Millennium Point Group

Data Protection Policy v1.5

1. Aim and scope of policy

1.1 Millennium Point Property Limited (**Millennium Point**) is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our staff, workers, directors and consultants ("**Workers**").

1.2 This Data Protection Policy ("**Policy**") sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect.

1.3 This Policy applies to all companies in our Group of companies. References in this Policy to "us", "we" and "our" are to Millennium Point Property Limited.

1.4 We recognise that you have an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy and to apply and implement its requirements when processing any personal data.

1.5 Data protection law is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. This Policy also sets out the consequences of failing to comply with these legal requirements. However, this Policy is not an exhaustive statement of data protection law nor of our or your responsibilities in relation to data protection.

1.6 If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact your line manager or Vanessa Currie, GDPR Compliance Manager.

2. Who is responsible for data protection?

2.1 All our Workers are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

2.2 We are not required to appoint a Data Protection Officer. However, we have still appointed Vanessa Currie responsible for overseeing our compliance with data protection laws and they have the title of GDPR Compliance Manager.

3. Why do we have a data protection policy?

3.1 We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting relationships with those individuals and trust in our brand. We believe that such relationships will enable our organisation to work more effectively with and to provide a better service to those individuals.

3.2 This Policy works in conjunction with other policies implemented by us from time to time and any other policies we implement from time to time.

4. **Status of this Policy and the implications of breach.**

4.1 Any breaches of this Policy will be viewed very seriously. All Workers must read this Policy carefully and make sure they are familiar with it. Breaching this Policy is a disciplinary offence and will be dealt with under our Disciplinary Procedure.

4.2 If you do not comply with Data Protection Laws and/or this Policy, then you are encouraged to report this fact immediately to the GDPR Compliance Manager. This self-reporting will be taken into account in assessing how to deal with any breach, including any non-compliances, which may pre-date this Policy coming into force.

4.3 Also, if you are aware of or believe that any other representative of ours is not complying with Data Protection Laws and/or this Policy you should report it in confidence to the GDPR Compliance Manager.

5. **Other consequences**

5.1 There are a number of serious consequences for both yourself and us if we do not comply with Data Protection Laws. These include:

5.1.1 For you:

5.1.1.1 **Disciplinary action:** Your terms require you to comply with our policies. Failure to do so could lead to disciplinary action including dismissal.

5.1.1.2 **Criminal sanctions:** Serious breaches could potentially result in criminal liability.

5.1.1.3 **Investigations and interviews**: Your actions could be investigated and you could be interviewed in relation to any non-compliance.

5.1.2 For the organisation:

5.1.2.1 **Criminal sanctions:** Non-compliance could involve a criminal offence.

5.1.2.2 **Civil Fines:** These can be up to £17.5 million or 4% of group worldwide turnover whichever is higher.

5.1.2.3 **Assessments, investigations and enforcement action**: We could be assessed or investigated by, and obliged to provide information to, the Information Commissioner on its processes and procedures and/or subject to the Information Commissioner's powers of entry, inspection and seizure causing disruption and embarrassment.

5.1.2.4 **Court orders:** These may require us to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

5.1.2.5 **Claims for compensation:** Individuals may make claims for damage they have suffered because of our non-compliance.

5.1.2.6 **Bad publicity:** Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner

quickly become public knowledge and might damage our brand. Court proceedings are public knowledge.

5.1.2.7 **Loss of business:** Prospective customers, customers, suppliers and contractors might not want to deal with us if we are viewed as careless with personal data and disregarding our legal obligations.

5.1.2.8 **Use of management time and resources:** Dealing with assessments, investigations, enforcement action, complaints, claims, etc takes time and effort and can involve considerable cost.

6. **Data protection laws**

6.1 The UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 ("**DPA 2018**") apply to any personal data we process (together "**Data Protection Laws**").

6.2 The provisions of the EU GDPR were incorporated directly into UK law at the end of the transition period. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context.

