

Privacy Policy

Welcome to the InstaVolt Limited's privacy policy.

InstaVolt respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from) or use our app and tell you about your privacy rights and how the law protects you.

Purpose of this privacy policy

This privacy policy aims to give you information on how InstaVolt collects and processes your personal data through your use of our website <https://www.instavolt.co.uk> and our app, including any data you may provide through your use of the website or app.

It is important that you read this privacy policy together with any other privacy policy or fair processing policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy policy supplements other notices and privacy policies and is not intended to override them. As our services are provided for drivers this policy is intended for persons of legal driving age. We do not knowingly collect data about children.

Controller

InstaVolt Limited is the controller and responsible for your personal data (collectively referred to as "InstaVolt", "we", "us" or "our" in this privacy policy).

Data Protection Principles

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Contact details

If you have any questions about this privacy policy or our privacy practices, please contact us in the following ways:

Email address: privacy@instavolt.co.uk

Telephone number: 01256 305900

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Changes to the privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review. This version was last updated on 9th August 2024.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

Third-party links

The website and app may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website or app, we encourage you to read the privacy policy of every website you visit.

1. The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

Identity Data : first name, last name, username or similar identifier, marital status, title, date of birth.

Contact Data : billing address, home address, email address and telephone numbers.

Financial Data : bank account and payment card details.

Third Party Information (If you register or log into our services via a third party such as Google, Facebook, Instagram, Twitter or Apple) : your user ID on the relevant platform, your name and your email address.

Transaction Data includes details about payments to and from you and other details of products and services you have purchased from us.

Technical Data i.e. data we get from your use of our services, includes internet protocol (IP) address, your login data, browser type and version, time zone setting, location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.

Profile Data includes your username and password, purchases made by you, your preferences, feedback and survey responses.

Usage Data includes information about how you use our website and services.

Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

We do not collect any **Special Categories of Personal Data** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with driver portal services when you sign up for an account with us). In this case, we may be unable to provide the services, or have to cancel a service you have with us. But we will notify you if this is the case at the time.

2. How is your personal data collected?

We use different methods to collect data from and about you including through:

Direct interactions. You may give us your Identity, Contact and Financial Data by filling in online forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- download our app from the Apple App Store or Google Play;
- log in to or create an account, either standalone (with email and password) or by federation with Facebook, Google or Apple platforms;
- subscribe to any other service or publication we offer;
- request marketing to be sent to you;
- enter a competition, promotion or survey; or
- give us feedback or contact us.

Automated technologies or interactions. As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our cookie policy for further details.

Third parties or publicly available sources. We will receive personal data about you from various third parties and public sources as set out below:

- Technical Data from analytics and search information providers
- Contact, Financial and Transaction Data from providers of technical and payment services
- Identity and Contact Data from data brokers or aggregators
- Identity and Contact Data from publicly available sources such as the DVLA.

3. How we use your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data although we will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Here is a glossary of some of the legal terms we use in relation to the purposes for which we use your personal data:

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best services/products and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against

any potential impact on you in respect of specific activities by contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as an account holder	(a) Identity (b) Contact	Performance of a contract with you
To allow you to register or log in to your account via a third party such as Facebook.	(a) Third Party Information	Necessary for the performance of a contract with you when you choose to register or log in via a third party such as Facebook.
To process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To enable you to partake in a prize draw, competition or complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation

To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Identity (b) Contact (c) Technical Usage (d) Profile (e) Marketing and Communications	Necessary for our legitimate interests (to develop our products/services and grow our business) Consent (when you opt into our marketing pop up on our app, once you have consented the option to opt out is included in every marketing email you receive)

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you.

You will receive marketing communications from us if you have requested information from us or obtained services from us and you have not opted out of receiving that marketing.

Third-party marketing

We will get your express opt-in consent before we share your personal data with any third party for marketing purposes.

Opting out

You can ask us or third parties to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by contacting us at any time on info@instavolt.co.uk.

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please see our Cookie Policy at <https://instavolt.co.uk/cookie-policy/>

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose,

please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

4. Disclosures of your personal data

We may share your personal data with the parties set out below for the purposes set out in the table above.

