Data Protection Policy

1. Introduction:

1.1 Yeomans Press Limited (The Company), company registration number 5306145, includes all trading names associated with it such as Yeomans Marketing.

1.2 The Company is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998, the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (The 'Act & Regulations').

1.3 The Company's business requires that it process certain information about individuals, both in using its own data sets and those of its clients and other third parties.

1.4 To comply with the Act & Regulations, the Company has to be open about how personal information is processed and must follow the principles of good information handling. This is a requirement in law and applies to all personal data for which the Company is the data controller and/or processor.

1.5 Personal data about individuals must be collected and used fairly, stored securely and not unlawfully disclosed; the data protection principles are summarised below.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation

of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

1.6 All staff, or any other person appointed by the Company to process personal data on its behalf, must ensure that they observe the data protection principles at all times.

2. Definitions

Personal Data

The GDPR applies to 'personal data', meaning any information relating to an identifiable living person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal Data:

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9 of the General Data Protection Regulation).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10 of the General Data Protection Regulation).

Data Controller:

Any person (an individual or legal person) who either alone or in common with other persons determines the purposes for which and the manner in which any personal data are to be processed. Most clients providing data for use by the Company are Data Controllers. The Company is also a Data Controller.

Data Processor:

In relation to personal data, means any person who processes the data on behalf of the data controller. The Company acts as Data Processor for many of its clients.

Data Subject:

A living individual who is the subject of personal data.

Processing:

In relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

Third Party:

In relation to personal data, means any person other than a) the data subject b) the data controller or c) the data processor or other person authorised to process data on behalf of the data controller.

Relevant Filing System

Any paper filing system or other manual filing system which is structured in such a way that information about an individual is readily accessible.

3. Authority

3.1 This document was adopted as a policy on Monday 2nd February 2009 and is effective as of that date. The policy was updated on 1st May 2018.

3.2 The policy will be subject to review at not less than two-yearly intervals.

3.3 A breach in the Company's Data Protection policy can result in disciplinary action.

4. Roles:

Data Protection Officer:

The Company's Data Protection Officer is responsible for drawing up guidance for best practice and for promoting policy compliance.

Senior Managers & Directors:

Senior Managers and Directors have a responsibility to ensure that data protection issues within their areas are managed in a way that meets the provisions of the Company's data protection policy.

5. Responsibilites:

5.1 Compliance with the provisions of the Act is the responsibility of all members of the Company's staff or employ who process personal data.

6. Confidentiality, Storage & Data Security:

6.1 The confidentiality of all personal data, either as Data Controller or Data Processor is a matter that the Company takes very seriously. The Company will ensure all reasonable steps are taken to comply with the principles of the Data Protection Act 1998 and the General Data Protection Regulation.

6.2 Personal data will be kept securely and access will only be permitted by authorised personnel.

6.3 Third party data upon which the Company is acting as Data Processor will be kept suitably safe as to comply with the principles of the Data Protection Act 1998 and the General Data Protection Regulation.

6.4 All staff or employ are responsible for ensuring that any personal data they hold or have been charged with responsibility for (in the role of data processor) is always maintained securely and not disclosed to any unauthorised third party.

6.5 All data storage systems will be at least password protected. Rights of access will only be granted to those persons with a legitimate need to process the data.

6.6 Any manual storage systems will not be left where they can be accessed by unauthorised personnel.

6.7 All staff should take the greatest care to ensure that personal data is not disclosed either orally or in writing to any unauthorised third party.

6.8 Staff should note that unauthorised or unlawful processing of personal data is a disciplinary matter, and in some cases may be considered as gross misconduct.

6.9 Data should not be kept for longer than is necessary for the purpose for which it was collected. In the instance of data where the Company is acting as Data Processor the data will be stored for a maximum of six months. This period is determined as the time in which clients can make a query in regard to the use of the data and the Company shall retain the data for checking purposes. Following six calendar months the data and all associated articles will be removed from all data storage systems. Emails will be kept for a maximum of 2 years. Where possible data should be securely transferred to The Company via an alternative means e.g. FTP transfer or other file sharing software.

6.10 Any Data Controller can request in writing that their data be kept for longer than the period as set out in section 6.9. This application should be made to the Data Protection Officer and should in all cases be reviewed on an annual basis.

6.11 Where the Data Controller is renting the data to a third party or client of the Company and the Company is entrusted with the data for a specific purpose or purposes extra care will be taken to ensure that the third party or client cannot obtain access to the data without the Data Controllers express permission.

7. Suppression

7.1 The Company shall recommend where appropriate the cleansing of databases obtained by Data Controllers to ensure that data subjects are protected from mis-use of the data. In particular the screening of data against the relevant Preference Service (MPS, FPS, TPS) the removal of individuals classed as “goneaway” and those persons notified as deceased.

7.2 An individual or organisation may contact the Company to ask for corrections to their information or removal from databases. This request should be acted upon within 60 days of receipt of the request.

7.3 In the instance on point 7.2 where the Company is acting as Data Processor the Data Controller will be notified in writing not more than 45 days from receipt of the request.

8. Data Collection

8.1 Where the Company is acting as data collector or has been asked to retrieve or collate data from a data collection source the Company shall make all reasonable efforts as to ensure itself that the data has been collected lawfully.

8.2 Any physical form on which data has been collected should bear a clear and prominent data protection statement explaining the purpose for which the collected data will be used and to whom the data may be disclosed.

8.3 Where collected data is to be used by third parties the Company shall advise the collector on best practice. Best practice advises that individuals shall be required to opt-in to allow data sharing.

9. Profiling

9.1 We may from time to time check the accuracy of personal data supplied to us by referring to third party information sources e.g. the Royal Mail PAF file.

9.2 We may also analyse the personal information you supplied to us alongside publicly available information to create a profile to better understand your interests, preferences and the appropriate opportunities to offer you. This is known in law as ‘profiling’. We may share your personal information with third parties to do this.

10. The Right to Access Personal Data:

10.1 The General Data Protection Regulation gives individuals who are subject of personal data a general right of access to personal data that relates directly to them. Consequently, under the provisions of the Act, a data subject can ask the Company to provide him/her with any information that relates directly to them as an individual.

10.2 This information will be provided free of charge unless the request is manifestly unfounded or excessive, particularly if repetitive, in which case the fee for supply will be £50. Multiple applications for the same information will also incur the £50 fee.

10.3 Subject access requests will be supplied within 28 days of receipt of the initial request unless the request is complex or numerous in which case the information shall be supplied within 90 days of the initial request with a notice to say that the request will take longer than the initial period sent within the first 28 days following receipt of the request.

10.4 All data subject access requests must be in writing and must contain supporting documentation as to proof of identity. All documents will be returned to the applicant along with the information requested.

10.5 All requests should be addressed to:

The Data Protection Officer
Yeomans Press Ltd
Unit 12 Branbridges Industrial Estate
Branbridges Road
East Peckham
TONBRIDGE
TN12 5HF

11. The right to be forgotten

11.1 The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as “the right to be forgotten”. Individuals can make a request verbally or in writing. The Company will respond to a request within 28 days. The right is not absolute. The Company will be required to take appropriate measures to ascertain the validity of the claim.

12 Accountability

12.1 The Company shall keep a detailed record of processing operations.