6.3 The Data Protection Laws all require that the personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

7. **Key words in relation to data protection**

7.1 **Personal data** is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into our possession). That living individual might be an employee, customer, prospective customer, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV).

7.2 **Identifiable** means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. if a name or video footage) or might do if taken together with other information available to or obtainable us (e.g. a job title and company name).

7.3 **Data subject** is the living individual to whom the relevant personal data relates.

7.4 **Processing** is widely defined under data protection law and generally any action taken by us in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

7.5 **Controller** is the person who decides how personal data is used, for example, we will always be a controller in respect of personal data relating to our employees.

7.6 **Processor** is a person who processes personal data on behalf of a controller and only processes that personal data in accordance with instructions from the controller, for example, an outsourced payroll provider will be a processor.

8. **Personal data**

8.1 Data will relate to an individual and therefore be their personal data if it:

8.1.1 identifies the individual. For instance, names, addresses, telephone numbers and email addresses;

8.1.2 its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;

8.1.3 relates to property of the individual, for example their home, their car or other possessions;

8.1.4 it could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you are able to link the data to the individual to tell you something about them, this will relate to the individual (e.g. salary details for a post where there is only one named individual in that post, or a telephone bill for the occupier of a property where there is only one occupant);

8.1.5 is biographical in a significant sense that is it does more than record the individual's connection with or involvement in a matter or event, which has no personal connotations for them. For instance, if an individual's name appears on a list of attendees of an organisation meeting this may not relate to the individual and may be more likely to relate to the company they represent;

8.1.6 has the individual as its focus, that is, the information relates to the individual personally rather than to some other person or a transaction or event he/she was involved in. For instance, if a work meeting is to discuss the individual's performance this is likely to relate to the individual;

8.1.7 affects the individual's privacy, whether in their personal, family, organisation or professional capacity, for instance, email address or location and work email addresses can also be personal data;

8.1.8 is an expression of opinion about the individual; or

8.1.9 is an indication of our (or any other person's) intentions towards the individual (e.g. how a complaint by that individual will be dealt with).

8.2 Information about companies or other legal persons who are not living individuals is not personal data. However, information about directors, shareholders, officers and employees, and about sole traders or partners, is often personal data, so business related information can often be personal data.

8.3 Examples of information likely to constitute personal data:

8.3.1 Unique names;

8.3.2 Names together with email addresses or other contact details;

8.3.3 Job title and employer (if there is only one person in the position);

8.3.4 Information about individuals obtained as a result of Anti Money Laundering checks or credit checks;

8.3.5 Customer profile information (e.g. preferences); and

8.3.6 Financial information and accounts (e.g. information about tax liabilities, income, expenditure, credit history).

9. **Lawful basis for processing**

9.1 For personal data to be processed lawfully, we must be process it on one of the legal grounds set out in the Data Protection Laws.

9.2 For the processing of ordinary personal data in our organisation these may include, among other things:

9.2.1 the data subject has given their consent to the processing;

9.2.2 the processing is necessary for the performance of a contract with the data subject;

9.2.3 the processing is necessary for the compliance with at legal obligation to which the controller is subject; or

9.2.4 the processing is necessary the legitimate interest reasons of the controller or a third party.

10. **Special category data**

10.1 Special category data under the Data Protection Laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data.

10.2 Under Data Protection Laws, this type of information is known as special category data and criminal records history becomes its own special category, which is, treated for some parts the same as special category data. Previously these types of personal data were referred to as sensitive personal data and some people may continue to use this term.

10.3 To lawfully process special categories of personal data we must also ensure that either the individual has given their explicit consent to the processing or that another of the following conditions has been met:

10.3.1 the processing is necessary for the performance of our obligations under employment law;

10.3.2 the processing is necessary to protect the vital interests of the data subject. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;

10.3.3 the processing relates to information manifestly made public by the data subject;

10.3.4 the processing is necessary for the purpose of establishing exercising or defending legal claims; or

10.3.5 the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.

