



SiteFolio Privacy Policy

Effective Date: June 22, 2026

Last Updated: June 22, 2026



Table of Contents

1. Scope of This Policy	3
2. Our Role	4
3. Personal Information We Collect	4
3.1 Account and User Information	4
3.2 Company and Site Information	5
3.3 Worker Information	5
3.4 Uploaded Documents	6
3.5 Payment and Billing Information	6
3.6 Technical and Usage Information	7
3.7 Communications	7
4. How We Collect Personal Information	8
5. How We Use Personal Information	8
6. Consent and Customer Responsibilities	9
7. Sensitive Information	9
8. How We Share Personal Information	10
8.1 With Customers and Authorized Users	10
8.2 With Service Providers	10
8.3 With Professional Advisors	11
8.4 For Legal and Safety Reasons	11
8.5 Business Transactions	11
8.6 With Consent	12
9. International Storage and Processing	12
10. Security Safeguards	12
11. Data Retention	13
12. Access, Correction, and Deletion	14
13. Accuracy	14
14. Cookies and Analytics	15
15. Email and Electronic Communications	15
16. Worker and Emergency Contact Information	15
17. Children and Minors	16
18. Privacy Breaches	16
19. Service Providers and Subprocessors	16
20. De-Identified and Aggregated Information	17
21. Links to Third-Party Sites	17
22. Changes to This Privacy Policy	18
23. Challenging Compliance and Questions	18
24. Contact Information	18



This Privacy Policy explains how **SiteFolio Technologies** (“SiteFolio,” “we,” “us,” or “our”) collects, uses, discloses, stores, retains, and protects personal information when individuals use SiteFolio, visit our website, create accounts, accept invitations, upload documents, submit worker information, receive notifications, or otherwise interact with our services.

SiteFolio is built for construction workforce compliance and onboarding. The platform may process personal information about general contractor administrators, trade managers, workers, employees, contractors, subcontractors, site personnel, emergency contacts, and other individuals.

We take privacy seriously because SiteFolio handles workforce, certification, contact, company, and site compliance information.

1. Scope of This Policy

This Privacy Policy applies to personal information we collect through:

1. the SiteFolio website;
2. the SiteFolio web application;
3. GC Admin portals;
4. Trade Manager portals;
5. worker onboarding workflows;
6. document upload and download features;
7. certification tracking features;
8. invitations and email notifications;
9. billing, support, demo, pilot, and sales interactions;
10. cookies and analytics tools; and
11. communications with us.

This Privacy Policy does not apply to third-party websites, tools, or services that are not controlled by SiteFolio.



2. Our Role

SiteFolio may act in different privacy roles depending on the situation.

For most Customer Data uploaded to or managed in the platform, SiteFolio acts as a service provider or processor for the Customer. The Customer determines what personal information is collected, what documents are required, who is invited, what workers are added, what certifications are requested, and how compliance records are used.

For account administration, website visits, billing, marketing, support, security, analytics, and direct communications with SiteFolio, SiteFolio may act as the organization responsible for that personal information.

Customers are responsible for providing privacy notices and obtaining any required consents from their employees, workers, contractors, subcontractors, emergency contacts, and other individuals whose personal information is submitted to SiteFolio.

3. Personal Information We Collect

The personal information we collect depends on how SiteFolio is used.

3.1 Account and User Information

We may collect:

1. name;
2. email address;
3. phone number;
4. job title or role;
5. company name;
6. company address;
7. password or authentication information;
8. account type;
9. profile settings;
10. invitation status;
11. login activity;
12. user permissions;
13. support communications; and
14. administrative contact information.



3.2 Company and Site Information

We may collect:

1. general contractor name;
2. trade company name;
3. project name;
4. site name;
5. site address;
6. industry type;
7. project or site contact details;
8. trade types;
9. site-specific requirements;
10. required business document types;
11. required agreement terms; and
12. compliance deadlines.

Some site information may identify individuals if it includes names, contact details, signatures, comments, or other personal information.

3.3 Worker Information

Customers and Trade Managers may submit Worker Data, including:

1. worker name;
2. email address;
3. phone number;
4. employer or trade company;
5. trade type;
6. job role;
7. worker ID or internal reference number;
8. certifications;
9. training records;
10. certification issue dates;
11. certification expiry dates;
12. uploaded certification files;
13. orientation status;
14. acknowledgement records;
15. site assignment information;
16. compliance status;
17. document status;
18. notes or comments; and



19. emergency contact information, if provided.

