Ashford

Information Security Policy

Ashford Colour Press will create an environment where the security of information, hard copy and electronic is maintained as appropriate. Implementation of the Information Security Policy will ensure compliance with legal requirements and provide a framework for the access, storage and dissemination of information in line with good practice.

All Ashford Colour Press Ltd staff are expected to ensure that information resources are handled with the appropriate levels of security in accordance with the Information Security Policy in order to maintain the confidentiality, integrity and availability of information.

Identifying and Managing Risks

We ensure appropriate security measures are in place to protect the personal and commercial data that we process. Risk assessments are undertaken in order to choose security measures that are appropriate to the data we hold.

We have a robust approach to information security, keeping our IT systems safe and secure is a high priority. To do so, we employ an IT Manager and an external IT supplier to provide specialist expertise and guidance on appropriate measures to secure our systems.

All reasonable steps are being taken to ensure data security both organisationally and technologically, we have the following in place to manage and maintain it.

Technical and Organisational Measures

As part of our data security measures, staff can only access our computer systems through password protected remote desktop system via our IT supplier. This IT supplier manages our servers, which in turn means we are ‘sharing’ data with them. The external IT supplier and internal IT Manager ensure data security, for example by keeping our virus protection software and firewall protection current, providing the best IT security available, and making us aware of evolving risks and threats.

We assess the need to utilise encryption, ie the process of encoding (or scrambling) information so that it can only be converted back to its original form (decrypted) by someone who (or something which) possesses the correct decoding key. Where necessary to protect personal or sensitive information this is in place.

ISO document, **Procedure 1. Document, Data & Record Control** covers aspects of Information Security to ensure documented information is available where needed and that it is suitable for use. It also seeks to ensure information and records are adequately protected against improper use, loss of integrity and loss of confidentiality.

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

Electronic Records (Data)

- The network is fully protected against viruses and utilizes firewalls.
- Access to information on the server is set up as relevant to an individual's position and job role.
- Incoming email is screened for viruses and any potential threat is quarantined.
- Obsolete equipment - in the event of any sensitive electronic data being held on equipment identified for disposal, we will make arrangements to remove data before final disposal using propriety software.
- CCTV systems are utilised to site as part of security measures. We control who can see the recordings, and have controls in place to sure the system is only used for the purpose it was intended for.
- Computer screens on which confidential or sensitive information is processed or viewed are sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.
- Data backed up to cloud based storage is subject to end-to-end encryption.

Information held in hard copy

- Members of staff who handle confidential or 'personal' paper documents take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times. Care should also be taken when printing confidential documents to prevent unauthorised disclosure.
- Hard copy confidential or personal information must be shredded, however if appropriate, other documents (with no personal information therein) can be segregated for recycling.

Roles and Responsibilities

We make it clear to all our staff the roles and responsibilities they have in relation to keeping information secure.

Our Employee Handbook and staff contracts make reference to data security and confidentiality, detailing what would constitute a breach of data security and the consequences of doing so. These terms cover all staff and all types of information whether in electronic, hard copy or other form.

New staff receive training upon induction, and leavers are required to return any electronic and hard copy records to the company.

All users are accountable for their use of information in line with information security policy.

Any employee who becomes aware of an incident or risk to information security has a duty to inform their immediate line manager, who in turn will pursue the matter to Quality Manager and IT Manager to ensure investigation and effective resolution.

Rob Hutcheson

R. Hutcheson

Director

Policy Version: January 2023

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