Data Protection Policy

VERSION: December 2022

INTRODUCTION

This policy gives important information about the data protection principles with which Mortgage and Surveying Services Limited and its group companies (referred to in this policy as the **'Company'**) must comply.

The Company obtains, keeps and uses personal information (also referred to as data) about job applicants, current and former employees, temporary and agency workers, contractors, interns, volunteers, apprentices, customers, clients, contractors, individuals interested in our business, and business associates for a number of specific lawful purposes. The Company may also share personal data with other organisations that carry out services for the Company.

This policy sets out how we comply with our data protection obligations under the Data Protection Act 2018 and the General Data Protection Regulation (UK GDPR) and seek to protect personal information. All personnel of the Company must comply with this policy when processing personal information.

We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information, and how (and when) we delete that information once it is no longer required.

SCOPE

This policy applies to the personal information (including special category personal data) processed by the Company and its third party suppliers.

We will review and update this policy regularly in accordance with our data protection obligations. It does not form part of any employee's contract of employment or with any other contractual agreement with any person and we may amend, update or supplement in from time to time.

DEFINITIONS

Controller: means the individual, organisation or other body that decides when, how and why personal data will be processed;

Criminal records information: means personal information relating to criminal convictions and offences, allegations, proceedings and related security measures;

Data breach: means a breach of security leading the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;

Data Subject: means an individual to whom the personal information relates;

Personal information: (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

Processor: means the individual , organisation or other body that processes personal data on behalf of a Controller.

Processing information: means obtaining, recording. Organising, storing, amending, retrieving, disclosing and/or destroying information, or suing or doing anything with it; and

Special category personal information: (known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

DATA PROTECTION PRINCIPLES

The Company will comply with the following data protection principles when processing personal information:

- we will process personal information lawfully, fairly and in a transparent manner
- we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes
- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay
- we will keep personal information for no longer than is necessary for the purposes for which the information is processed
- we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage

BASIS FOR PROCESSING PERSONAL INFORMATION

In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e
    - that the data subject has consented to the processing; or
    - that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
    - that the processing is necessary for compliance with a legal obligation to which The Company is subject; or
    - that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
    - that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
    - that the processing is necessary for the purposes of legitimate interests of The Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject

- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose)
- document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles
- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s)
- where special category personal information is processed, also identify a lawful special condition for processing that information and document it

- where criminal records information is processed, also identify a lawful condition for processing that information, and document it

When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

- conduct a legitimate interest's assessment (LIA) and keep a record of it, to ensure that we can justify our decision
- if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA)
- keep the LIA under review, and repeat it if circumstances change
- include information about our legitimate interests in our relevant privacy notice(s)

SPECIAL CATEGORY PERSONAL INFORMATION

The Company may from time to time need to process special category personal information. We will only process special category personal information if:

- we have a lawful basis for doing so as set out in paragraphs above
- one of the special conditions for processing special category personal information applies:
    - the data subject has given explicit consent
    - the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject
    - the processing is necessary to protect the data subject's vital interests
    - the data subject is physically incapable of giving consent
    - processing relates to personal data which are manifestly made public by the data subject
    - the processing is necessary for the establishment, exercise or defence of legal claims
    - the processing is necessary for reasons of substantial public interest

Before processing any special category personal information, staff must notify compliance@mssl.co.uk of the proposed processing, in order that the Compliance Team may assess whether the processing complies with the criteria noted above.

Special category personal information will not be processed until:

- the assessment referred to above has taken place and the Company has determined that it can process special category personal information legitimately
- unless an exemption applies, the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it, in accordance with the requirements of data protection law
- The Company will not carry out automated decision-making (including profiling) based on any individual's special category personal information
- The Company's relevant data protection privacy notice will set out the types of special category personal information that the Company processes, what it is used for and the lawful basis for the processing

CRIMINAL RECORDS INFORMATION

Criminal records information will be processed in accordance with the Company's Criminal Records Information Policy.

DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

DPIAs are a tool to help the Company identify and minimise the data protection risks of new projects. They are part of our accountability obligations and an integral part of "data protection by default and by design" approach. Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risk to individuals
- what measures can be put in place to address those risk and protect personal information

DOCUMENTATION AND RECORDS

We will keep written records of processing activities including:

- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- where possible, retention schedules
- where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document:

- information required for privacy notices
- records of consent if necessary
- controller-processor contracts
- the location of personal information
- DPIAs
- records of data breaches

If we process special category personal information or criminal records information, we will keep written records of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose
- the lawful basis for our processing
- the condition on which that processing is undertaking
- whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy

We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

- carrying out information audits to update what personal information the Company holds
- distributing questionnaires and talking to staff across the Company to get a more complete picture of our processing activities
- reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing
- We document our processing activities in electronic form, so we can add, remove and amend information easily

PRIVACY NOTICES

The Company will issue privacy notices from time to time, including 'just in time notices', informing individuals about the personal information that we collect relating to them, how they can expect their personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

INDIVIDUAL RIGHTS

Individuals have the following rights in relation to their personal information:

