SHEAF CLOSE, LODGE FARM INDUSTRIAL ESTATE
HARLESTONE ROAD, NORTHAMPTON NN5 7UZ

Registered No. 504862 England

Information Security Management System Policy

Standards

Belmont Press Limited is one of the UK's leading lithographic printing companies. Consistent standards for network access and authentication are critical to Belmont Press information security and are required by regulations or third-party agreements. Any user accessing the company's computer systems has the ability to affect the security of all users of the network.

Scope

The scope of this policy includes all users who have access to Belmont Press computers or require access to the network. This policy applies to employees, and anyone requiring access to the network. Public accesses to the company's external website or public web applications are excluded from this policy.

- ICT systems belonging to, or under the control of, Belmont Press Limited
- Information stored, or in use, or in hard copy physical form
- Information in transit across the data networks
- Control of information leaving Belmont Press Limited
- Information access resources
- All parties who have access to, or use of ICT systems and information belonging to, or under the control of, Belmont Press Limited

Application of this policy applies throughout the information lifecycle from acquisition / creation, through to utilisation, storage and disposal.

Objectives

The objective of information security is the business continuity of Belmont Press Limited and to minimise the risk of damage by preventing security incidents and reducing their potential impact. Please also see our Data Breach Notification Policy.

Policy

- The policy objective is to protect the organisations information assets against all internal, external, deliberate or accidental attacks.
- The security policy ensures the following:

  - Information will be protected against unauthorised access
  - Confidentiality of information is assured
  - Integrity of information is maintained
  - Availability of information for business purposes will be maintained
  - Legislative and regulatory requirements will be met
  - Business continuity plans will be developed, tested and maintained
  - Information security training will be available to all employees
  - All actual or suspected breaches of information security will be reported to the Information Security Manager and will be thoroughly investigated

- Procedures exist to support the policy, including virus control measures, passwords and continuity plans.
- Business requirements for availability of information and systems will be met
- The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementation
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the Information Security Policy is mandatory
- This policy will be reviewed at least annually to ensure applicability and compliance

Belmont Press Limited is recognised as an approved supplier to NAA, QCA and Government Departments for secure printing of Key Stage 1, 2 & 3 Level Examination Papers and confidential, restricted and classified documents.

We have documented operational procedures in place when producing this category of work.

Listed below are typical examples of the criteria that we have in place.

- Files are encrypted or the preferred use of a ShareFile system for security.
- Any files on disc are kept in a Data Safe when not being worked on.
- The disc is signed in and out at all stages.
- All data and jobs produced are backed-up at the end of each day and each week and are stored in a secure environment off-site
- Files are Password protected.
- Data can be anonymised after a given time, specified by the client, which is normally 3 months.

Our ICO Number is Z7860018

We are not certified to ISO 27001 at the moment but may look into it, if required, in the future. That said, we are fully compliant to The General Data Protection Regulation (GDPR) which came into force in May 2018. We rewrote several procedures and processes, and appointed 2 members of staff to act as DPO's after completion of a GDPR course. Please also see our GDPR Policy.

The following security measures are in place as a standard.

- Our premises have CCTV covering perimeter fences and all entrances and exits.
- CCTV is monitored and footage is archived.
- We have strong spiked metal perimeter fencing encompassing all sites.
- All premises have secure keypad entry on all entrances.
- Visitors are required to sign confidentiality forms at reception.
- Visitors are issued with security badges and are escorted at all times whilst on company premises.
- All forms of data storage including mobile telephones, cameras, laptop computers etc are required to be surrendered for safe keeping at reception.

Please also see our Data Processor Agreement, attached, should the need arise to use a sub-contractor.