10.4 To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:

10.4.1 ensure that either the individual has given their explicit consent to the processing; or

10.4.2 ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

10.5 We would normally only expect to process special category personal data or criminal records history data usually in a Human Resources context.

10.6 **When do we process personal data?**

10.7 Virtually anything we do with personal data is processing including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction. So even just storage of personal data is a form of processing. We might process personal data using computers or manually by keeping paper records.

10.8 Examples of processing personal data might include:

10.8.1 Using personal data to correspond with customers;

10.8.2 Holding personal data in our databases or documents; and

10.8.3 Recording personal data in personnel or customer files.

11. **Outline**

11.1 The main themes of the Data Protection Laws are:

11.1.1 good practices for handling personal data;

11.1.2 rights for individuals in respect of personal data that controllers hold on them; and

11.1.3 being able to demonstrate compliance with these laws.

11.2 In summary, data protection law requires each controller within the Group to:

11.2.1 only process personal data for certain purposes;

11.2.2 process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure and processing it fairly and in a transparent manner);

11.2.3 provide certain information to those individuals about whom we process personal data, which is usually provided in a privacy notice, for example you will have received one of these from us as one of our Workers;

11.2.4 respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them); and

11.2.5 keep adequate records of how data is processed and, where necessary, notify the ICO and possibly data subjects where there has been a data breach.

11.3 Every member of our 'Workers' has an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy.

11.4 Data protection law in the UK is enforced by the Information Commissioner's Office ("**ICO**"). The ICO has extensive powers.

12. **Data protection principles**

12.1 The Data Protection Laws sets out six principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

12.1.1 Processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;

12.1.2 collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");

12.1.3 adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");

12.1.4 accurate and where necessary kept up to date;

12.1.5 kept for no longer than is necessary for the purpose ("storage limitation");

12.1.6 processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

13. **Data subject rights**

13.1 Under Data Protection Laws, individuals have certain rights (**Rights**) in relation to their own personal data. In summary these are:

13.1.1 The rights to access their personal data, usually referred to as a subject access request

13.1.2 The right to have their personal data rectified;

13.1.3 The right to have their personal data erased, usually referred to as the right to be forgotten;

13.1.4 The right to restrict processing of their personal data;

13.1.5 The right to object to receiving direct marketing materials;

13.1.6 The right to portability of their personal data;

13.1.7 The right to object to processing of their personal data; and

13.1.8 The right to not be subject to a decision made solely by automated data processing.

13.2 The exercise of these Rights may be made in writing, including email, and verbally and should be responded to in writing by us (if we are the relevant controller) without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

13.3 Where the data subject makes the request by electronic form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

13.4 If we receive the request from a third party (e.g. a legal advisor), we must take steps to verify that the request was, in fact, instigated by the individual and that the third party is properly authorised to make the request. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.

13.5 There are very specific exemptions or partial exemptions for some of these Rights and not all of them are absolute rights. However, the right to not receive marketing material is an absolute right, so this should be complied with immediately.

13.6 Where an individual considers that we have not complied with their request e.g. exceeded the time- period, they can seek a court order and compensation. If the court agrees with the individual, it will issue a Court Order, to make us comply. The Court can also award compensation. They can also complain to the regulator for privacy legislation, which in our case will usually be the ICO.

13.7 In addition to the rights discussed in this document, any person may ask the ICO to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the privacy legislation. The ICO must investigate and may serve an "Information Notice" on us (if we are the relevant controller). The result of the investigation may lead to an "Enforcement Notice" being issued by the ICO. Any such assessments, information notices or enforcement notices should be sent directly to our GDPR Compliance Manager from the ICO.

13.8 In the event of a Worker receiving such a notice, they must immediately pass the communication to our GDPR Compliance Manager.

14. **Notification and response procedure**

14.1 If a member of staff has a request or believes they have a request for the exercise of a Right, they should:

14.1.1 pass the call to their supervisor/manager. The supervisor/manager should take and record all relevant details and explain the procedure. If possible, try to get the request confirmed in writing addressed to our GDPR Compliance Manager and

14.1.2 inform our GDPR Compliance Manager of the request.

