Information Security Policy

Ashford Colour Ltd, part of the Pureprint Group, is committed to protecting the confidentiality, integrity, and availability of information in both hard copy and electronic form. This policy supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA), as well as other relevant legal and contractual requirements. It provides a framework for the secure access, storage, processing, and dissemination of information in line with recognised good practice.

This policy applies to:

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

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

Information Security CIA

All staff are expected to ensure that information resources are handled with appropriate levels of security in accordance with this policy, in order to:

- Maintain **confidentiality** – ensuring information is only accessible to those with authorised access.
- Maintain **integrity** – safeguarding the accuracy and completeness of information.
- Maintain **availability** – ensuring information is accessible when required by authorised users.

Identifying and Managing Risk

We undertake regular information security risk assessments to ensure that technical and organisational measures are proportionate to the risks presented by the information we hold and process. These assessments take account of:

- The type, volume, and sensitivity of data.
- Legal and contractual obligations.
- Evolving threats and vulnerabilities.

Risk assessments are conducted in conjunction with our GDPR Statement of Applicability, Data Protection Policy, and supporting security procedures.

Technical and Organisational Measures

We implement a layered approach to information security, including:

Access Controls

- User access is role-based and granted only as required for an individual's duties.
- Strong authentication measures are in place for system access.

IT Security

- **Our** servers and systems are managed by an approved external IT provider, with whom we have GDPR and DUAA-compliant contractual agreements.
- Systems are protected with up-to-date antivirus, endpoint security, and firewalls.
- Data backups to secure cloud-based storage are end-to-end encrypted.

Encryption

- Encryption is applied to protect personal or sensitive information in transit and at rest, where appropriate.

CCTV

- CCTV recordings are retained for a maximum of 30 days unless required for legal purposes. Access to recordings is restricted and monitored.

Disposal of Information Assets

- Obsolete IT equipment is securely wiped using certified methods before disposal.
- Hard copy confidential or personal data is securely shredded; non-confidential materials are recycled where appropriate.

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

Physical Security

- Confidential documents are locked away when not in use.
- Workstations are locked when unattended and positioned to avoid unauthorised viewing.

Information Held

Details of the personal data we hold, why we hold it, and how long it is retained are recorded in our Information Asset Register. This register supports compliance with UK GDPR and DUAA by enabling prompt correction or deletion of data when required.

Incident Reporting and Breach Management

Any employee who becomes aware of an incident, suspected breach, or risk to information security must report it immediately to their line manager, who will escalate to the relevant Director. We have procedures in place for the detection, reporting, and investigation of data breaches, in line with UK GDPR and DUAA. Where a breach poses a risk to individuals' rights and freedoms, the ICO and affected individuals will be notified as required.

Roles and Responsibilities

- **Directors** – Ensure resources are in place for effective implementation of this policy.
- **All Users** – Responsible for protecting information and following company procedures.
- **Managers** – Ensure their teams understand and comply with this policy.

Information security responsibilities are included in all employee contracts, and breaches may result in disciplinary action up to and including dismissal.

Training and Awareness

- All new staff receive information security and data protection training at induction.
- Annual refresher training is provided to all employees.
- Additional role-specific training is given where required.

This policy is reviewed at least annually, or sooner if legal, technological, or operational changes require it. It is made available externally on our website and internally through training and awareness programmes.

R. Hutcheson

R. Hutcheson
Director
Policy Version: August 2025