- **Right to be informed** about how, why and on what basis that information is processed
- **Right of access** to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request
- **Right of rectification** to have data corrected if it is inaccurate or incomplete
- **Right of erasure** to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- **Right to restrict the processing** of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the Company no longer needs the personal information, but they require the data to establish, exercise or defend a legal claim
- **Right to restrict the processing of personal information temporarily** where they do not think it is accurate (and the Company is verifying whether it is accurate), or where they have objected to the processing (and the Company is considering whether the organisation's legitimate grounds override their interests)
- **Right to data portability** by allowing individuals to obtain and reuse their personal data for their own purposes across different services. This right only applies to information understand their spending habits. The right only applies to information an individual has provided to a controller
- **Right to object** individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes
- **Rights in relation to automated decision making and profiling.** UK GDPR has additional rules to protect individuals if a Processor is carrying out solely automated decision-making that has legal or similarly significant effects on them

The Company trains all staff on how to respond to requests to exercise the above rights and has processes in place to ensure such requests are dealt with. If the Company is not the data controller of the data to which the right relates the Company will usually contact the data controller regarding the request before responding (depending upon the requirements set out in the contractual arrangement between the Company and the controller).

Staff should contact the Compliance Team if they receive a request from a data subject (whether written of verbally).

EMPLOYEE OBLIGATIONS

The Company expects its employees to help meet its data protection obligations to individuals.

If employees have access to personal information, they must:

- only access the personal information that they have authority to access, and only for authorised purposes
- only allow other members of staff to access personal information if they have appropriate authorisation; only allow individuals who are not our staff to access personal information if they have specific authority to do so from the Compliance Team
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's Data Protection Breach Policy)
- not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on personal devices that are used for work purposes

Staff are trained to contact the Compliance Team if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of special category personal information, without one of the conditions in the above paragraph being met
- any data breach as set out below
- access to personal information without the proper authorisation
- personal information not kept or deleted securely
- removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures being in place
- any other breach of this policy or of any of the data protection principles set out above

In the event of such a report, the Company will fully investigate and rectify the situation.

INFORMATION SECURITY

The Company will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- making sure that, where possible, personal information is encrypted
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Where the Company uses external organisations to process personal information on its behalf, additional security arrangements will be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations provide that:

- the organisation may act only on the written instructions of the Company
- those processing the data are subject to a duty of confidence
- appropriate measures are taken to ensure the security of processing

- sub-contractors are only engaged with the prior consent of the Company and under a written contract
- the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will assist the Company in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments
- the organisation will delete or return all personal information to the Company as requested at the end of the contract unless legally required to keep the data
- the organisation will submit to audits and inspections, provide the Company with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Company immediately if it is asked to do something infringing data protection law

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Compliance Team.

STORAGE AND RETENTION OF PERSONAL INFORMATION

Personal information (and special category personal information) will be kept securely in accordance with the Company's Information Security and Data Protection Breach Policy.

Personal information (and special category personal information) will not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff follow the Company's Record Management Policy which sets out the relevant retention period, and the criteria that should be used to determine the retention period.

Personal information (and special category information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

DATA BREACHES

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored
- unauthorised success to or use of personal information either by a member of staff or third party; loss of data resulting from an equipment or systems (including hardware and software) failure
- human error, such as accidental deletion or alteration of data
- unforeseen circumstances, such as a fire or flood
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it

The Company will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals
- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law unless is not the Data Controller, in which case The Company shall report the breach as soon as possible to the relevant Data Controller

INTERNATIONAL TRANSFERS

The Company will not transfer personal information outside the UK unless appropriate safeguards are in place.

TRAINING

The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

The Company keep a log of all employee data protection training and testing to ensure that all staff have competent knowledge of data protection requirements.

CONSEQUENCES OF EMPLOYEES FAILING TO COMPLY

The Company takes compliance with this policy very seriously. Failure to comply may result in disciplinary action against our employees, including dismissal. Employees are informed about the importance of maintaining data protection compliance at all times and are informed that if they fail to do so they could be subject to disciplinary action, including dismissal.

FURTHER INFORMATION

The Compliance Team is responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies.

If you have any questions or comments about the content of this policy or if you need further information, you should contact compliance@mssl.co.uk.

POLICY SIGN OFF

Date of Issue:	20/12/2022
Date of Next Review:	20/12/2024
Name:	Vicky Wallis – Head of Facilities & Compliance
Signed:	V Wallis

AMENDMENT HISTORY

Version	Modified On	Modified By	Comments
1.0	12/10/2020	Parmjit Samplay	
2.0	13/10/2020	Parmjit Samplay	Included company logo and signoff info
3.0	20/10/2020	Parmjit Samplay	Updated next review date
4.0	03/08/2021	Parmjit Samplay	Reviewed Policy - no changes are required
5.0	04/08/2021	Parmjit Samplay	Next review date amended: 15/08/23
6.0	20/12/2022	Sarah Tuck	Updated owner, updated content (lawyer approved) and updated review date 20/12/2022