HIBITS

HIGHWAY BUSINESS SERVICES

Privacy Policy

Website · Clients · Managed IT · Cybersecurity · Calls · AI & Automation

Effective 28 October 2026 | Version 2.0 | Public privacy notice

We are committed to protecting personal information and being transparent about how we use it. This policy covers our website, customer communications and the technology services we supply to businesses and individuals.

Key practices All configured inbound and outbound business calls are recorded with notification and ordinarily retained for 12 months. Remote access is authorised. Support information retained only for technical learning is anonymised. Customer information used with AI remains subject to protective controls.

Contents

Sections 1–13

1. Who we are and how to contact us
2. When we are a controller and when we are a processor
3. Who this policy applies to
4. Categories of personal information
5. How we obtain information
6. Why we use information and our lawful bases
7. Our website, forms and enquiries
8. Cookies and similar technologies
9. Telephone call recording, notification and AI transcription
10. Remote support, access logs and managed monitoring
11. Cybersecurity, networks and connectivity
12. Cloud, email, hosting, domains and backups
13. Hosted telephony, messaging and collaboration

Sections 14–26

14. Artificial intelligence, automation and customer-data protection
15. Hardware sales, repairs, refurbishment and disposal
16. Billing, direct debits and finance
17. Marketing, newsletter and business prospecting
18. Who we share information with
19. International transfers
20. How we secure information
21. How long we retain information
22. Security incidents and personal data breaches
23. Your data protection rights
24. How to complain
25. Children, healthcare, education and sensitive records
26. Changes to this policy

Highway Business Services | hello@hibits.co.uk | 01227 640547

Highway Business Services is committed to protecting personal information and handling it lawfully, fairly, transparently and securely. This policy explains how we use information through **https://hibits.co.uk**, in our customer relationships and while delivering IT, communications, cybersecurity, cloud, automation and AI services.

At a glance: We record inbound and outbound business calls, notify participants that recording takes place, and ordinarily retain recordings for **12 months**. We use authorised remote access to support customer systems and inspect personal files or communications only where necessary and permitted. We retain technical learning from resolved support matters in **anonymised form** when identifiable information is no longer required. We protect customer information handled through AI services and do not authorise its use to train public AI models without a separate lawful and expressly authorised arrangement.

1. Who we are and how to contact us

Highway Business Services is the trading name of **Hibits Ltd**, company number **11430444**, registered in England and Wales.

- **Registered office:** Marlowe Innovation Centre, Marlowe Way, Newington, Kent, CT12 6FA.
- **Trading/contact address:** 54 The Strand, Deal, Kent, CT14 7DP.
- **Email:** hello@hibits.co.uk.
- **Telephone:** 01227 640547.
- **Website:** https://hibits.co.uk.

For personal information enquiries, rights requests or complaints, email **hello@hibits.co.uk** with the subject **Data Protection Enquiry** or write to the registered office.

We comply, where applicable, with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (as amended), the Data (Use and Access) Act 2025, the Privacy and Electronic Communications Regulations 2003 (PECR), and relevant information-security and communications rules.

This is our public privacy notice. Separate service terms, data processing agreements, cookie information and workforce privacy notices may apply to particular activities.

2. When we are a controller and when we are a processor

We are a controller when we decide why and how to use personal information for our own operations. Examples include website enquiries, sales and marketing, customer accounts, invoicing, our own call recordings and transcripts, security, complaints, supplier management and business administration.

We are commonly a processor when we access, host, back up, secure, migrate or support information on behalf of a business, school, charity, healthcare provider or other customer. The customer will normally control its employees', pupils', patients', service users' and other contacts' information and give us documented instructions on how to process it.

Our roles can differ for the same service. For example, we may be a processor for the contents of a customer's email system, but a controller for our own invoice and contact records. Our legal role depends on the facts, not merely a contractual label.

Where required, customer-controlled processing is governed by written terms consistent with Article 28 UK GDPR, including confidentiality, security, authorised subprocessors, assistance with rights and incidents, and return or deletion when the service ends.

3. Who this policy applies to

This policy covers visitors to our website; private and residential customers; existing, former and prospective business customers; authorised customer contacts; employees and representatives of customer organisations; callers; support users; suppliers; prospective suppliers; newsletter subscribers; marketing prospects; training or event attendees; and others communicating with us.

