Horton Building Plastics
trading as Windows Plus Doors
Privacy Policy & Cookie Policy Pack

Effective date: 12 June 2026

Part A – Privacy Policy

Horton Building Plastics, which may also trade as Windows Plus Doors (*"we", "us", "our"*), is committed to protecting personal data and handling it lawfully, fairly, and transparently. This Privacy Policy explains what personal data we collect, how we use it, the lawful bases we rely on, who we share it with, how long we keep it, and the rights available to individuals in connection with that data.

1. Who we are and how to contact us

Horton Building Plastics is the data controller responsible for the personal data described in this Privacy Policy. Horton Building Plastics may also trade as Windows Plus Doors.

Business name: Horton Building Plastics

Trading style: Windows Plus Doors

Address: Unit 9 Britannia Park Industrial Estate, Stoke-on-Trent

Email: info@hortonbp.co.uk

Telephone: 01782 219916

If you have any questions about this Privacy Policy, want to exercise your rights, or wish to make a data protection complaint, please contact us using the details above.

2. Scope of this Privacy Policy

- customers and prospective customers;
- trade account applicants and account holders;
- individuals whose details are provided when orders, enquiries, quotations, deliveries, and collections are arranged;
- website visitors;
- people who contact us by phone, email, website form, social media, or in person;
- individuals whose personal data we receive from credit reference agencies, fraud prevention sources, or publicly available records where relevant to an application or account.

3. Categories of personal data we collect

Category	Examples
Identity data	Name, title, business contact name, company details where applicable.

Contact data	Billing address, delivery address, email address, telephone number.
Account and transaction data	Customer account references, order history, quotations, invoices, payment status, delivery and collection information.
Financial and credit data	Payment history, credit status, credit commitments, public record data, affordability and identity information obtained through credit reference processes where relevant.
Communications data	Emails, calls, messages, notes of enquiries, complaints, requests, and service contact history.
Technical and usage data	IP address, browser type, device information, website usage information, cookie identifiers, pages viewed, and diagnostic information.
Marketing and preference data	Subscription preferences, marketing consent records, suppression lists, communication preferences and engagement history.
Compliance and verification data	Records relating to fraud prevention, sanctions / legal checks if used, audit trail records, and evidence supporting regulatory or contractual compliance.

4. How we collect personal data

- directly from you when you contact us, request a quotation, place an order, apply for or use an account, make a payment, or interact with us in person;
- from your use of our website, including through cookies and similar technologies where deployed;
- from delivery arrangements, account administration, and customer service interactions;
- from credit reference agencies and related data partners where credit checks, affordability checks, identity verification, or fraud prevention checks are carried out;
- from publicly available sources where this is relevant to verifying identity, addresses, directorships, trading information, or recovering debts;
- from service providers, advisers, or counterparties where they share relevant data with us for operational or legal reasons.

Where we obtain personal data from a source other than the individual, we aim to describe the categories of data and the source in this policy and, where required, provide appropriate privacy information in line with applicable law.

5. Purposes of processing and lawful bases

We only process personal data where we have a lawful basis to do so. The main lawful bases we rely on are contract, legal obligation, legitimate interests, and consent. The table below links each core processing activity to the data used and the lawful basis relied upon.

Purpose / activity	Typical personal data used	Lawful basis	Notes
To respond to enquiries and provide quotations	Identity, contact, communications, project / order details	Legitimate interests and, where steps are requested before a contract, contract	Necessary to manage incoming sales enquiries and requested quotations.
To set up, manage, and service customer accounts	Identity, contact, account, transaction, communications data	Contract and legitimate interests	Necessary to administer customer relationships, orders, balances, and service queries.
To process orders and supply goods	Identity, contact, transaction, payment and delivery data	Contract	Necessary to fulfil orders, arrange delivery or collection, and issue associated documents.