14.2 If a letter or fax exercising a Right is received by any member of staff, they should:

14.2.1 pass the letter to their supervisor/manager;

14.2.2 the supervisor/manager must log the receipt of the letter with our GDPR Compliance Manager and send a copy of it to them; and

14.2.3 our GDPR Compliance Manager will then respond to the data subject on our behalf.

14.3 If an email exercising a Rights is received by any member of staff, they should:

14.3.1 pass the email to their supervisor/manager;

14.3.2 the Supervisor/manager must log the receipt of the email with our GDPR Compliance Manager and send a copy of it to them; and

14.3.3 our GDPR Compliance Manager will then respond to the data subject on our behalf.

14.4 Our GDPR Compliance Manager will co-ordinate our response, which may include written material provided by our appointed legal representative. The action taken will depend upon the nature of the request. The GDPR Compliance Manager will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from the GDPR Compliance Manager should suffice in most cases.

14.5 The GDPR Compliance Manager will inform the relevant management line of any action that must be taken to legally comply. The GDPR Compliance Manager will co-ordinate any additional activity required to meet the request.

14.6 The manager / Director who receives the request will be responsible for ensuring that the relevant response is made within the time period required.

14.7 The GDPR Compliance Manager's reply will be validated by the relevant manager of the department producing the response. For more complex cases, the letter/email to be sent will be checked by our appointed legal advisors.

15. **Your main obligations**

15.1 What this all means for you can be summarised as follows:

15.1.1 Treat all personal data with respect;

15.1.2 Treat all personal data how you would want your own personal data to be treated;

15.1.3 Immediately notify your line manager or the GDPR Compliance Manager if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;

15.1.4 Take care with all personal data and items containing personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and

15.1.5 Immediately notify the GDPR Compliance Manager if you become aware of or suspect the loss of any personal data or any item containing personal data. For more details on this see our separate Data Breach Policy which applies to all our Workers regardless of their position or role in our organisation.

16. **Your activities**

16.1 Data protection laws have different implications in different areas of our organisation and for different types of activity, and sometimes these effects can be unexpected.

16.2 Areas and activities particularly affected by data protection law include human resources, payroll, security (e.g. CCTV), customer care, sales, marketing and promotions, health and safety and finance.

16.3 You must consider what personal data you might handle, consider carefully what data protection law might mean for you and your activities, and ensure that you comply at all times with this policy.

17. **Practical matters**

17.1 Whilst you should always apply a common- sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don'ts:

17.1.1 Do not take personal data out of the organisation's premises (unless absolutely necessary).

17.1.2 Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else.

17.1.3 Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc. and this would include paper files, mobile phone, laptops, IT tablets, memory sticks etc.

17.1.4 Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, IT tablets, memory sticks etc.

17.1.5 If you are staying at a hotel, then utilise the room safe or ask the hotel staff to store items containing personal data when you do not need to have them with you.

17.1.6 Do encrypt laptops, mobile devices and removable storage devices containing personal data.

17.1.7 Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

17.1.8 Do password protect documents and databases containing personal data.

17.1.9 Never use removable storage media to store personal data unless the personal data on the media is encrypted.

17.1.10 When picking up printing from any shared printer always check to make sure you only have the printed matter that you expect, and no third party's printing appears in the printing.

17.1.11 Use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste, do not place them in a bin or skip etc., and either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.

17.1.12 Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

17.1.13 When in public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device you are using when you have personal information on display. If necessary, move location or change to a different task.

17.1.14 Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.

17.1.15 Do challenge unexpected visitors or employees accessing personal data.

17.1.16 Do not leave personal data lying around, store it securely.

17.1.17 When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead, use initials or just first names to preserve confidentiality.

17.1.18 If taking down details or instructions from a customer in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.

17.1.19 Never act on instructions from someone unless you are sure of their identity and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.

