GDPR DATA PROTECTION POLICY

1. INTRODUCTION AND PRIVACY STATEMENT

D&M Building Services Ltd (D&M) needs to gather and use certain information about individuals in order to carry out its functions. These can include customers, employees, contractors, business contacts and other people the organisation has a relationship with. In addition, D&M may be required by law to collect and use information in order to comply with the requirements of local and central government.
This personal information must be handled and dealt with properly however it is collected, recorded and used, whether it is on paper, in computer records or recorded by other means. D&M regards the lawful and appropriate treatment of personal information as very important to its successful operations and essential to maintaining confidence between the company and those with whom it carries out business. D&M fully endorses and adheres to the principles of data protection legislation.
Your information will be used to provide you with information and services that you request from us an, and for other legitimate business purposes. We may offer you the opportunity to opt in to receiving additional information about our activities or those of our partners and service providers. You may opt out of this at any time by contacting us.
Occasionally, we conduct surveys to evaluate the impact of our policies and services. The results of these surveys will be used solely for evaluation purposes.

2. POLICY STATEMENT

This policy describes how this information must be collected, handled and stored to meet the company's data protection standards, and to comply with the law.
This policy applies to all D&M suppliers, contractors and staff (including Directors), and to all data that the company holds relating to identifiable, living individuals, even if that information technically falls outside of data protection legislation.
Data protection legislation describes how companies such as D&M must collect, handle and store personal and sensitive information. These rules apply whether the information is stored electronically, on paper or on other materials.

3. DEFINITIONS

Some helpful definitions are set out below to assist in your understanding of this Policy:
Personal data: means information about a living person who can be identified by that information or by that information together with other information that the Data Controller has or is likely to obtain. This is information that relates to an identifiable living individual, whether in personal, family or business life.

Sensitive Personal Data: means certain personal data that is given special status in data protection legislation. Sensitive personal data is personal data consisting of information as to:
- racial or ethnic origin.
- political opinions.
- religious beliefs (or other beliefs of a similar nature).
- trade union membership.
- physical or mental health condition.
- sexual life.
- Medical information.

- commission or the alleged commission of an offence.
- proceedings for any offence, the disposal of such proceedings or the sentence of any Court in such proceedings.

Sensitive Personal data can only be collected and processed with that individual's express consent, which would generally require the consent to be written.

Processing: means using information in any way.

Data Controller: means a company who decides the purposes for which and the way in which personal data is processed. D&M are the Data Controller in respect of staff and customer's personal and sensitive data.

Data Subject: means all staff and customers of D&M.

Subject Access Request: means a request made by or on behalf of an individual for the information held about an individual.

4. RESPONSIBILITIES

All staff are responsible for protecting information located across the company and contained in different file formats and stored on physical devices by ensuring that information is collected, stored and handled appropriately.
Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.
Responsibility for ensuring the effective communication, implementation and operation of this Policy rests with the Managing Director of D&M who will be responsible for taking action where there is evidence of a breach of this policy and for ensuring that records are kept in accordance with the principles of this policy.
Helen Llewellyn, Data Protection Officer for D&M, is responsible for:
- Notifying the Information Commissioner's Office.
- Acting as a liaison point for the Information Commissioner's Office
- Keeping the Board updated about data protection responsibilities, risks and issues.
- Processing Subject Access Requests.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Reviewing this policy in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

5. STATUTORY OBLIGATIONS

In dealing with personal information D&M will fully comply with the terms of the relevant legislation as follows:
- General Data Protection Regulation (EU) 2016/679
- Data Protection Act 2018

- Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Housing Act 1985
- The Social Security Administration (Fraud) Act 1997
- European Directives
- Tenants' Guarantee
- Health & Safety Regulations
- Regulation of Investigatory Powers Act 2000 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
- Equality Act 2010

D&M will also consider best practice in the implementation of this policy.
D&M is not subject to the Freedom of Information (FoI) Act and there is no statutory obligation for us to respond to FoI requests. We endeavor to provide requested information where we can and where it is readily available

6. DATA USE AND SECURITY

How we handle information is very important. Our clients / customers have entrusted their information with us, and if we were to misuse or lose personal information it could cause serious harm or distress to people. Confidential and sensitive information needs to be kept secure, but it also needs to be available when required. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.
The need to ensure that personal data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.
All staff should ensure that:

- Any personal data which they hold is kept securely.
- Identity checks are carried out before giving out personal information.
- Data is held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Data is regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Data is not shared informally. When access to confidential information is required, employees can request it from their line managers.
- Personal data is not disclosed either orally or in writing, intentionally or otherwise to any unauthorised third party.
- Where personal data is processed by a third party on behalf of D&M, there is a written contract between the parties which specifies that the data processor agrees to act on D&M's instructions only, and to abide by the provisions of data protection legislation in connection with data security. A *Data Sharing Protocol* is attached at *Appendix 6.*

- All personal information in the form of manual records should be:
- Kept in a locked filing cabinet or
- Kept in a locked drawer
- Care must be taken to ensure that manual records or printouts containing personal data are not left where they can be accessed by unauthorised staff.
- Manual records, or printouts containing personal data that are no longer required are shredded or bagged and disposed of securely.
- Identifiable images are not used nor personal data uploaded online without the express consent of the individual.
- Personal data is not sent in the body of an email as this form of communication is not secure. Personal data may be attached within an email so long as the attachment is password protected.
- Data is protected by strong passwords that are changed regularly and never shared between employees.
- Data stored on removable media (like a CD or DVD) is kept locked away securely when not being used.