When customers engage us to support their systems, we may also encounter personal information relating to their employees, clients, pupils, patients, service users, volunteers and other contacts. For those individuals, the customer's own privacy notice will usually be the primary explanation of how their information is used.

Our general website and commercial marketing are not directed at children. Separate employment or recruitment notices may be used for our personnel and applicants.

4. Categories of personal information

Depending on the interaction and service, we may handle:

- **Identity and contact details:** names, job titles, organisations, business or home addresses, email addresses, telephone numbers, authorised contacts and communication preferences.
- **Commercial and financial details:** quotations, orders, contracts, licence allocations, customer identifiers, service plans, invoices, direct debit/payment references, transaction status and correspondence.
- **Website information:** contact or quote form entries, newsletter preferences, IP address, browser/device information, pages visited, referral information, security logs and cookie choices.
- **Device and network details:** hardware identifiers, serial numbers, installed applications, operating systems, IP addresses, network configuration, user account names, patch status, security alerts, performance and diagnostic data.
- **Support material:** ticket descriptions, notes, timestamps, screenshots, log extracts, approved remote-session records, files or email content viewed with authorisation, and relevant attachments.
- **Communications:** emails, telephone numbers, call recordings, voicemail, audio transcripts, AI-generated summaries where enabled, SMS, WhatsApp and other messages, plus video-meeting content where recorded with notice.
- **Security information:** authentication events, access logs, threat indicators, malware findings, firewall and email-security events, incident evidence and vulnerability information.
- **Equipment and disposal information:** device ownership, collection and delivery details, warranty/service history, and data on devices being repaired, migrated or securely disposed of.

As a technology provider, we may encounter confidential or special category information (such as health, safeguarding or educational records) within customer systems. We do not generally seek that information through ordinary website forms. Any such access is restricted to the authorised purpose; if we act as controller, we identify the necessary lawful basis and additional statutory condition.

5. How we obtain information

We collect information directly when you contact us by form, telephone, email, social media, video call or messaging service; request a quote; purchase a service; attend a meeting; or use technical support.

We also receive information from customer administrators and authorised users, monitoring and security platforms, telephone and cloud services, payment and technology partners, referrals, and lawful professional/business directories or prospecting providers.

We may process technical information automatically when a device is enrolled in an agreed managed service. Information available publicly does not automatically give us permission to use it for marketing; the applicable UK GDPR and PECR rules still apply.

6. Why we use information and our lawful bases

Our lawful basis depends on the activity and the person's relationship with us. We may rely on **contract** (including pre-contract steps requested by an individual), **legal obligation**, **legitimate interests**, **consent**, and where genuinely applicable another statutory lawful basis. For processing on a customer's behalf, the customer normally determines the lawful basis for its own purposes.

Activity	Typical lawful basis when we are controller
Answering enquiries, quotations and service requests	Contract/pre-contract steps where applicable, or legitimate interests
Managing customer relationships, contracts and support	Contract for individuals, or legitimate interests for business contacts
Billing, accounting, tax and statutory records	Contract and/or legal obligation
IT maintenance, security, abuse prevention and incident handling	Legitimate interests; legal obligation or another basis where applicable
Recording our business telephone calls for quality, training, instructions and disputes	Legitimate interests, subject to necessity and balancing checks
Sending optional promotional communications	Consent or legitimate interests where lawful, subject to PECR
Using optional cookies and tracking technologies	Consent where required; relevant lawful exception where available
Handling access requests, privacy complaints and regulatory obligations	Legal obligation
Preventing or resolving fraud, claims, litigation and disputes	Legitimate interests and/or legal obligation

Our legitimate interests include operating and improving a reliable technology business, supporting customers, preventing fraud and misuse, protecting information and systems, and maintaining appropriate business records. We consider whether these uses are necessary, proportionate and consistent with individuals' rights and reasonable expectations.

We do not rely on consent where a different lawful basis is more appropriate merely because someone continues to use a service.

7. Our website, forms and enquiries

Our website describes managed IT, cybersecurity, cloud, connectivity, hosted phone systems, AI, automation, consultancy, training and other services. It provides contact and quotation routes and, on some pages, newsletter subscription facilities. We use information submitted through those features to provide the requested response, arrange discussions, prepare proposals and administer any resulting services.

