

BubbleCharge Host Privacy Standards

Effective Date: September 1, 2026

Introduction

Trust is fundamental to the BubbleCharge community. Finders trust Hosts with access to personal information needed to coordinate charging sessions, while Hosts trust Finders to use charging locations responsibly.

As a Host on BubbleCharge, you may receive personal information about Finders before, during, and after a reservation. This information is provided solely for the purpose of facilitating EV charging services through the BubbleCharge platform.

These Host Privacy Standards explain how Hosts must collect, use, store, share, and protect Finder information when using BubbleCharge in Canada and the United States.

Failure to comply with these standards may result in warnings, temporary restrictions, suspension, removal of listings, or permanent account termination.

1. Information Available to Hosts

To facilitate charging reservations, BubbleCharge may provide Hosts with certain information about a Finder.

Depending on the booking and verification requirements, this information may include:

Full name

Phone number

Vehicle make and model

Charging requirements

Reservation details

Identity verification status

Certain information may only become available after a reservation is confirmed.

BubbleCharge may limit the information shared with Hosts to protect user privacy and platform security. Similar platforms provide Hosts only the information necessary to manage reservations and deliver services.

2. Permitted Use of Finder Information

Hosts may use Finder information only when reasonably necessary to:

Manage reservations

Coordinate charging sessions

Communicate regarding bookings

Verify arrival or check-in

Resolve operational issues

Comply with legal obligations

Provide charging-related services

Hosts must not use Finder information for unrelated purposes.

Examples of prohibited uses include:

Marketing products or services

Sending unsolicited promotional messages

Creating mailing lists

Selling personal information

Building external customer databases

Contacting Finders after a booking for non-booking purposes

Sharing Finder information with unauthorized third parties

Finder information belongs to the Finder and must be treated as confidential.

3. Data Minimization

Hosts should collect only the information necessary to provide charging services.

Hosts must not request unnecessary information, including:

Social insurance numbers

Social Security numbers

Banking credentials

Credit card details

Passwords

Financial account login information

Sensitive personal information unrelated to charging services

If BubbleCharge already provides necessary information through the platform, Hosts should avoid collecting duplicate information.

4. Communication Standards

Hosts should not pressure Finders to move communications to third-party services unless reasonably necessary for coordinating a charging session.

Hosts may not require Finders to create accounts on external websites or applications as a condition of receiving charging services. Similar restrictions are used by major marketplace platforms to protect users and maintain privacy safeguards.

5. Sharing Finder Information

Hosts must not disclose Finder information to anyone except when reasonably necessary to provide charging services or comply with applicable law.

Permitted disclosures may include:

Property managers assisting with charging access

Household members directly involved in hosting

Service providers assisting with access management

Legal authorities when required by law

Emergency responders during emergencies

Hosts remain responsible for ensuring any authorized recipient protects Finder information appropriately.

Unauthorized disclosure is prohibited.

Examples include:

Posting Finder information online

Sharing Finder details on social media

Providing Finder contact information to marketers

Disclosing reservation details to unrelated individuals

6. Security Requirements

Hosts must take reasonable steps to protect Finder information from unauthorized access, use, disclosure, alteration, or loss.

Reasonable security measures include:

Using secure passwords

Protecting mobile devices

Locking computers when unattended

Avoiding public disclosure of booking information

Deleting information no longer required

Restricting access to authorized individuals only

Hosts should not store Finder information longer than necessary to manage reservations, satisfy legal obligations, or resolve disputes. Privacy-focused platforms generally require hosts to retain data only for legitimate business and legal purposes.

7. Recording Devices and Monitoring

Transparency is required whenever monitoring devices are present near a charging location.

Hosts must clearly disclose any:

Exterior security cameras

Video doorbells

License plate recognition systems

Audio recording devices permitted by law

Other monitoring technologies that may capture Finder activity

Hidden recording devices are strictly prohibited.

Hosts must not place recording devices in locations where individuals have a reasonable expectation of privacy.

Where required by law, Hosts must obtain consent before collecting audio recordings.

8. Identity Verification Information

BubbleCharge may require identity verification for safety, fraud prevention, payment processing, regulatory compliance, or trust and safety purposes.

If a Host receives identity-related information:

The information may only be used for verification purposes.

Copies should not be retained longer than necessary.

Information must not be shared with unauthorized parties.

Information may not be used for marketing or profiling.

Hosts must comply with applicable privacy laws when handling identity documents or verification information.

9. Canada-Specific Privacy Obligations

Hosts operating in Canada are responsible for complying with applicable privacy laws, including laws that may apply within their province or territory.

Where applicable, Hosts should:

Use personal information only for identified purposes.

Limit collection to what is necessary.

Protect information using appropriate safeguards.

Dispose of information securely when no longer needed.

Respond appropriately to privacy concerns or requests.

BubbleCharge expects all Canadian Hosts to respect recognized privacy principles concerning transparency, accountability, security, and responsible information handling.

10. United States Privacy Obligations

Hosts operating in the United States are responsible for complying with all applicable federal, state, and local privacy laws.

Depending on the Host's location, additional obligations may apply regarding:

Data disclosures

Consumer rights

Information retention

Security requirements

Data breach notifications

Hosts are responsible for understanding any privacy obligations that apply to their activities.

11. Data Breaches and Security Incidents

If a Host becomes aware of unauthorized access, disclosure, theft, loss, or misuse of Finder information, the Host must promptly:

Secure affected systems or records.

Limit further exposure where possible.

Notify BubbleCharge through designated reporting channels.

Cooperate with any investigation.

Comply with applicable legal reporting requirements.

BubbleCharge may take temporary action to protect users while an incident is investigated.

12. Respecting Finder Privacy at Charging Locations

Hosts should respect the personal privacy of Finders while they access charging services.

Hosts should not:

- Monitor Finders unnecessarily

- Record conversations without authorization

- Enter a Finder's vehicle without permission

- Photograph Finders without consent

- Collect personal information beyond what is necessary

Finders should be able to access charging services without unreasonable intrusion into their privacy.

13. Enforcement

BubbleCharge may investigate alleged violations of these Host Privacy Standards.

Depending on severity, enforcement actions may include:

- Educational notices

- Warnings

- Temporary restrictions

- Listing suspension

- Payout holds

- Account suspension

- Permanent removal from the platform

BubbleCharge reserves the right to cooperate with legal authorities where required by law.

14. Changes to These Standards

BubbleCharge may update these Host Privacy Standards periodically to reflect operational, legal, regulatory, or security developments.

Updated versions will be posted on the BubbleCharge platform and become effective upon publication unless otherwise stated.

15. Contact

Questions regarding these Host Privacy Standards may be directed to:

support@bubblecharge.com

BubbleCharge Inc.

Canada

Protecting privacy is a shared responsibility. Hosts who respect Finder privacy help maintain a trusted, secure, and reliable charging community for everyone.