- Data is stored only on designated drives, servers and devices, and should only be uploaded to an approved cloud computing services.
- Data is encrypted before being transferred electronically - the IT team can explain how to send data to authorised external contacts.
- Screens for computers and other devices are always locked when left unattended.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Assistance is sought from the Data Protection Officer if they are unsure about any aspect of data protection.

Staff working outside of the companies' business premises should take care to avoid extra risks by not discussing sensitive information publically or where it can be overheard, and should be careful about accidentally disclosing data when handling devices in the presence of other people.
All possible steps will be taken to maintain effective security for the whole of the computer system. Access to information stored on computer systems and devices should be appropriately password protected. Staff must take all necessary steps to avoid careless loss of data, particularly when working remotely.
A *staff checklist* is included at *Appendix 1* to act as a guide for staff.
A *document retention schedule*, informed by National Housing Federation guidelines, is attached at *Appendix 3* to ensure the company complies with the fifth principle.
Cross-Border Data Transfers
Staff must take special care in connection with requests for the transfer of personal data out of the European Economic Area (EEA). If you are in any doubt, please contact the Data Protection Officer.

7. TRAINING

All staff are required to attend data protection training to help them understand their responsibilities when handling data. Staff are expected to attend Data Protection Awareness training as part of their 6-month induction process; this will be conducted when there are sufficient numbers to make the training viable.
Staff who have not received this training must contact Helen Llewellyn to book a place on the next available training session.

8. BREACHES

It is the responsibility of all staff (including Directors) to comply with this policy, and to understand their obligation to ensure that they have regard to the eight data protection principles above when accessing, processing or disposing of personal information.
Failure to observe the data protection principles within this policy may result in staff incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if employment records are accessed without the requisite authority, the organisation will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.
In addition, a failure to comply with this policy could expose the business to enforcement action by the Information Commissioner. This could result in restrictions being imposed on our use of personal data, fines of up to €10 million), or complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.
Where an individual suffers damage or loss because of unauthorised disclosure, inaccurate or missing data, or the loss or destruction of data in relation to him/her, he/she may seek compensation from the courts.
For these reasons, it is important that all staff familiarise themselves with this policy.
Any breach and/or potential breach of data protection legislation must be reported immediately to your Head of Service. If staff are concerned about reporting a breach or potential breach then they are able to do this under the Whistle Blowing Policy which is available on the Intranet.
Always report lost or missing information immediately as the cost of hiding or ignoring a loss can be far worse.

9. SURVEILLANCE AND MONITORING

D&M has a legitimate interest in monitoring the behavior of staff and customers who attend offices. For instance, D&M may wish to carry out monitoring in order to prevent inappropriate behavior or to prevent or detect any unlawful act.
Monitoring can take several forms. It can involve e-mail and Internet monitoring, telephone monitoring or monitoring by way of vehicle tracking & CCTV.
In carrying out such monitoring the Association uses CCTV cameras in what are considered to be "public" areas of the workplace. Generally, the use of such CCTV cameras is notified by using suitable signage at obvious places at the entrance to the monitored areas; however, (even in the absence of such signage) staff and customers should be aware that public space within D&M's business premises may be monitored in this way.
D&M may involve the police in such monitoring where specific criminal activity has been identified.
D&M holds information on the destination and duration of calls made from the companies' telephone system, and from the use of other IT systems and devices. D&M may use this information if misuse is suspected.
In operating this policy individuals must comply with the requirements laid down in D&M's Internet Usage and Monitoring and reporting Policy.

10. SUBJECT ACCESS REQUEST

All individuals who are the subject of personal data held by D&M are entitled to ask what information the company holds about them and why, how to gain access to this information, be advised how the information is kept up to date and be advised how the Association is meeting its data protection obligations.
If an individual contacts D&M requesting this information, this is called a subject access request.
Subject access requests from individuals can be made verbally or in writing. For convenience, a Subject Access Request Form is available at Appendix 2, but there is no obligation for individuals to use this form.
Subject Access Requests should be passed immediately to the Data Protection Officer or in their absence to the relevant Director or Executive Director.
The Data Protection Officer will always verify the identity of anyone making a subject access request before handing over any information.
Where the provision of information would reveal the identity of a third party, the information may not be provided unless either the consent of that third party is obtained, or the information relating to them can be redacted so as to ensure their identify is not revealed.
Confidential and personal information cannot normally be disclosed to an unauthorised third party, unless a '*consent to disclose*' form (*Appendix 4*) has been received and verified.
In certain circumstances, data protection legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances D&M will disclose requested data. However, the Data Protection Officer will ensure the request is legitimate.

11. MONITORING

The managing director will ensure that monitoring is in place to assess the effectiveness of the Policy and its implementation
This will involve routine checks in respect of access authorisation levels, compliance with security in collecting, handling and storing records and collecting data, analysis and reporting, where necessary, on number of grievances and actions taken to deal with any breach of this policy.

12. REVIEW

The Policy will be reviewed regularly and in any event at no more than two-yearly intervals.
Complaints: D&M recognises the importance of listening to, and dealing positively with, complaints about its services. Any complaints received in relation to D&M's handling of data will be dealt with in accordance with D&M's Complaints Policy.

Equal Opportunities and Diversity: In operating this policy D&M will comply with the requirements laid down in D&M's Equality and Diversity Policy.

13. APPENDICES

APPENDIX 1: Staff Checklist
APPENDIX 2: Subject Access Request form
APPENDIX 3: Retention Schedule
APPENDIX 4: Consent to Disclose form
APPENDIX 5: Request For Data form
APPENDIX 6: Data Sharing Protocol

Yours faithfully,

Mr. David Llewellyn
Director