Effective Date: November 19, 2025

1. Introduction

At Tassel & Wicker (referred to as "we," "us," or "our"), we value your privacy and are committed to protecting your personal data. This Privacy Notice explains how we collect, use, and protect your personal data when you use our website, purchase items from the organisation, or interact with us.

We are committed to protecting your privacy and handling your personal data in an open and transparent manner. This Privacy Policy sets out how we collect, use, store, and share your personal data, and explains your rights under UK data protection law.

2. Who We Are

Business Name: Tassel & Wicker

Jurisdiction: United Kingdom

Type of Business: Retail business specialising in lifestyle products, home goods and gifts.

Contact Email for privacy: Info@tasselandwicker.com

For all privacy and data protection inquiries, or to exercise your data subject rights, please contact us directly at the email address provided above: info@tasselandwicker.com.

3. Personal Data We Collect

We collect and process the following categories of personal information:

- Identifiers: Names, Email addresses, Phone numbers, Addresses, Photos, ID or passport information
- Commercial Information: Payment Details, Location data.
- Internet Activity Information: Website activity or cookies.

Personal information is anything that directly or indirectly identifies and relates to a living person, such as a name, address, telephone number, date of birth, unique identification number, photographs, video recordings. WE DO NOT COLLECT video recordings.

Some personal information is ‘special category data’ and needs more protection due to its sensitivity. This includes any information about an identifiable individual that can reveal their sexuality and sexual health, religious or philosophical beliefs, racial origin, ethnicity, physical or mental health, trade union membership, political opinion, genetic/biometric data. Personal information relating to criminal offences and convictions, although not ‘special category data’, is still sensitive in nature and merits higher protection.

We do not collect Health information or Employment details.

4. How We Collect Your Data

We collect data through the following methods:

- Website forms when you populate them.
- Sign-up sheets
- Newsletter Subscription forms
- Cookies
- Social media interactions

5. Why We Collect and Use Your Data (Our Lawful Basis)

We collect your personal data for the following purposes, based on the identified lawful basis:

Purpose of Collection	Lawful Basis
To provide a product or service	Performance of a contract with you
To process payments or invoices	Performance of a contract with you
To contact customers or respond to enquiries	Legitimate Interests (responding to customer requests)
To send marketing or newsletters	Consent (where required) or Legitimate Interests (for existing customers)
To improve our website or services	Legitimate Interests (improving customer experience)
To meet legal or tax requirements	Compliance with a legal obligation
To recruit staff or volunteers	Legitimate Interests or Pre-contractual steps.

6. Sharing Your Personal Data

We share your personal data with third-party service providers and partners to operate our business effectively. We will only share data necessary for them to perform their services.
Examples of parties we share data with:

- Newsletter/Marketing Providers: Email addresses shared with services to send you marketing communications.
- Financial Services Providers: Payment Details shared with services to process your payments.
- Other Service Providers: As needed depending on the context, which may include logistics partners, IT service providers, etc.

We take steps to ensure all third parties are compliant with UK General Data Protection Regulation(GDPR).

7. Data Storage and Security

- Storage Locations: We store data on company computers, on our website database, and in the cloud (iCloud).
- Security Measures: We use the following measures to protect your data:
    - Passwords: Data is stored in locations accessible only with a password.
    - Encryption: We use methods such as hashing, pseudonymisation, and anonymization to encrypt data.
    - Access Controls: Security measures ensure only authorised individuals can access personal data, systems, or files when required.

8. International Data Transfers

Some of our third-party service providers may host data outside the UK. Where this is the case, we will ensure appropriate safeguards such as Standard Contractual Clauses are in place to ensure your personal data is protected to the same standard as in the UK.

We share your personal data with certain service providers who are based outside the UK and the European Economic Area (EEA). This is necessary to facilitate our business operations, such as:

- Using cloud hosting services (for website and data storage).

- Utilising specific software platforms like email marketing, customer relationship management.

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

1. Adequacy Decisions

We may transfer your data to countries that have been deemed to provide an adequate level of protection for personal data by the UK government.