To process and reconcile payments	Identity, contact, transaction, payment status and related finance data	Contract, legal obligation, and legitimate interests	Includes accounting, debt collection, and reconciliation.
To deliver or collect goods	Identity, contact and delivery data	Contract and legitimate interests	Necessary to coordinate deliveries, collections, and proof of delivery / collection.
To carry out credit checks, affordability checks, identity verification, and fraud prevention	Identity, contact, financial and credit data, public record data	Legitimate interests and legal / regulatory obligations where applicable	Supports responsible account management, fraud prevention, and risk control.
To keep business records and comply with tax, accounting, and legal obligations	Identity, contact, transaction, financial and communications data	Legal obligation	Includes statutory record keeping and responding to lawful requests.
To handle complaints, subject access requests, and other rights requests	Identity, contact, communications and relevant account / transaction data	Legal obligation and legitimate interests	Necessary to comply with data protection and consumer obligations and to resolve issues.
To improve our website, systems, and service quality	Technical, usage, communications and feedback data	Legitimate interests and, where required for non-essential cookies, consent	Helps us monitor performance, improve usability, and maintain security.
To send marketing communications	Identity, contact, marketing preference and engagement data	Consent where required, and legitimate interests where permitted by law	Individuals can opt out at any time.
To protect our business, network, systems, staff, customers, and suppliers	Identity, technical, communications, account and verification data	Legitimate interests and legal obligation where applicable	Includes fraud prevention, system security, incident response, and audit controls.

6. Legitimate interests

Where we rely on legitimate interests, we assess whether the processing is necessary and consider the impact on individuals, including whether appropriate safeguards are in place and whether the processing would be expected in the circumstances.

The legitimate interests pursued by the controller (if processing is based on legitimate interests).

Our legitimate interests include operating our business, fulfilling contractual obligations, ensuring system and data security, preventing fraud, supporting audit and compliance activities, and protecting TransUnion data. These interests are balanced against the rights and freedoms of individuals, with appropriate safeguards in place.

7. Data sharing and disclosure of personal data

We do not sell, rent, or trade personal data. We may, however, share personal data where necessary for legitimate operational reasons, compliance reasons, or the provision of services. The categories of recipients are set out below.

Recipient category	Why personal data may be shared	Typical data involved
Delivery and logistics providers	To deliver goods, coordinate routes, confirm delivery / collection, and resolve service issues.	Identity, contact and delivery data.
Payment processors / banking / finance systems	To process payments, reconcile accounts, manage refunds and payment failures, and support fraud controls.	Identity, contact, transaction and payment-related data.

IT, software, website, communications, and hosting providers	To host systems, maintain business continuity, support email / CRM / cloud systems, and safeguard services.	Identity, contact, communications, technical and related operational data.
Professional advisers	To obtain legal, accounting, audit, insurance, debt recovery, or other professional support.	Relevant identity, contact, transaction, finance, and communications data limited to what is necessary.
Credit reference agencies and related data partners	To assess applications, support creditworthiness decisions, verify identity, prevent fraud and manage risk.	Identity, contact, financial, credit, payment history and public record data.
Regulators, courts, law enforcement, or public authorities	To comply with legal obligations, defend legal claims, or respond to lawful requests.	Only the information reasonably necessary to comply.
Business transaction counterparties	If we reorganise, buy, sell, transfer, or merge part of the business, data may be reviewed or transferred in that context.	Relevant customer, supplier, account, and operational data subject to confidentiality and legal safeguards.

Where third parties process personal data on our behalf, we expect them to protect it, keep it secure, and only use it in accordance with applicable law and our instructions where relevant.

8. Credit Reference and Affordability Checks

Credit Reference and Affordability Checks

To help us assess applications, prevent fraud, and meet our legal and regulatory obligations, we may obtain information about you from credit reference agencies (CRAs).

We obtain this information via Creditsafe, which uses its data partner TransUnion to supply consumer credit and identity data.

Creditsafe Business Solutions Limited is authorised and regulated by the Financial Conduct Authority

FCA Firm Reference Number: 742313

TransUnion International UK Limited is authorised and regulated by the Financial Conduct Authority

FCA Firm Reference Number: 737740

The information we receive may include data relating to your identity, credit commitments, payment history, and public record information. This data is used solely for legitimate business purposes, including creditworthiness assessment, identity verification, and fraud prevention, in accordance with applicable data protection laws.