Website hosting, form delivery, spam prevention, email marketing and booking facilities may involve specialist suppliers. When a feature involves a separate provider, their role and privacy information may also apply. We seek to limit form collection to information reasonably needed for the stated purpose.

Please do not send passwords, payment card security codes, medical records or other unnecessary sensitive information through ordinary web forms or unsecured messages. We may ask you to use a more secure channel for sensitive support matters.

8. Cookies and similar technologies

Our website may use cookies, scripts, tracking pixels, web storage and similar technologies for security, functionality, remembering preferences, analytics and—where enabled—marketing measurement.

We provide cookie and consent controls through our website where relevant. We request consent before using technologies that require consent under PECR. Certain strictly necessary and other narrowly defined technologies may be permitted without consent when all statutory conditions are satisfied; some exceptions require clear information and a simple way to object.

Marketing tracking and cross-site advertising are not automatically exempt from consent. We do not claim that every analytics, advertising or other tracking tool is active on every page. Actual technologies, providers,

purposes and durations may change as the website evolves and should be shown in the website's current cookie settings or declaration.

You can revisit the website's consent controls to change your preferences where offered, and can also manage cookies in your browser. Some functionality may be affected if necessary cookies are blocked.

9. Telephone call recording, notification and AI transcription

We record inbound and outbound business telephone calls made or received through our configured business phone systems. Call participants are notified that recording takes place, including through an appropriate call-opening announcement or verbal notice. This policy provides further information about the purposes and handling of those recordings.

We use recordings to monitor and improve service quality; train and coach staff; check technical instructions and customer authorisations; confirm transactions and agreed actions; investigate complaints; resolve disputes; prevent fraud; and protect our customers, personnel and business. Our usual lawful basis is legitimate interests, supported by appropriate necessity and proportionality assessments.

Recordings may include a person's voice, name, telephone number, conversation content, call date, time and duration. Our authorised team and relevant providers may access recordings only as needed for the stated purposes. We do not routinely publish or disclose recordings.

Routine call recordings are retained for 12 months and then deleted in accordance with the recording platform's retention settings. A particular recording may be held for longer where reasonably necessary for a documented legal claim, complaint, investigation or statutory obligation. Backups and deletion cycles may affect the precise technical removal date.

Where AI transcription or summarisation is enabled, call audio may be processed to create a transcript, summary, action points or a support ticket. Those derived records are subject to appropriate access controls, security safeguards and the retention rules for their purpose; an identifiable transcript saved in a support ticket is treated as personal information rather than automatically kept forever.

Please avoid disclosing unnecessary special category information or payment card security codes during calls. If you would prefer to communicate in writing, contact us at **hello@hibits.co.uk**; we will consider an appropriate alternative where practicable.

Individuals may ask for access to personal information in recordings, subject to identity checks, third-party rights and applicable exemptions. We may provide an appropriate recording extract, redacted recording or transcript.

If we supply a customer with a telephone system that supports recording, AI transcription or call analytics, the customer is normally responsible for its own staff/caller notices, lawful basis, configuration and retention arrangements.

10. Remote support, access logs and managed monitoring

We provide remote monitoring, management and support for customer devices and systems, including unattended access where this forms part of an agreed support arrangement. Monitoring can collect device health, software inventories, patch status, login and system event information, alerts and technical diagnostics.

We log relevant remote access and connection activity for accountability and security. **We do not routinely make video recordings of remote desktop support sessions.** A session or the inspection of particular files, emails or other content is carried out only where authorised and reasonably necessary to fix a fault or perform an agreed task. Where maintenance requires standing authorisation, this is governed by the customer's service agreement and access controls.

Customers may require additional permissions or controls for particularly sensitive systems. Our ability to access a device does not constitute unrestricted permission to inspect unrelated personal information.

11. Cybersecurity, networks and connectivity

To deliver security and networking services, we may handle firewall events, endpoint alerts, logins, email-security findings, network and DNS metadata, wireless access logs, vulnerability information, suspected malware and security incident evidence.