3.4 Uploaded Documents

The platform may process documents uploaded by Customers or users, including:

1. worker certifications;
2. trade licenses;
3. safety training cards;
4. WHMIS, fall protection, confined space, hot work, high voltage, Red Seal, first aid, CPR, or similar certifications;
5. business licenses;
6. certificates of insurance;
7. workers compensation clearance certificates;
8. tax forms;
9. health and safety policies;
10. site safety acknowledgements;
11. contractor agreements;
12. signed documents;
13. orientation documents;
14. equipment documents;
15. photos or scans of documents; and
16. other documents required by a Customer.

Uploaded documents may contain additional personal information depending on their contents. Users should avoid uploading unnecessary personal information.

3.5 Payment and Billing Information

If we charge fees, we may collect:

1. billing contact name;
2. billing email address;
3. company billing information;
4. subscription details;
5. invoice records;
6. payment status;
7. tax information;
8. transaction history; and
9. limited payment metadata.



We use third-party payment processors where available. We do not intend to store full credit card numbers on our own systems.

3.6 Technical and Usage Information

We may collect:

1. IP address;
2. device information;
3. browser type;
4. operating system;
5. pages viewed;
6. features used;
7. login timestamps;
8. session activity;
9. approximate location derived from IP address;
10. error logs;
11. security logs;
12. audit logs;
13. file upload and download events;
14. email delivery events;
15. referral URLs; and
16. cookies or similar technologies.

3.7 Communications

We may collect information when you:

1. contact us;
 2. request a demo;
 3. request support;
 4. respond to a survey;
 5. join a pilot;
 6. provide feedback;
 7. communicate by email, phone, video call, chat, form, or other method; or
 8. interact with sales, onboarding, or customer success.
-



4. How We Collect Personal Information

We collect personal information:

1. directly from you;
 2. from Customers who create accounts or invite users;
 3. from Trade Managers who upload worker information;
 4. from workers who complete onboarding or provide information;
 5. from documents uploaded to the platform;
 6. automatically through use of the Services;
 7. from service providers;
 8. from payment processors;
 9. from email delivery providers;
 10. from support and analytics tools; and
 11. from public or business contact sources where permitted by law.
-

5. How We Use Personal Information

We use personal information to:

1. provide, operate, maintain, and improve SiteFolio;
2. create and manage accounts;
3. authenticate users;
4. manage invitations;
5. create site workspaces;
6. enable Customers to define compliance requirements;
7. enable Trade Managers to upload worker and company documents;
8. store certifications, expiry dates, signed agreements, acknowledgements, and business documents;
9. display dashboards, status indicators, missing items, expiry information, and compliance summaries;
10. enable document review, approval, rejection, download, and export;
11. send onboarding invitations, reminders, account notices, status notices, password reset emails, and service messages;
12. provide support and troubleshooting;
13. process payments and invoices;
14. secure the Services;
15. detect, prevent, and investigate fraud, abuse, unauthorized access, security incidents, or policy violations;



16. maintain audit logs and records;
 17. comply with legal, regulatory, contractual, accounting, tax, and reporting obligations;
 18. enforce our Terms and agreements;
 19. develop new features;
 20. analyze product usage and performance;
 21. communicate about demos, pilots, renewals, updates, and services;
 22. send marketing communications where permitted by law; and
 23. protect the rights, safety, property, and interests of SiteFolio, Customers, workers, users, and third parties.
-

6. Consent and Customer Responsibilities

Where required by law, we collect, use, or disclose personal information with consent or other legal authority.

Customers and Trade Managers are responsible for ensuring that they have the right to submit personal information to SiteFolio.

This includes responsibility for:

1. informing workers that their information may be submitted to SiteFolio;
2. explaining the purposes for collection, use, and disclosure;
3. obtaining consent where required;
4. complying with employment, labour, privacy, union, contractor, and site rules;
5. ensuring emergency contacts are notified where required;
6. ensuring uploaded documents are lawful and appropriate;
7. limiting uploads to information reasonably necessary for the compliance workflow; and
8. responding to worker privacy requests where the Customer controls the information.

If you provide personal information about another person, you represent that you have the legal right to do so.

7. Sensitive Information

SiteFolio is intended for workforce compliance records, not for general medical records, background checks, financial records, government identification records, or unrelated sensitive personal information.



Users should not upload social insurance numbers, banking details, passport scans, driver's licence scans, medical records, biometric information, criminal background checks, immigration records, or other highly sensitive personal information unless:

1. it is strictly necessary for a legitimate compliance purpose;
2. the Customer has legal authority to collect and use it;
3. the individual has received appropriate notice;
4. consent has been obtained where required; and
5. the upload is permitted by applicable law and contract.