17.1.20 Do not transfer personal data to any third party without prior written consent of your line manager or our GDPR Compliance Manager.

17.1.21 Do notify your line manager or our GDPR Compliance Manager immediately of any suspected security breaches or loss of personal data.

17.1.22 If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to our GDPR Compliance Manager. For more details on this see our separate Data Breach Policy which applies to all our Workers regardless of their position or role in our organisation.

17.2 However, you should always take a common- sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of our GDPR Compliance Manager.

18. **Foreign transfers of personal data**

18.1 Personal data must not be transferred outside the UK unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of personal data or we put in place adequate protections.

18.2 These protections may come from special contracts we need to put in place with the recipient of the personal data, from them agreeing to be bound by specific data protection rules or due to the fact that the recipients own country's laws provide sufficient protection. It may also be necessary to perform a Transfer Impact Assessment.

18.3 These restrictions also apply to transfers of personal data outside of the UK even if the personal data is not being transferred outside of our group of companies.

18.4 You must not under any circumstances transfer any personal data outside of the UK without your line manager's or the GDPR Compliance Manager's prior written consent.

18.5 We will also need to inform data subjects of any transfer of their personal data outside of the UK and may need to amend their privacy notice to take account of the transfer of data.

18.6 If you are involved in any new processing of personal data, which may involve transfer of personal data outside of the UK, then please seek approval of your line manager or our GDPR Compliance Manager prior to implementing any processing of personal data, which may have this effect.

19. **Queries**

19.1 If you have any queries about this Policy, please contact either your line manager or the GDPR Compliance Manager.

Version 1.5: 06.10.2022

Policy Control

This is a controlled document. Whilst this document may be printed, the electronic version located on the S: Drive will be the most up to date version and the controlled copy. Any printed copies of the document are not controlled.

Date of Issue:	23-5-18	**Next Review Date:**	06.10.2023
Version:	1	**Last Review Date:**	06.10.2022
Document Owner:	Vanessa Currie		
Department:	People, Learning and Development.		
Policy Approval Route			
Policy Ref. No.	**Policy Name**	**Approved By:**	**Date Approved:**
1	Data Protection Policy	Gateley and Exec team	23.5.18

20. **Amendment History**

Issue:	Policy Ref. No.:	Date:	Reason for Change:	Authorised by:
2	1.2	12.6.19	No changes annual policy review.	A Vlahakis – Interim CEO; JJ Mian – Interim Finance Director; Rebecca Delmore – Commercial Director; Linda Degg – Facilities Director
3	1.3	30.06.2020	Policy ref no. changed to 1 Policy name added. Issue 1.2 changed to 2 Policy reference number changed to version 1.3	A Vlahakis – Interim CEO; JJ Mian – Interim Finance Director; Rebecca Delmore – Commercial Director; Linda Degg – Facilities Director Vanessa Currie – Head of PLD
4	1.4	07.09.2021	Removed GDPR Compliance manager name and left title. Section 19. Section 5.1.2.2 – UK GDPR now uses a sterling figure so the number for the maximum fine has been updated to	Tom Hughes – Gateleys A Vlahakis –CEO; JJ Mian –Finance Director;

			£17.5 million. Section 6.1 – removed reference to the Data Protection Act as this is outdated legislation. Removed Section 6.3 which refers to the implementation date as the 25th May 2018 as the policy is now in effect. Removed the term "data" as **data** controller and **data** processor terms are no longer used – the former terms were those used in the DPA 1998 and were used interchangeably at the time that the GDPR was implemented but have since dropped out of usage in favour of the controller and processor (no "data") terms used in the GDPR. Section 18 – replaced references to the EEA with UK. Section 18.2 – added that a Transfer Impact Assessment may be required.	Rebecca Delmore – Commercial Director; Linda Degg – Facilities Director Vanessa Currie – Head of PLD
1.5	1.5	06.10.2022	Annual review – no changes.	A Vlahakis (CEO) V Currie (Head of PLD)