This helps us detect threats, protect systems, diagnose failures, respond to incidents and produce contracted security reports. A specific investigation may require limited inspection of affected files, accounts or messages and disclosure to authorised vendors, specialists, insurers or authorities where legally justified.

We may supply or help administer public/guest Wi-Fi. Where a separate venue or organisation controls the Wi-Fi service, it may have its own notices and controller responsibilities for visitor data, registration or access logs.

12. Cloud, email, hosting, domains and backups

Our services may include Microsoft 365 and other cloud platforms, website and domain management, hosted services, business email, identity administration, virtual machines, storage, security filtering, email archiving, backup, recovery and disaster recovery.

These services may require authorised administrative access to customers' files, mailboxes, databases, user accounts and system configurations. Where we act as processor, this is governed by customer instructions and the relevant service terms.

Backup retention periods are determined by the relevant customer's service plan and system settings. Backups can contain earlier copies of data that have subsequently changed or been deleted from live systems. Restoration, rotation and deletion follow agreed retention, security and technical requirements, including limitations associated with immutable backups.

We do not guarantee that every product is hosted in the UK. Where geographical storage or support restrictions are important, they must be agreed for the particular service.

13. Hosted telephony, messaging and collaboration

Our VoIP and communications services may involve extensions, phone numbers, caller identification, call metadata, routing information, recordings, voicemail, messages, transcripts and service logs. Advanced phone features may use automated or AI-enabled transcription, routing, summaries and analytics.

We may communicate through SMS, WhatsApp Business, Teams, email, video meeting platforms and other business tools. If a conversation is used to open or progress a support ticket, relevant content may be retained in the service history, subject to our retention and anonymisation practices.

Third-party carriers, messaging services and communications platforms may have their own roles and notices. Customers using their own recording or messaging functions remain responsible for meeting applicable transparency, marketing and employment-monitoring obligations.

14. Artificial intelligence, automation and customer-data protection

We use and build AI and automation services for tasks such as triaging enquiries and support tickets, generating draft communications, analysing documents, transcribing calls, processing authorised business workflows, integrating applications, preparing reports, supporting software development and powering business agents. We may use different AI models, hosting environments, API services, enterprise products and automation platforms depending on the project.

Customer information remains protected when we use AI. We apply our confidentiality, security, access-control, contractual and data-protection obligations to personal and commercially confidential information used in AI-assisted work, just as we do to other customer information. These protections include, where

appropriate, limiting data shared with a provider, restricting access, using approved business or enterprise accounts, applying available retention controls, recording permitted uses and checking transfer arrangements.

We do not authorise identifiable customer data or confidential customer materials to be used to train public or general-purpose AI models without separate, specific authorisation and a valid lawful basis. Where an AI provider's standard consumer product permits reuse of prompts or files for model training, we do not treat that product as an approved destination for identifiable confidential customer data merely because it is publicly accessible. We instead use an appropriately configured protected service, minimise or genuinely anonymise the input, or avoid that processing.

Where customer information is passed to an AI provider to perform an authorised task, that provider may process it under relevant contractual arrangements. We assess the provider's intended use, retention, access, location and security where relevant. A supplier's independent privacy notice may also apply depending on its role. We do not suggest that every AI vendor or model offers identical security, hosting or training terms.

AI-generated material may be inaccurate. Human review and safeguards are applied proportionately, especially to sensitive or consequential tasks. Where an automation project could make a solely automated decision with legal or similarly significant effects, the relevant controller must assess the UK GDPR rules and provide required protections.

No technology can be guaranteed entirely risk-free; our commitment is to apply appropriate, assessed safeguards and prevent unauthorised use or disclosure rather than make an absolute security guarantee.

15. Hardware sales, repairs, refurbishment and disposal

When supplying, configuring, repairing, collecting, migrating or disposing of computers and other equipment, we may process names, addresses, telephone numbers, device identifiers, service histories, warranty details and information stored on a device.

Our technicians access files or accounts only when relevant to the authorised task. Customers should keep suitable backups where practicable and remove unnecessary information before repair or transfer. Where approved repair, shipping, manufacturer or recycling partners are involved, we limit disclosures and apply relevant safeguards.

Data wiping, physical destruction or disposal certification is provided according to the agreed service specification; not every collection or repair automatically includes certified destruction of data.