Further information about how Creditsafe and TransUnion process your personal data can be found in their respective privacy notices:

Creditsafe Privacy / Transparency Notice:

Transparency Notice | Customers & Suppliers

TransUnion CRAIN (Credit Reference Agency Information Notice):

https://www.transunion.co.uk/legal/privacy-centre/pc-credit-reference

TransUnion Bureau Privacy Notice:

https://www.transunion.co.uk/legal/privacy-centre/pc-bureau

9. International data transfers

Some of our service providers may store or process personal data outside the UK. Where this happens, we aim to ensure that appropriate legal safeguards are in place, such as an adequacy decision, an approved transfer mechanism, or equivalent contractual and technical protections.

Because suppliers and systems can change over time, this Privacy Policy describes the principle we apply rather than naming every individual hosting location. If you need more detail about a particular transfer in connection with a rights request, you may contact us using the details above.

10. Data retention

We retain personal data only for as long as is reasonably necessary for the purposes for which it was collected, to meet legal and regulatory obligations, to resolve disputes, and to protect our legitimate business interests. Retention periods may vary depending on the type of data and the context in which it was collected.

Record type	Typical retention approach	Reason
Financial and accounting records	Typically up to 6 years after the end of the relevant financial period or relationship, unless longer retention is required.	Tax, accounting, audit, and legal obligations.
Customer account and transaction records	Usually the duration of the relationship and then a reasonable follow-on period.	Operational continuity, repeat business history, complaints handling, and legal protection.
Quotation and enquiry records where no account is opened	Usually 12 to 24 months unless a longer period is justified.	Business administration, service follow-up, and evidence of communications.
Marketing records and consent logs	Retained while marketing continues and for a reasonable period after unsubscribe / objection.	Compliance evidence and suppression management.
Credit assessment and fraud prevention records	Retained for as long as reasonably necessary for risk management, audit, compliance, and dispute handling.	Protection against fraud, financial risk management, and evidential requirements.
Website analytics / cookie records	Varies by cookie and system configuration.	Performance monitoring, consent management, and security.

We may retain limited information for longer where there is an outstanding dispute, legal claim, ongoing investigation, or another lawful reason to preserve records. When data is no longer required, we aim to delete it, anonymise it, or otherwise dispose of it securely.

11. Security of personal data

- access controls and permissions;
- system, account, and data security measures;
- appropriate supplier and software controls where third parties support our systems;
- measures designed to prevent unauthorised access, alteration, disclosure, loss, or destruction of data;
- processes to support audit, compliance, fraud prevention, and incident management.

No method of transmission or storage is completely secure. However, we aim to apply measures that are appropriate to the nature of the data and the risks involved.

12. Your data protection rights

- the right to be informed about how your personal data is used;
- the right to request access to your personal data;
- the right to request correction of inaccurate or incomplete personal data;
- the right to request erasure in certain circumstances;

- the right to request restriction of processing in certain circumstances;
- the right to object to processing in certain circumstances, including certain marketing and legitimate interests processing;
- the right to data portability in certain circumstances;
- the right to withdraw consent where consent is the lawful basis relied on for particular processing;
- rights relating to automated decision-making where applicable under law.

These rights are not absolute and may be subject to exemptions or conditions under applicable law. To exercise a right, please contact us with enough information to identify you and the request you are making.

13. Complaints and how to contact us about privacy matters

If you have a concern about how we handle personal data, we encourage you to contact us first so that we can investigate and try to resolve the matter. Please email info@hortonbp.co.uk or use the contact details in Section 1.

When a complaint is received, we aim to log it, review the concern, investigate where necessary, and respond with an outcome. If you remain dissatisfied, you may raise the matter with the UK Information Commissioner's Office (ICO).

14. Automated decision-making and profiling

In some circumstances, we may conduct automated decision making or profiling using personal data. This involves the use of automated systems to evaluate certain information about an individual, such as risk factors, affordability indicators, or fraud signals, based on predefined rules or algorithms. Making or profiling using personal data. This involves the use of automated systems to evaluate certain information about an individual, such as risk factors, affordability indicators, or fraud signals, based on predefined rules or algorithms. Making or profiling using personal data. This involves the use of automated systems to evaluate certain information about an individual, such as risk factors, affordability indicators, or fraud signals, based on predefined rules or algorithms.

Where automated decision making is used, it may result in decisions such as the approval, restriction, or rejection of an application or service.