2. Appropriate Safeguards (Contractual Clauses)
Where an adequacy decision does not exist, we will use appropriate safeguards, which include implementing:

The International Data Transfer Agreement (IDTA) issued by the UK Information Commissioner's Office (ICO); OR

The International Data Transfer Addendum to the European Commission's Standard Contractual Clauses (SCCs).

These contractual documents provide specific obligations on the recipient of the data to protect your personal data to the standard required by UK data protection law.

3. Necessity/Derogations:
In the absence of an adequacy decision or appropriate safeguards, we may rely on a specific derogation for the transfer such as where the transfer is necessary for the performance of a contract between you and us, or you have given explicit consent to the proposed transfer after being informed of the risks. This is typically only for one-off or non-systematic transfers.

9. Your Data Protection Rights
Under UK data protection law, you have the following rights, which you can exercise by contacting us at Info@tasselandwicker.com

- Right to Opt-out of Marketing: You can always opt out of marketing by following the unsubscribe link provided in our marketing emails.
- Right to Access (Subject Access Request): You have the right to ask for a copy of the personal data we hold about you.
- Right to Rectification: You have the right to ask us to correct data that you believe is inaccurate or incomplete.
- Right to Erasure ('Right to be Forgotten'): You have the right to ask us to delete your personal data.

If you wish to exercise your rights (Access, Correction, Deletion), please contact us via info@tasselandwicker.com, and we will process your request manually.

10. Data Retention and Disposal
We will only keep your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

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 unauthorized use or disclosure of your personal data, the purposes for which we process your personal data, and any applicable legal requirements.

We adhere to the following standard retention periods:

- Financial & Tax Records: We generally retain financial transaction data (including payment details and associated customer information) for six years after the end of the relevant tax year, to comply with legal obligations set by His Majesty's Revenue and Customs (HMRC).
- Customer Order History: This data is retained for a period of up to one year after the last purchase to cover potential contractual claims, manage warranty issues, and provide customer support.
- Marketing Consent (Email List): We retain your email address until you unsubscribe.

11. Disposal Methods: When data is no longer needed, we will safely dispose of it by:
Digital Data (Website/Computers/iCloud): We use methods such as secure deletion (wiping) software to ensure data is permanently removed and cannot be recovered. Where data is highly sensitive, we may use anonymisation to retain statistical information without identifying you.

12. Website Cookies and Tracking

We use tracking tools and cookies on our website such as:

Cookie Name	Provider	Purpose	Type	Expiry	Category
_stripe_mid	Stripe	Used for fraud prevention and distinguishing users during payment. Helps Stripe identify the device for secure checkout.	Third party(Strict)	1 year	Strictly Necessary
__vercel_toolbar	Vercel	Enables the Vercel developer toolbar in preview environments. Not used for tracking.	First-party	17 days	Functional/Performance
auth-storage	This Website(Next.js + Firebase Auth)	Stores encoded authentication/session data for logged-in users	First-Party	128	Strictly Necessary

cookieConsent	This Website	Stores whether the user accepted the cookie banner	First-Party	21 days	Preferences

13. Data Breach Procedure

A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

We have a procedure in place to deal with any suspected personal data breach and will follow these steps:

1. Containment & Assessment: We will immediately take steps to contain the breach and assess the risk level and the extent of the data compromised.
2. Notification to the ICO: If the breach is likely to result in a risk to the rights and freedoms of individuals, we will report the breach to the Information Commissioner's Office (ICO) in the UK within 72 hours of becoming aware of it.
3. Notification to Affected Individuals: If the breach is likely to result in a high risk to the rights and freedoms of individuals like identity theft, or financial loss, we will inform the affected individuals directly and without undue delay, advising them on the steps they can take to protect themselves.
4. Investigation & Remediation: We will investigate the cause of the breach and take measures to prevent any reoccurrence like enhancing security protocols, or providing extra staff training.
5. Documentation: We will keep a detailed record of all personal data breaches, regardless of whether we are required to notify the ICO or the individuals.

Do you accept these terms and conditions?