16. Billing, direct debits and finance

We process billing contacts, payment references, invoices, purchase orders, bank or direct debit information, payment status and related correspondence for accounting and customer administration.

We may use **GoCardless**, banks, distributors or other payment service providers. A provider may process payment information as an independent controller or processor according to the service involved and may provide its own privacy notice. We do not request customers to submit card verification/security codes through ordinary technical support channels.

Financial records may need to be retained to meet legal, tax and audit obligations or to establish and defend claims.

17. Marketing, newsletter and business prospecting

We may send newsletters, guidance, product information and offers to existing customers or prospective customers, and conduct legitimate business-to-business prospecting using referrals, professional networks, public business information and lawful commercial databases.

Electronic marketing by email, SMS, WhatsApp or similar stored message is subject to PECR. The requirements differ between corporate subscribers (such as limited companies) and individual subscribers (including sole traders and certain partnerships). We obtain consent where required or rely on an applicable soft opt-in only where all conditions are met. Where UK GDPR applies to a named business contact, we identify a lawful basis and provide appropriate transparency.

For live marketing calls we respect internal objections and screen relevant numbers against the Telephone Preference Service and Corporate Telephone Preference Service where required. Automated marketing calls are subject to separate restrictions.

You can object to direct marketing at any time by emailing **hello@hibits.co.uk** or using the unsubscribe process supplied with an electronic marketing message. We will stop using your personal data for direct marketing and may keep limited suppression information to respect your choice. Necessary service, invoice and security notices are not promotional marketing.

18. Who we share information with

We disclose personal information only where necessary and lawful for the relevant purpose. Recipients may include authorised members of our team, contracted support personnel, cloud and hosting providers, cybersecurity vendors, telecoms and messaging services, software distributors, accountants, auditors, insurers, banks, payment providers, relevant professional advisers and public authorities where required or permitted.

Depending on the customer and service, technology partners may include **Microsoft, Google, Apple, Syncro, ScreenConnect, Splashtop, Webroot, Hornetsecurity, 3CX, Twilio, 20i, Livedrive, GoCardless**, and authorised AI, connectivity, network, domain, backup and integration providers. This list is illustrative rather than exhaustive: not every provider receives each customer's data, and some suppliers act as independent controllers.

Where a provider acts as a processor or subprocessor, we apply appropriate contractual arrangements and authorisation requirements. We do not sell customer personal information to data brokers as a business activity.

19. International transfers

Some cloud, telecommunications, technical support and AI providers may access or process personal information outside the United Kingdom, even where the primary service is hosted in the UK.

Where UK transfer restrictions apply, we use an appropriate lawful mechanism, such as relevant UK adequacy regulations, the International Data Transfer Agreement, the UK Addendum to standard contractual clauses or another permitted route. We assess additional risks and safeguards where required.

Data residency and international support restrictions vary by product. Customers requiring a specific location or restricted transfer arrangement should ensure it is expressly documented in the relevant service specification.

20. How we secure information

We apply security measures proportionate to the nature of the service and the relevant risks. Depending on the environment, these may include restricted permissions and least-privilege administration; multi-factor authentication; secure remote access; appropriate encryption; secure credential handling; endpoint protection; monitoring; patching; backup and recovery measures; access and audit logs; supplier due diligence; confidentiality obligations; staff instructions; and incident-response processes.

We seek to minimise access to customer content and provide access only to people with a legitimate operational need. Our specific security arrangements depend on the service, configuration and applicable

contract. No electronic system can be guaranteed completely secure, and this policy does not represent a claim to hold any particular certification unless independently confirmed.

21. How long we retain information

We retain identifiable personal information for no longer than necessary for its purpose, subject to appropriate legal, contractual, security and dispute-related needs. We review retention and delete, minimise or anonymise information when identification is no longer justified.

