



Data Protection Policy

This Data Protection Policy sets out how Ashford Colour Press Ltd complies with the principles of GDPR.

The policy aims to address data protection in a consistent manner and to demonstrate accountability under the GDPR. This is a standalone policy statement, however, it also forms part of a group of documents which together make up our GDPR Manual, is part of our general staff policy and integrates with our ISO management system.

The policy sets out our approach to data protection together with responsibilities for implementing the policy and monitoring compliance.

The policy has been approved by management, published and communicated to all staff. The policy is reviewed and updated at planned intervals, or when required to ensure it remains current.

Ashford Colour Press Ltd is registered with the Information Commissioner's Office (ICO) as a Data Controller, registration number ZA 183327.

Awareness

At all times we are working to GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place. This document is our GDPR Data Protection Policy and we also have a GDPR procedures document in place called a Statement of Applicability, which all employees are aware of, and are required to work in accordance with. Responsibilities for data protection compliance and IT security form part of every employee's contract.

Information Held

Details of all data held is documented in our Information Asset Register. In it we record what data we hold, where it came from, why we hold it, how we use it, who we share it with, and how long it will be retained. These records are maintained so that if shared data is found to be incorrect, we are able to notify the third party, so they can correct their record.

In general terms, we process information to enable us to provide a printing service, to support and manage our employees, promote and advertise our products and services, and maintain our own accounts and records.

Communicating Privacy Information

We have a documented Privacy Notice in compliance with GDPR legislation. This sets out the steps we follow when personal data is collected, such as our identity and how we intend to use the information, the lawful basis for processing the data, our data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way we are handling their data.

Under the legislation, we are not formally required to designate a Data Protection Officer (DPO), we have a nominated person to take responsibility for data protection compliance, this will be the Finance Director. The ISO Manager has also been nominated for the day to day running of Data Protection within Ashford Colour Press Ltd.

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

Individuals' Rights

Our **GDPR Statement of Applicability** covers all the rights individuals have, including how we delete personal data or provide data electronically and in a commonly used format when requested to do so.

We work to uphold and comply with the GDPR rights for individuals which include:

- 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; and
- the right not to be subject to automated decision-making including profiling.

Our systems will allow us to locate and delete the data. Any request to delete data would be referred to the designated Director to make the decisions about deletion and keep the data subject informed of the process.

When requested to do so, we will provide the personal data in a structured commonly used and machine readable form, and will provide the information free of charge.

Subject Access Requests

Our GDPR Statement of Applicability covers how we will handle requests to take account of the new rules. Therefore we will:

- Not charge for complying with a request.
- Comply within a month.
- Reserve the right to refuse or charge for requests that are manifestly unfounded or excessive.
- If we refuse a request, we will tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest, within one month.

We will always explain our lawful basis for processing personal data when we answer a subject access request.

Lawful Basis for Processing Personal Data

The lawful bases for our data processing activity are a combination of **Legitimate Interest and Contractual** for activities relating to staff, suppliers, existing customers and other stakeholders, and **Consent** for marketing communications purposes to new prospects.

The decision for selection of the Legal Bases we rely upon are as follows:

Legitimate Interests:

- We use people's data in ways they would reasonably expect in order to carry out our business and communicate with them.
- Processing is necessary as we could not provide products and ongoing services to prospects and our existing customers without processing this information.
- We have balanced our commercial interests against the individual's interests, rights and freedoms. Our processing has a minimal privacy impact.

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

Contract:

- We have a contract with an individual and need to process their personal data to comply with our obligations under the contract ie employment contract
- We haven't yet got a contract with an individual, but they have asked us to do something as a first step (eg provide a quote) and we need to process their personal data to do what they ask.
-

Consent:

- We aim to deliver effective, timely communications to our prospects, such as newsletters, relevant information on opening times etc.
- We will follow the steps below when relying on Consent as a legal basis.
-

Processing of new prospect information is necessary under this legal basis in order to provide communications relevant to commercial requirements. We will always make it clear when requesting Consent what the data will be used for and have clear, simple ways for people to withdraw consent.

Where Relying on Consent as a Legal Basis:

- When using Consent it means we are offering individuals real choice and control, putting individuals in charge to build customer trust and engagement, and enhance our reputation.
- Consent practices and existing consents have been checked and refreshed where needed to comply fully with GDPR.
- Consent requires a positive opt-in, we don't use pre-ticked boxes or any other method of default consent.
- We will only obtain clear and specific statement of consent.
- Our consent requests are kept separate from other terms and conditions.
- We are specific and 'granular' so that we get separate consent for separate things.
- We are clear and concise when asking for consent.
- Third party controllers who will rely on the consent are named.
- We make it easy for people to withdraw consent and tell them how.
- Evidence of consent is recorded – who, when, how, and what we told people.
- Consent is kept under review, and refreshed if anything changes.
- We avoid making consent to processing a precondition of a service.
-

Children

No data processing relating to children or children's data is undertaken.

Data Breaches

We have procedures in place to detect, report and investigate a personal data breach.

In accordance with GDPR we will notify the ICO, and where necessary individuals, of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage.

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

Data Protection by Design and Data Protection Impact Assessments

As GDPR makes privacy by design an express legal requirement under the term 'data protection by design and by default', we have adopted this approach.

To do so we undertake **Privacy Impact Assessments (PIA)** and approach new projects with privacy and data protection in mind from the outset. Consideration is given to this from the start of any new project, then throughout its lifecycle. Existing data is under continuous review through our internal auditing process.

As part of this approach we have a **Privacy Notice** and conduct **Privacy Impact Assessments (PIAs)** to ensure ongoing compliance.

PIAs, also referred to as 'Data Protection Impact Assessments', are mandatory in certain circumstances and will be used where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

Under such circumstances DPIAs will be carried out, however, no profiling or large scale processing operations are currently undertaken by us.

If a DPIA indicates that the data processing is high risk, and we cannot sufficiently address those risks, we will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Data Protection Officer

Although we are not required to formally designate a Data Protection Officer (DPO), we have a nominated person to take responsibility for data protection compliance, this is our Finance Director. The ISO Manager has also been nominated for the day to day running of Data Protection within the Ashford Colour Press Ltd.

International

Our main establishment is located at: *Unit 220/230, Fareham Reach, Fareham Road, Gosport Hampshire, UK.*

We do not carry out cross-border processing, i.e. have establishments in more than one EU member state, or have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states. The location above is identified as the main establishment for the sake of completeness.

Rob Hutcheson

R. Hutcheson

Director

Data Protection Policy – Rev 1 April 18 Reviewed January 2022

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