- Service Providers that we use to help with certain aspects of our operations, for example for website hosting or payment services.
- Other members (current and future) of the same group of companies (which means a parent company, a subsidiary, joint venture or other company that controls or is controlled by or is under common control with InstaVolt).
- Partners, being third parties such as advertisers, associates and other potential business partners.
- Professional advisers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities based in the United Kingdom.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

5. International transfers

Where we share your personal data within the InstaVolt group of companies this will not involve transferring your data outside the European Economic Area (**EEA**).

However, some of our external third parties are based outside the EEA so their processing of your personal data will involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

6. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

7. Data retention

How long will you use my personal data for?

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

By law we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax purposes.

In some circumstances you can ask us to delete your data: see "*your legal rights*" below for further information.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

8. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. You may ask us to delete or remove personal data. You have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. If you request erasure of your personal data you will not be able to receive the services.

Note: in respect of our platform users who are InstaVolt mobile app account holders or InstaVolt webpage account holders:

- If you make a request for us to delete or remove your personal data, this will result in your account being terminated and permanently erased;
- If you delete your account*, this will automatically result in your personal data being deleted and removed by us, with all other data relating to your account being automatically anonymized.

*A mobile app account may be deleted by going to Settings within the account and clicking on Delete Account, and a webpage account may be deleted by going to My Profile within the account and clicking on Delete Account.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to

object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- If you want us to establish the data's accuracy.
- Where our use of the data is unlawful but you do not want us to erase it.
- Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.
- You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact us.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

To make any of the above requests

Email us: privacy@instavolt.co.uk Or

call us: 01256 305900

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

9. Privacy information for Job Applicants

All processing of job applications shall be in line with the aforementioned data privacy principles. All job applicants also have the rights of access, erasure, correction, objection, and restriction listed above.

Processing

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you:

- The information you have provided to us in your curriculum vitae
- The information you have provided on our application form, including name, title, address, telephone number, personal email address, date of birth, gender, employment history, qualifications,
- Any information you provide to us during an interview

How we will use information about you

We will use the personal information we collect about you to:

- Assess your skills, qualifications, and suitability for the role
- Carry out background and reference checks, where applicable
- Communicate with you about the recruitment process
- Keep records related to our hiring processes
- Comply with legal or regulatory requirements

Lawful Basis for Processing Applicant Data

It is in our legitimate interests to decide whether to appoint you to role since it would be beneficial to our business to appoint someone suitable to that role (UK GDPR Article 6(f))

We also need to process your personal information to decide whether to enter into a contract of employment with you (UK GDPR Article 6(b)).

Having received your CV and covering letter, we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the role.

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully.

Data security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will retain your personal information for a period of one month after we have communicated to you our decision about whether to appoint you to the role. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with applicable laws and regulations.

If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

10. CCTV

We use CCTV cameras to view and record individuals on and around our premises in order to maintain a safe environment for visitors. However, we recognise that the images of individuals recorded by CCTV cameras are personal data which must be processed in accordance with data protection legislation. As a controller, we have registered our use of CCTV with the Information Commissioner's Office (ICO) and seek to comply with its best practice suggestions.

Reasons for the use of CCTV

We currently use CCTV as outlined below. We believe that such use is necessary for legitimate business purposes, including:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime and
- for the personal safety of visitors and other members of the public and to act as a deterrent against crime.

This list is not exhaustive and other purposes may be or become relevant.

Monitoring

CCTV monitors the InstaVolt sites and the areas surrounding electric vehicle charge points 24 hours a day and this data is continuously recorded.

Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property. Images are monitored by authorised personnel during operating hours only.

How we will operate any CCTV

Where CCTV cameras are placed, we will ensure that signs are displayed at the surveillance zone to alert individuals that their image may be recorded. The signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored. Live feeds from CCTV cameras will only be monitored where this is reasonably necessary. We will ensure that live feeds from cameras and recorded images are only viewed by approved persons whose role requires them to have access to such data.

Use of data gathered by CCTV

In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security.

We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

Retention and erasure of data gathered by CCTV

Data recorded by the CCTV system will be stored. Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. In all other cases, recorded images will be kept for no longer than 30 days

At the end of their useful life, all images stored in whatever format will be erased permanently and securely

Requests for disclosure

We may share data with other group companies and other associated companies or organisations, for example shared services partners where we consider that this is reasonably necessary for any legitimate purposes. In appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime. No images from CCTV will ever be posted online or disclosed to the media.

Subject access requests

Data subjects may make a request for disclosure of their personal information and this may include CCTV images. In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual. We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.