Data Protection Policy

This policy outlines how Ashford Colour Ltd complies with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, **and the Data (Use and Access) Act 2025 (DUAA)**. It provides a framework for the responsible, lawful, and secure handling of personal data.
It applies to:

- All employees and contractors
- All systems, processes, and data controlled or processed by Ashford Colour Ltd
- Both electronic and hard copy information

Ashford Colour Ltd is committed to maintaining the confidentiality, integrity, and availability of personal data. We aim to handle all data fairly, lawfully, and transparently, in line with our legal obligations and the expectations of data subjects.

We are registered with the Information Commissioner's Office (ICO) as a Data Controller: ZB890205

In general terms, we process information to:

- Provide a printing service
- Support and manage our employees
- Promote and advertise our products and services
- Maintain our accounts and records

Awareness and Accountability
We operate in accordance with the accountability principle of UK GDPR and DUAA, maintaining effective policies and procedures to demonstrate compliance. All employees must follow this policy and with our GDPR Procedures Document (Statement of Applicability). Data protection and IT security responsibilities are included in each employee's contract.

Information Held
Details of all personal data held are recorded in our Information Asset Register, including:

- What data we hold
- Why we hold it
- Where it came from
- How it is used and shared
- How long it is retained

These records enable us to correct or update shared data promptly when we are notified of errors.

Privacy Information
We maintain a documented Privacy Notice that complies with UK GDPR and DUAA.
This Notice is available on our website and it explains:

- Who we are
- How we use data
- Our lawful bases for processing
- Retention periods
- Rights of individuals
- How to raise concerns with the ICO

This policy is made available to relevant interested parties externally on our website and internally through training and awareness programmes.

Data Protection Responsibility
While we are not legally required to designate a Data Protection Officer (DPO), our Finance Director holds overall responsibility for data protection compliance.

Individuals' Rights
Our GDPR Statement of Applicability outlines how we uphold the rights of individuals under UK GDPR and DUAA,including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

---

Subject Access Requests (SARs)
We follow these principles:

- No charges for SARs unless the request is manifestly excessive
- Responses provided within one month, with the ability under DUAA to pause ('stop the clock') while awaiting clarification or ID verification.
- Conduct 'reasonable and proportionate' searches in line with DUAA requirements
- Reasons give if a request is refused
- Individuals informed of their rights to complain to the ICO

Data will be supplied in a commonly used format, free of charge, unless the request is manifestly excessive.

Lawful Basis for Processing
We rely on:

- **Legitimate Interests** for general business and customer relationships, fraud prevention, maintaining security, and emergency response (recognised legitimate interests under DUAA)
- **Contract** for obligations related to employees, customers, and suppliers
- **Consent** for marketing communications to new prospects

Consent Management
Where we use consent:

- It is specific, freely given, and actively opted into
- Pre-ticked boxes are not used
- Consent requests are clear, granular, and easy to withdraw
- Consent is recorded and reviewed
- Separate consent is obtained for different purposes
- Controllers relying on consent are named

We never make consent a precondition of service and withdrawal of consent is straightforward and always respected.

Children's Data
We do not process data relating to children.

Data Breaches
We have procedures to detect, report, and investigate data breaches. Where a breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the ICO and affected individuals as required.

This policy is made available to relevant interested parties externally on our website and internally through training and awareness programmes.

Data Protection by Design & DPIAs
We apply data protection by design and by default. Privacy Impact Assessments (PIAs) are carried out for new projects, and existing data processes are reviewed through internal audits.

A Data Protection Impact Assessment (DPIA) will be conducted where:

- New technologies are deployed
- Profiling is likely to significantly affect individuals
- When there is large-scale processing of special category data

If a DPIA indicates high risk which cannot be sufficiently mitigated, we will consult the ICO before proceeding.

Third-Party and Outsourced Services
Where we share personal data with external service providers, we ensure appropriate data protection agreements are in place. To ensure that outsourced providers meet our legal and security obligations under UK GDPR and DUAA.

International Transfers
We operate solely from the UK. Where international transfers are required, we follow DUAA's "not materially lower" protection standard, ensuring the destination offers protections comparable to UK standards.

R. Hutcheson

R. Hutcheson
Director
Policy Version: August 2025

This policy is made available to relevant interested parties externally on our website and internally through training and awareness programmes.