JOHN MOORE HERITAGE SERVICES

Data Protection Policy Statement

John Moore Heritage Services is fully committed to compliance with the requirements of the General Data Protection Regulation 2018 (GDPR), which came into force on the 25th of May 2018. JMHS will therefore follow procedures that aim to ensure that all employees, contractors, consultants at JMHS who have access to any personal data held by or on behalf of JMHS, are fully aware of and abide by their duties and responsibilities under the Act.

In order to operate efficiently, JMHS has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the GDPR to ensure this.

JMHS regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between JMHS and those with whom it carries out business. The company will ensure that it treats personal information lawfully and correctly.

To this JMHS fully endorses and adheres to the principles of data protection as set out in the General Data Protection Regulation. The GDPR stipulates that anyone processing personal data must comply with the following principles:

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
g) accidental loss, destruction or damage, using appropriate technical or organisational measures.

PASTURE FARMHOUSE, BOARSTALL
AYLESBURY HP18 9UR
TELEPHONE 01865 358300
Email: info@jmheritageservices.co.uk
John Moore Heritage Services Ltd
Registered in England and Wales No. 10019494

The GDPR provides conditions for the processing of any personal data. It also makes a distinction between personal data and sensitive personal data.

Personal Data
The GDPR applies to 'personal data' meaning any information relating to an identifiable 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).

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).

JMHS will, through appropriate management and the use of strict criteria and controls, ensure that:

- the Company observes fully the conditions regarding the fair collection and use of personal information
- the Company has a valid lawful basis in order to process personal data
- that such lawful basis is correctly documented
- the data processing is exclusively carried out when necessary
- the collection and processing of information is restricted to appropriate data and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- additional conditions are identified for processing special category data
- a request for consent is issued when that is the most appropriate lawful basis for processing
- strict checks are applied to determine the length of time information is held
- appropriate technical and organisational security measures are taken to safeguard personal information
- certain types of personal data breach as specified in the GDPR are reported to the relevant supervisory authority

JMHS will ensure that the following rights of people about whom the information is held can be fully exercised under the GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure

- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

In addition, JMHS will ensure that:

- there is someone with specific responsibility for data protection in the organisation
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- everyone managing and handling personal information is appropriately supervised;
- anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, is aware of the correct procedure
- enquiries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are regularly assessed and evaluated
- performance with handling personal information is regularly assessed and evaluated
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures

All contractors and consultants must:

- ensure that they and all of their staff who have access to personal data held or processed for or on behalf of JMHS, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the GDPR. Any breach of any provision of the GDPR will be deemed as being a breach of any contract between JMHS and that individual, company, partner or firm
- allow data protection audits by JMHS of data held on its behalf (if requested)
- indemnify JMHS against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation
- confirm that they will abide by the requirements of the GDPR with regard to information supplied by JMHS

JMHS's employees training
All Staff are to be made fully aware of this policy and of their duties and responsibilities under the GDPR. All Senior Staff (Director and Managers) will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- paper files and other records or documents containing personal/sensitive data are kept in a secure environment, in the Director's office, at a location separate from the Company's main office
- digital files containing personal data are held on the Director's computer, which is password protected and only accessible by Management
- individual passwords are issued to staff for access to the Company's server, in order to track and monitor access to non-sensitive data

JMHS will take steps to ensure that all employees that handle personal information of individuals will be trained to:

- Identify the different categories of data
- Understand the 6 principles of GDPR
- Understand the lawful basis for processing data under GDPR
- Understand the individual's 8 rights

- Contact the appropriate person regarding data protection queries within the Company
- Process a Subject Access Request
- Handle a data breach situation

The Director will be responsible for ensuring that the Policy is implemented.

The General Data Protection Regulation requires every data controller who is processing personal data, to notify and renew their notification. Failure to do so is a criminal offence. To this end the Director will be responsible for the processing of personal data.

Last Revised: 03/04/2019

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

DATA PROTECTION BILL
https://publications.parliament.uk/pa/bills/lbill/2017-2019/0074/18074.pdf