Record category	Normal retention or governing criterion
Our routine recorded business calls	**12 months**; longer only where a specific documented lawful reason applies
Former customer contracts and account records	Normally **six years** after the customer relationship ends, subject to statutory duties and relevant claims
Unconverted enquiries and sales prospect records	Normally **two years** after the last substantive contact, unless another lawful reason applies
Accounting, invoices and tax records	Retained in line with statutory accounting and tax obligations (commonly six years for many records)
Identifiable support tickets and case histories	Kept while needed to support an active service, maintain appropriate account history, resolve disputes or fulfil lawful obligations; reviewed and anonymised or deleted once identifiable information is no longer required, normally within the former-customer retention framework
Anonymised technical learning and problem-resolution notes	May be retained long term, including indefinitely, only where individuals cannot reasonably be re-identified
Customer system backups	According to each customer's contracted plan, technical settings and applicable instructions
Security logs and monitoring data	According to system-specific retention, risk, service and contractual requirements
Marketing records and unsubscribe lists	Marketing records retained while lawful and useful; minimal suppression records as needed to honour an opt-out
Website cookies, analytics and form logs	According to the relevant purpose, cookie declaration and system retention settings

Support-ticket anonymisation: We maintain technical experience and recurring-fault resolutions for learning, troubleshooting and improving service. Before retaining such material solely for long-term knowledge purposes, we remove or irreversibly anonymise identifiers and other information capable of revealing a person, including within free-text notes and attachments where relevant. Replacing names with codes is not necessarily anonymisation; information that can still be linked back to an individual remains personal data and is subject to retention limits and rights.

Legal holds, ongoing complaints, claims or regulatory requirements may justify retaining particular identifiable records longer. Customer data processed solely on their behalf is returned, deleted or retained according to their lawful instructions and the applicable contractual terms. Copies in backups may persist until their scheduled expiry where lawful and technically appropriate.

22. Security incidents and personal data breaches

We investigate suspected or confirmed incidents, take appropriate containment and recovery steps and record our decisions. When acting as controller, we assess reporting duties to the Information Commissioner's

Office (ICO) and affected individuals. If a breach is reportable to the ICO, the usual requirement is notification without undue delay and, where feasible, within 72 hours of becoming aware of it.

When acting as processor, we notify the relevant customer controller without undue delay after becoming aware of a personal data breach, in accordance with legal and contractual duties. Not every technical incident is a personal data breach.

23. Your data protection rights

Subject to the applicable conditions and exemptions, individuals may have rights to be informed; access personal information; request correction or deletion; restrict processing; receive information in a portable format in qualifying circumstances; object to certain processing; withdraw consent where used; and obtain safeguards relating to certain automated decisions.

To exercise your rights, email **hello@hibits.co.uk** with the subject **Data Protection Request** and describe your request. We may seek proportionate identity verification to protect your information and other individuals. We ordinarily respond without undue delay and within one month, subject to lawful extensions, pauses and restrictions. Most requests are free of charge.

If the information is controlled by a customer and we act solely as its processor, the customer ordinarily decides how to respond and we assist as required. The right to object to processing for direct marketing is absolute.

24. How to complain

If you are unhappy with how we process personal information, email **hello@hibits.co.uk** with **Data Protection Complaint** in the subject line, or write to our registered office. Please explain your concern and provide relevant dates or correspondence if possible.

We provide an accessible way to complain, acknowledge a data protection complaint **within 30 days**, investigate and take appropriate steps without undue delay, keep the complainant informed as required and communicate the outcome without undue delay.

You also have the right to complain to the **Information Commissioner's Office**, https://ico.org.uk, telephone **0303 123 1113**, or seek an appropriate legal remedy. You do not have to resolve a complaint with us before contacting the ICO.

25. Children, healthcare, education and sensitive records

We may support customers such as schools, charities, healthcare and care providers whose systems contain personal information about children, patients, vulnerable people or other individuals requiring additional protection.

We access such records only to the extent authorised for support, restoration, migration or security tasks, apply appropriate confidentiality and access safeguards, and follow relevant controller instructions. The customer is generally responsible for its own legal bases, special category conditions, transparency and retention obligations. Our duties as processor and any separate controller obligations still apply.

26. Changes to this policy

We may revise this policy as our website, suppliers, services, AI systems, operating practices or legal requirements change. The effective date and version above identify the current published policy. If a material change requires additional notification or consent, we will take appropriate action.

Privacy contact: Highway Business Services (Hibits Ltd), Marlowe Innovation Centre, Marlowe Way, Newington, Kent, CT12 6FA. Email **hello@hibits.co.uk**. Telephone **01227 640547**. Website **https://hibits.co.uk**.