If unnecessary sensitive information is uploaded, Customer remains responsible for that upload.

8. How We Share Personal Information

We may share personal information as described below.

8.1 With Customers and Authorized Users

Information submitted to a site workspace may be visible to the Customer, GC Admins, Trade Managers, project users, reviewers, or other Authorized Users according to their permissions.

For example:

1. a GC Admin may view trade company documents and worker certification status for that site;
2. a Trade Manager may view workers and documents submitted by that trade company;
3. reviewers may approve or reject business documents;
4. users may see status indicators, expiry dates, upload records, and acknowledgement records; and
5. authorized users may export available records.

8.2 With Service Providers

We may share personal information with trusted service providers who help us operate the Services, including providers for:

1. cloud hosting;
2. database services;
3. file storage;
4. authentication;



5. email delivery;
6. payment processing;
7. analytics;
8. error monitoring;
9. security;
10. customer support;
11. logging;
12. backups; and
13. professional services.

These providers may only use personal information to provide services to us, subject to contractual, legal, or technical safeguards.

8.3 With Professional Advisors

We may share information with lawyers, accountants, auditors, insurers, consultants, investors, and advisors where reasonably necessary for business, legal, compliance, insurance, financial, or corporate purposes.

8.4 For Legal and Safety Reasons

We may disclose personal information if we reasonably believe disclosure is necessary to:

1. comply with law;
2. respond to a subpoena, court order, regulator request, government request, or legal process;
3. enforce agreements;
4. investigate security incidents;
5. prevent fraud, abuse, or unlawful activity;
6. protect rights, property, safety, or security;
7. respond to emergencies; or
8. establish, exercise, or defend legal claims.

8.5 Business Transactions

If SiteFolio is involved in a merger, acquisition, financing, investment, due diligence process, restructuring, sale of assets, bankruptcy, or similar transaction, personal information may be disclosed or transferred as part of that transaction, subject to appropriate confidentiality and legal protections.



8.6 With Consent

We may share personal information with consent or at the direction of the Customer or individual.

9. International Storage and Processing

SiteFolio is based in Canada and is intended primarily for Canadian construction customers.

However, we and our service providers may store or process personal information in Canada, the United States, the European Union, or other jurisdictions depending on our hosting, storage, authentication, email, payment, support, and security providers.

Personal information stored or processed outside your province or country may be subject to the laws of that jurisdiction, including lawful access by courts, law enforcement, regulators, and government authorities.

By using SiteFolio or submitting information to the Services, you acknowledge that personal information may be transferred, stored, or processed outside your province or country.

10. Security Safeguards

We use reasonable administrative, technical, and physical safeguards designed to protect personal information against loss, theft, misuse, unauthorized access, disclosure, copying, alteration, and destruction.

Safeguards may include:

1. encrypted connections;
2. access controls;
3. authentication;
4. role-based permissions;
5. tenant isolation;
6. database security rules;
7. secure file storage;
8. signed file links;
9. logging and monitoring;
10. data validation;



11. password controls;
12. restricted internal access;
13. service provider review;
14. backups;
15. security updates; and
16. incident response procedures.

No method of transmission or storage is completely secure. We cannot guarantee absolute security.

Customers and users are responsible for maintaining the security of their own accounts, passwords, devices, networks, user permissions, exported files, and downloaded documents.

11. Data Retention

We retain personal information for as long as reasonably necessary to provide the Services, maintain records, comply with legal obligations, resolve disputes, enforce agreements, maintain security, support audits, and fulfill the purposes described in this Privacy Policy.

Unless otherwise agreed in writing or required by law, we may retain worker-related Customer Data for one year from the worker's last site activity or for the retention period configured by the Customer, whichever applies.

"Site activity" may include being added to a site, assigned to a site, included in a compliance record, having a certification uploaded or updated, completing onboarding, being included in a daily log, or being otherwise associated with an active site workspace.

We may retain certain records longer where necessary, including:

1. invoices and payment records;
2. legal records;
3. security logs;
4. audit logs;
5. dispute records;
6. backup copies;
7. de-identified or aggregated data;
8. records required by law; and
9. records needed to protect rights, safety, or security.



After deletion from active systems, information may remain in backups for a limited period until overwritten through normal backup cycles.

12. Access, Correction, and Deletion

Individuals may request access to or correction of their personal information.

Because most worker and compliance data is controlled by our Customers, workers and trade personnel should generally contact their employer, trade company, general contractor, or the Customer responsible for the site workspace first.

You may also contact us at privacysitefolioteam@gmail.com.ca. We may need to verify your identity and may redirect the request to the applicable Customer where the Customer controls the information.