Individuals have the right to request human intervention, to express their point of view, and to challenge decisions made solely by automated means. Further information about automated decision making and how to exercise these rights can be obtained by contacting us using the details provided in this Privacy Policy. Making and how to exercise these rights can be obtained by contacting us using the details provided in this Privacy Policy-making and how to exercise these rights can be obtained by contacting us using the details provided in this Privacy Policy

15. Third-party websites and services

Our website or communications may contain links to third-party websites or services. Those third parties are responsible for their own privacy practices, notices, and cookie usage. We are not responsible for the privacy content or handling practices of third-party sites that we do not control.

16. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in legal requirements, business practices, suppliers, systems, or website functionality. The latest version should be made available through the appropriate publication channel, including our website where relevant.

Part B – Cookie Policy

This Cookie Policy explains how Horton Building Plastics uses cookies and similar technologies on its website, how those technologies are categorised, and what choices users have in relation to them.

1. What are cookies and similar technologies?

Cookies are small text files and similar identifiers stored on or accessed from a device when a website or online service is used. Similar technologies can include tracking pixels, scripts, tags, local storage, and other tools that store or access information on a device or support online measurement and functionality.

2. Why we use cookies

- to make the website function properly;
- to support security and technical operation;
- to remember choices or preferences where used;
- to understand website usage and performance;
- to support analytics, communications, marketing, and related functionality where those features are enabled.

3. Cookie categories we may use

Category	Purpose	Consent position	Examples / notes
Strictly necessary	Essential for core website operation, security, form submission, or user-requested services.	Generally does not require consent where genuinely necessary.	May include security, session, basket, or load-management cookies if used.
Preferences / functionality	Remembers user choices or display settings and supports usability.	Consent or another permitted approach may apply depending on how the technology is used.	May include language, accessibility, interface, or site preference settings.
Analytics / statistical	Helps us understand traffic, page interaction, and performance.	Consent may be required unless a lawful exemption applies in the specific implementation.	Whether an exemption is available depends on how the analytics are configured and used.
Marketing / advertising / tracking	Measures campaigns, supports targeted advertising, or tracks behaviour across services.	Requires consent before use.	Includes advertising, remarketing, and cross-site tracking tools where deployed.

4. Consent and user choice

Where consent is required for a cookie or similar technology, we aim to request that consent through an appropriate consent mechanism before the technology is deployed. Users should be able to accept, reject, or manage relevant non-essential categories, and should be able to revisit those choices.

Users may also be able to manage certain cookies through browser settings, although doing so may affect how the website functions.

5. Third-party cookies and embedded services

If our website uses third-party services such as analytics tools, payment components, mapping tools, embedded media, marketing tags, or chat systems, those services may set or access cookies or similar identifiers. The specific technologies used can change over time depending on the website build and suppliers in use.

Third-party providers may process information under their own privacy and cookie notices, as well as under contractual arrangements with us where applicable.

6. Cookie information and review

A website-specific cookie inventory or cookie table is recommended for publication alongside this policy where practical, because individual cookies, durations, providers, and purposes depend on the live website configuration

and any embedded services. This policy is intended to provide the overarching framework and category-level explanation.

7. How long cookies stay on a device

Some cookies are session-based and expire when a browser session ends. Others are persistent and remain for a set period unless deleted sooner. The lifespan depends on the specific tool or service involved.

8. Changes to this Cookie Policy

We may update this Cookie Policy to reflect changes to law, guidance, suppliers, website functionality, or the technologies used on the website. The current version should be made available through the website or other relevant publication location.

9. Contact

Questions about this Cookie Policy or about privacy more generally can be sent to info@hortonbp.co.uk.

Part C – Operational publication checklist

- Confirm the controller's registered / trading address and website publication footer details.
- Confirm whether any separate staff / recruitment privacy notice is also required.
- Confirm the live website cookies and publish a website-specific cookie table if possible.
- Confirm the actual suppliers used for hosting, email, payment processing, analytics, CRM, and delivery if you want to name them specifically.
- Confirm whether any finance / BNPL / retail finance journey is used and whether additional lender disclosures are required.
- Check whether any CCTV, call recording, or employee monitoring notice is needed separately.
- Ensure privacy and cookie links appear in the website footer and at key collection points such as forms, account applications, and checkout where applicable.
- Check that the complaints handling process is implemented operationally, not just documented in the policy.