Acanthus
50 years of fine printing

Acanthus Press Data Protection Policy

Our data protection policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal and customer data.

The Data Protection Act 1998 places obligations on organisations that use personal information and gives individuals certain rights.

The Act states that those who record and use personal information must be open about how the information is used and must follow the eight principles of ''good information handling''.

Under the Act every organisation (the data controller) that processes personal information (personal data) must notify the information Commissioner's Office, unless they are exempt. Failure to do so is a criminal offence.

Data controllers are required to inform the information Commissioner of certain details about their processing of personal information. The Commissioner uses these details to make an entry describing the processing in the register, which is available to the public at: **www.ico.gov.uk**

The main purpose of notification and the public register is to promote openness in the use of personal information.

Acanthus Press is registered under the data Protection Act

Data Controller Name: **Acanthus Press Limited**

Registration Number: **Z8575265**

We are a Tier 1 company for those employing less than 250 people.

We are committed to:

- ensuring that we comply with the eight data protection principles, as listed below
- meeting our legal obligations as laid down by the Data Protection Act 1998
- ensuring that data is collected and used fairly and lawfully
- processing personal data only in order to meet our operational needs or fulfill legal requirements
- taking steps to ensure that personal data is up to date and accurate
- establishing appropriate retention periods for personal data
- ensuring that data subjects' rights can be appropriately exercised
- providing adequate security measures to protect personal data
- ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- ensuring that all staff are made aware of good practice in data protection
- providing adequate training for all staff responsible for personal data
- ensuring that everyone handling personal data knows where to find further guidance
- ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly
- regularly reviewing data protection procedures and guidelines within the organisation

21 Ryelands Business Park, Bagley Road, Wellington TA21 9PZ
t: 01823 663339 **e:** roger@acanthuspress.ltd.uk **www.acanthuspress.ltd.uk**

Data protection principles

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

To All Staff

Your Personal Data

Personal data is information that identifies you. It can be anything from your name, address or telephone number to where you went to school or the things you buy.

We often need to use information about you with regard to company accounting (income, taxation and pensions), banking and social security.

The Data Protection Act (1998) governs how we collect, store, process and share your data.

Any person or organisation that uses personal information is known as a data controller. A data controller must comply with the eight principles of the data protection act. These ensure that personal information is:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than is necessary
- processed in line with your rights
- secure
- not transferred to other countries without adequate protection

Our data protection policy outlines our commitment to the data protection principles and how we deal with personal information.

We are required by law to share or make available some of the personal information we collect and hold. This information is shared to safeguard public funds and for the prevention and detection of fraud. For more details on this please read the fair processing notice.

The Information Commissioner's Office (ICO) oversees compliance with the data protection act. We have to tell the ICO about what we do with the personal information that we hold and this information is held on a register of data protectors.

Protecting Your Personal Information

Your personal information is important and you should treat it as you would any other valuable item.

With crimes like identity theft on the rise, it is important to always safeguard your personal information. Criminals can use your personal details to open bank accounts, apply for credit cards and apply for state benefits in your name.

You can take these simple steps to help safeguard your information:

- store any documents carrying any personal details in a safe place
- shred or destroy all documents containing any personal details before throwing them away
- ask the courier for advice on secure postage if you have to post any personal documents
- limit the number of documents containing personal details which you carry around on a daily basis.
- check your bank and credit card statements carefully for unfamiliar transactions.
- use different passwords and PINs for different accounts.
- be careful when using public computers to access your personal information.
- check your credit file regularly for any suspicious applications
- always think about who you are giving information to and why they would need it — be cautious!
- protect your home computer with anti-virus, firewall and anti-spam software before going online
- when you move house, redirect all your mail and inform your bank, utilities companies and other organisations of your new address.