Subject to applicable law, we may decline or limit a request where:

1. we cannot verify identity;
 2. the request is excessive, abusive, or unlawful;
 3. disclosure would reveal another person's information;
 4. disclosure would reveal confidential business information;
 5. the information is subject to legal privilege;
 6. the information must be retained for legal, security, audit, contractual, or dispute purposes; or
 7. the Customer instructs us not to delete information that it is legally entitled or required to retain.
-

13. Accuracy

We rely on Customers, Trade Managers, users, and workers to provide accurate and current information.

Customers are responsible for keeping worker information, certification records, expiry dates, business documents, site requirements, and account information accurate and up to date.

If you believe information about you is inaccurate, contact the Customer responsible for the record or contact us at sitefolioteam@gmail.com



14. Cookies and Analytics

We may use cookies, local storage, pixels, and similar technologies to:

1. keep users signed in;
2. remember preferences;
3. secure accounts;
4. understand product usage;
5. measure website performance;
6. improve the Services;
7. detect abuse;
8. troubleshoot errors; and
9. support marketing and analytics.

You can control cookies through your browser settings. Some features may not work properly if cookies are disabled.

15. Email and Electronic Communications

We may send transactional and service-related emails, including invitations, account notices, password resets, onboarding instructions, compliance workflow notices, document update notices, expiry reminders, billing notices, and security notices.

These messages are part of the Services and may be necessary for account administration or compliance workflows.

We may also send marketing or promotional messages where permitted by law. Marketing messages will identify SiteFolio and include an unsubscribe mechanism where required.

Even if you unsubscribe from marketing communications, we may still send transactional, legal, security, billing, and service-related messages.

16. Worker and Emergency Contact Information



If emergency contact information is submitted to SiteFolio, the Customer or user submitting it is responsible for ensuring that the emergency contact has been notified where required and that the information is reasonably necessary for a legitimate site, safety, employment, or compliance purpose.

Emergency contact information should only be used for appropriate emergency, safety, site, employment, or compliance purposes.

Customers should not upload unnecessary personal details about emergency contacts.

17. Children and Minors

SiteFolio is intended for business and construction workforce use. It is not intended for children.

Users must not submit information about individuals under the age of 16 unless legally authorized and necessary for a legitimate employment, apprenticeship, training, site access, or compliance purpose.

18. Privacy Breaches

If we become aware of a privacy breach involving personal information under our control, we will assess the breach and take reasonable steps to contain, investigate, and remediate it.

Where required by law, we will notify affected individuals, Customers, regulators, or other parties.

If a Customer becomes aware of an actual or suspected breach involving SiteFolio accounts, Customer Data, downloaded files, user credentials, or exported records, the Customer must notify us promptly at sitefolioteam@gmail.com.

19. Service Providers and Subprocessors

We may use third-party service providers to support the Services. These may include cloud infrastructure, database, storage, authentication, email, payment, analytics, support, security, and monitoring providers.



Our service providers may change from time to time. We will use reasonable measures to ensure service providers protect personal information in a manner consistent with this Privacy Policy and applicable law.

Customers may request information about current material service providers by contacting sitefolioteam@gmail.com

20. De-Identified and Aggregated Information

We may use information that has been aggregated, anonymized, or de-identified so that it does not reasonably identify an individual.

We may use this information to:

1. improve the Services;
2. understand industry trends;
3. develop product features;
4. measure usage;
5. create benchmarks;
6. secure the Services;
7. support business planning; and
8. produce analytics or reports.

We will not attempt to re-identify de-identified information except where permitted by law, such as for security testing or legal compliance.

21. Links to Third-Party Sites

The Services may contain links to third-party websites, documents, tools, or services. We are not responsible for the privacy practices, security, content, or policies of third parties.

You should review third-party privacy policies before using third-party services.



22. Changes to This Privacy Policy

We may update this Privacy Policy from time to time.

If changes are material, we will provide notice by email, in-app message, website notice, or other reasonable means.

The updated Privacy Policy will be effective on the date stated at the top of the policy. Continued use of the Services after the updated Privacy Policy becomes effective means you acknowledge the updated policy.

23. Challenging Compliance and Questions

If you have questions, concerns, requests, or complaints about privacy, contact:

SiteFolio Technologies

Email: sitefolioteam@gmail.com

We will respond within a reasonable time and in accordance with applicable law.

If you are not satisfied with our response, you may contact the Office of the Privacy Commissioner of Canada or the applicable provincial privacy regulator.

24. Contact Information

SiteFolio Technologies

Email: sitefolioteam@gmail.com