DATA PROTECTION & PRIVACY POLICY

Context and Overview:
Key Details

- Policy prepared by Phillip Plato
- Prepared for Plato Estates & the associated business inc P A Plato Grandchildren's Trust
- Approved by the Board/Members on – 11 December 2020
- Policy to become operational on: - 12 December 2020
- Next review date: - 30 December 2022

Introduction:
Plato Estates Ltd and its associated business (hereafter collectively referred as "The Business") needs to gather and use certain information about individuals that it may employ or do business with.

These individuals will include directors and employees and certain self-employed contractors/consultants as well as potential information relating to suppliers, contractors, and other people that the Business has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Data Protection standards of The Business and to comply with the law.

Why this policy exists:
This data protection policy ensures that Plato Estates Ltd & Plato Property Investments LLP

- Complies with data protection law and follows good practice.
- Protects the rights of employees, self-employed contractors, and others &.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risk of a data breach.

Data Protection Law:
The Data Protection Act 1998 describes how all organisations including Plato Estates Ltd must collect, handle and store personal information. The requirements of the Act are supplemented by the GDPR coming into effect on 25th May 2018.

These rules must apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must be:

1. Processed fairly and lawfully.
2. Obtained only for specific lawful purposes.
3. Be accurate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside the European Union unless that country or territory also ensures an adequate level of data protection.

People, Risks and Responsibilities:

Policy scope :
This policy applies to;

- The Executive Board directors of Plato Estates Ltd & Members of Plato Property Investments LLP.
- All staff and self-employed consultants of The Business.
- All self-employed contractors, suppliers and other people working on behalf of The Business including external third party Data Processors (such as payroll agencies).

It applies to all data that the Business holds relating to identifiable individual people even if that information technically falls outside the Data Protection Act.
This data can include:

- Names of individuals.
- Postal address.
- Email address.
- Telephone number.
- A photograph of the individual.
- Bank or credit card details.
- Medical information.
- Plus any other information relating to an identifiable individual.

Data Protection Risks:
This policy opts to protect The Business from real data security risks including:

- Breaches of confidentiality – for instance information being given out inappropriately.
- Failing to offer choice – for instance all individuals should be free to choose how the company uses data relating to them.
- Reputational damage – the company could suffer if hacker successfully gained access to sensitive data.

Responsibilities:
Everyone who works for or with Plato Estates Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.
In addition, each area of operation within The Business or which is engaged externally as a "Data Processor" that handles personal data must ensure that it is handled and processed in line with this policy and that data protection principles are applied.
The following people have key areas of responsibility:

- The Board of Directors/Designated Members is/are ultimately responsible for ensuring that the Business meets its legal obligations.
- Due to the nature of the organisation and its size there is no individual named as a Data Protection Officer.
- Each individual employee or designated Data Processor is responsible for keeping the Executive Directors/Designated Members updated about data protection responsibilities, risks and issues and reviewing data protection procedures in their area of operation and to ensure that people they are working with are aware of this policy and given appropriate training or instruction.
- Third Party Data Processors are required to be aware of their responsibilities to safeguard data and to ensure that any computer systems, paper based services and equipment used for storing data meet acceptable security standards and that regular checks and scans are performed to ensure software is functioning correctly and that any backups are stored

securely. Particular reference should be made to any data storage on cloud computing services.

General Staff Guidelines:

- The only people able to access date covered by this policy should be those who need it for their work.
- Data should not be shared informally and should only be retained if it is necessary for the effective operation of the Business.
- All employees, self employed contractors & consultants should be required to keep all data secure by taking sensible precautions and following these guidelines:
    - Data should only be stored on a system that has suitable antivirus software, firewalls and password protection installed.
    - Regular backups should be made but only in accordance with the company's approved procedures.
    - Specifically personal data should never be copied onto memory sticks, CD's or personal computers/laptops that are not part of the private network of the Business and similarly paper records containing personal details should not be left on open desks but locked away securely.
    - Any paper records that need to be deleted should be shredded and any personal information held in digital format that is no longer appropriate or necessary for the effective operation of the Business should be deleted, including from back up copies.
- Any personnel within the Business or who operate as Third Party Data Processors and who have any concerns about the procedures or that data might have been compromised, must immediately alert the Directors or Designated Members.

Data Storage:

These rules describe how and where data should be safely stored.

- When data is stored on paper it should be kept in a secure locked place where unauthorised people cannot see it or access it.
- Paper printouts should not be left where unauthorised people could see them such as on a printer or in open view on a desk.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is secured electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. The aforementioned comments about virus protection, firewall, passwords and backup also apply. The server should only retain data in encrypted form.
- If data is stored on removable media (such as CD or DVD) these should be kept locked away securely when not being used.
- Data should not be uploaded to cloud computing services unless they have been approved by the IT contractor retained by The Business and the Directors/Designated Members.
- Data should be backed up frequently and the Disaster Recovery Policy adhered to. The data backups should be tested regularly and kept securely offsite.

