBE, QUIT, CANCEL, END, REVOKE	Ends messaging	Any of these, in any letter case, ends messaging for that number. The system sends one final confirmation and then suppresses the number.
START, UNSTOP, YES	Re-subscribes	Re-subscribes a number that had previously opted out, if the person chooses to return.

HELP, INFO	Support	Returns support contact information and the name of the program (see Section 9).

8.1 How opt-outs are handled

- An opt-out takes effect immediately, and no further campaign messages are sent to that number except a single opt-out confirmation.
- The opted-out number is recorded and suppressed so it is not re-enrolled in any future campaign or workflow.
- Opt-outs received by another reasonable method, such as a phone call or email, are honored, and the number is suppressed within ten business days at the latest, though the aim is same-day.
- Opt-out instructions appear in at least one message per month for any recurring program, so recipients always know how to stop.

> **Service continuity note.** If a client opts out of texts, Grey Street continues to reach them about urgent service matters — such as an outage or security incident — through other channels, such as a phone call or email. The opt-out ends the text channel, not the service relationship.

9. HELP and Support

A recipient who replies HELP or INFO, or who does not know how to reach Grey Street, receives a reply that identifies the program, gives a support phone number, and repeats the stop instruction. A sample HELP reply appears in Section 12. Recipients can also reach Grey Street through the phone number and contact form on the company website.

10. Message Content Standards

- **Sender identity.** Every message, or at least the first message in an exchange, identifies Grey Street by name so recipients always know who is texting.
- **Minimum necessary information.** Messages avoid sensitive detail and never include system credentials or client end-user regulated data such as protected health information or payment card data. Sensitive detail is handled by phone or a secure channel rather than SMS.
- **No prohibited content.** Grey Street sends no content in the restricted SHAFT categories (sex, hate, alcohol, firearms, tobacco) and none of the other categories carriers restrict, such as high-risk financial offers.
- **Links.** Messages avoid public URL shorteners such as generic bit.ly or tinyurl links, which trigger carrier spam filters, and use the Grey Street domain or a dedicated branded link instead.
- **Consistency with registration.** Grey Street sends only content that matches its registered use cases. Sending off-topic content is a common reason campaigns get flagged.

11. Message Frequency and Timing

Message frequency varies with each client's service activity and is disclosed at opt-in as varying rather than a fixed number. Grey Street sends messages during reasonable hours, generally 8:00 AM to 9:00 PM in the recipient's local time, and applies any stricter quiet hours required by the recipient's state. Urgent service-related contact that a client would expect, such as an outage or security alert, is the narrow exception, and is handled with judgment and, where needed, by phone.

12. Sample Messages

The samples below reflect the actual messages Grey Street sends. Bracketed fields are filled at send time. At least one sample in each campaign carries the sender name and the opt-out instruction, as carriers require.

Opt-in confirmation

```
Grey Street: You are now subscribed to service and support texts. Msg frequency
varies. Msg & data rates may apply. Reply HELP for help, STOP to unsubscribe.
```

Service appointment reminder

```
Grey Street: Reminder of your service visit on [date] at [time]. Reply C to confirm
or call (678) 212-1090 to reschedule. Reply STOP to opt out.
```

Support ticket update

```
Grey Street: Update on ticket [#] – [status]. Questions? Call (678) 212-1090. Reply
STOP to opt out.
```

Maintenance or outage notice

```
Grey Street: A maintenance window for your systems is scheduled [date] [time
window]. Details at thegreystreet.com. Reply STOP to opt out.
```

Billing reminder

```
Grey Street: Invoice [#] is due [date]. View or pay at thegreystreet.com.
Questions? Call (678) 212-1090. Reply STOP to opt out.
```

HELP reply

```
Grey Street service texts. For help call (678) 212-1090 or visit thegreystreet.com.
Reply STOP to unsubscribe.
```

Opt-out confirmation

```
Grey Street: You are unsubscribed and will get no more texts from this program. We
will still reach you about urgent service matters by phone. Reply START to rejoin.
```

13. Privacy and Data Handling

- Grey Street publishes a Privacy Policy and SMS Terms on its website at thegreystreet.com/privacy, reachable from the opt-in disclosure, and keeps them current.
- SMS opt-in and consent data is not sold or shared with third parties for their own marketing, and the Privacy Policy states this plainly.
- Data is shared only with service providers, such as the CSP, that are needed to deliver messages, and only for that purpose.
- Grey Street does not place phone numbers, credentials, or regulated client data in message links or web addresses, and follows each client's industry protocols.

14. Recordkeeping, Audit, and Renewal

- Consent records (number, date and time, method, and disclosure shown) are retained for at least four years and are available for audit.
- Opt-out and suppression records are retained so no opted-out number is re-enrolled.
- Screenshots of the opt-in forms are hosted at a publicly reachable link for carrier verification during registration.
- Brand and campaign registrations are renewed on the annual cycle the CSP and TCR require, and registered content is reviewed to confirm it still matches what Grey Street actually sends.

15. Roles and Responsibilities

Role	Responsibility
Policy owner	Maintains this policy, approves campaign registrations, and reviews the program annually.
Client onboarding staff	Collect and record consent correctly, and give clients the disclosure and opt-out information.
Messaging operator	Sends only registered content, honors opt-outs immediately, and keeps consent and suppression records.
CSP (for example Twilio)	Submits brand and campaign registration to TCR and provides the delivery platform and compliance tooling.

16. Policy Review and Acknowledgment

Grey Street reviews this policy at least once a year and whenever the TCPA, the CTIA guidelines, state law, or carrier and CSP requirements change. Everyone who authors, schedules, or reviews messages reads and follows it. Questions about the policy go to the policy owner.

This document is a general operating policy provided for convenience and does not constitute legal advice. Grey Street should have qualified counsel review it before brand and campaign registration, and should confirm current TCR field wording inside its CSP account.