Data Use:

- No data relating to an identifiable individual should be used by any member of the Business for any purposes other than that directly related to the operation of the Business or its related activities. For example it would be inappropriate to use an email address to contact someone for personal reasons unrelated to the Business.

- Personal data should not be shared informally. In particular it should never be sent by email and a classic error to be avoided is mass emails where all recipients can been seen in the address bar rather than using the bcc bar.
- Employees should not save copies of personal data onto their personal devices such as tablets, phone or laptops that have not been approved for such use by the Business IT contractor.

Data Accuracy:

The law requires that the Business takes reasonable steps to ensure that data is kept accurate and up to date.
It is the responsibility of all employees and retained contractors including Third Party Data Processors, who work with personal data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data should be held in as few places as necessary.
- Staff & retained contractors should take every opportunity to ensure date is updated. For example by confirming an individual's data is correct when they call or visit.
- Data should be updated as soon as inaccuracies are discovered. For instance, if an individual can no longer be reached on their stored telephone number or email address it should be removed from the database.

Subject Access Requests:
All individuals who are the subject of personal data being held by Plato Estates Ltd and its associated business, Plato Property Investments LLP are entitled to:

- Ask what information the Business holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the Business requesting this information this is called a subject access request.

Subject access requests from individuals should be made by email addressed to the Managing Director at solutions@platoestates.com .

The recipient of a subject access request will aim to provide the relevant data within 14 days of receipt of the request. However, before doing so, the Business must always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data for Other Reasons:
In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.
Under these circumstances the Business will disclose requested data, however the relevant Data Controller will ensure the request is legitimate, seeking assistance from the Directors and from legal advisors if necessary.

Providing Information:
Plato Estates Ltd aims to ensure that all individuals are aware that their data is being processed and that they understand:

- How the data is being used.
- How to exercise their rights.

- That the data will not be disclosed to any third party nor sold for marketing purposes. Under the principles of GDPR, the Business will not adopt a policy of "*click here to read our privacy policy*". The privacy policy will be stated expressly on the company website.
- Similarly, the Business will not adopt the principle of implied consent using pre ticked boxes on websites and apps. Conversely where applicable, individuals will have to consciously opt in to give consent for use of their data.

To this end the company will use the following privacy statement setting out how data relating to individuals is used by the Business.

Privacy Statement (to appear on website or modified / attached to emails /forms as appropriate).

This privacy statement sets out how Plato Estates Ltd and its associated business uses and protects any information that you give to the Business or when you use the company website.

Plato Estates is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website, then you can be assured that it will only be used in accordance with this privacy statement for the purposes of effective running of this business.

Plato Estates Ltd may change this policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes. This policy is effective from 25 May 2018.

What we collect:
We may collect the following information:
- Name and contact information including email address.
- Demographic information such as postcode, preferences and interests.
- Other information relevant to customer surveys.

What we do with the information we gather:
We require this information to to understand your needs and to provide you with a better service, and in particular for the following reasons:
- Internal record keeping.
- To periodically send promotional emails about news relating to Plato Estates Ltd and associated operations that we think you may find interesting or of benefit.
- We may also use your information to contact you for market research purposes and may contact you by email, phone, fax or social media.
- We will never disclose your personal information to third parties nor sell your data to any other organisation without first seeking your personal and informed consent before doing so.

Security:
We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable, physical, electronic and managerial procedures to safeguard and secure the information we collect.

How we use cookies:
A cookie is a small file which asks permission to be placed on your computers hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular website. Cookies allow web applications to respond to you as an individual. A web

application can tailor its operation to your needs by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps our website administrators analyse data about webpage traffic and to improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system. A cookie does not give us access to your computer or any information about you other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies but you can usually modify your browser setting to decline cookies if you prefer.

Links to other websites:
Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that third party website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Controlling your personal information:
You may choose to restrict the collection or use of your personal information in the following ways:

- Whenever you are asked to fill in a form on the website look for a box requiring you to indicate that you consent for the information to be used by anybody for direct marketing purposes. If this is not ticked by you, it will not be shared for that direct marketing activity.
- If you have previously agreed to us using your personal information for direct marketing, you may change your mind at any time by giving us notification in writing or by emailing us.

We will not sell, distribute or lease your personal information to third parties without your prior permission.

You may request details of personal information which we hold about you under the Data Protection Act 1998. Such requests can be made to the Managing Director at solutions@platoestates.com

If you believe that any information, we are holding on you is incorrect or incomplete, please write or email Plato Estates Ltd as soon as possible and we will promptly correct any information found to be incorrect.

Abbreviated Privacy Statement **(for use on forms, website data capture areas etc)**

Plato Estates Ltd respects everyone's privacy and will never sell, share or disclose your data to a third party without your express consent. We only retain data that is necessary for the effective operation of our business. You may request to be removed from any database we retain or request details of any information our company holds on you via our full Privacy Policy (click here).