The Tiny Treehouse Data Protection Policy

DATA PROTECTION POLICY

CONTENTS

1. POLICY STATEMENT

During the course of our activities Emma Loyns LLP trading as The Tiny Treehouse("**we**", "**our**", "**us**") will collect, store and process Personal Data about our customers, clients, suppliers, Personnel, applicants, website users, shareholders and other third parties (both past and present). We are the Data Controller of all Personal Data relating to our Personnel and Personal Data used in our business for our own commercial purposes. We recognise that the correct and lawful treatment of this data is important both to the individual Data Subjects, but also to us in maintaining confidence in the organisation and providing for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. We rely on all those that work with or for us to help us comply with our data protection obligations. We are exposed to significant potential fines, depending on the breach, for failure to comply with the provisions of applicable data protection legislation.

See the final section of this policy for the key definitions used in this policy.

Whenever the terms 'processing' or 'process' are used in this policy, this means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

2. WHAT DOES THIS POLICY COVER?

This policy and any other documents referred to in it sets out the basis on which we will process the Personal Data of our customers, clients, suppliers, Personnel, applicants, website users, shareholders and other third parties (both past and present).

It sets out Personnel rights and obligations in relation to Personal Data.

3. ALL PERSONNEL COMPLIANCE

This policy applies to all Personnel who work for or with us ("**you", "your"**). You must comply with this policy at all times. You must attend any training on the requirements of this policy. Any breach of this policy may result in disciplinary action for employees (up to and including summary dismissal) and in contractual implications for others (usually immediate termination). This policy is an internal document and may not be shared with any third parties or regulators without prior authorisation from. This policy does not form part of any employee's contract of employment or other Personnel contracts and may be amended at any time.

4. PERSONNEL OBLIGATIONS

Personnel at all levels may have access to Personal Data of other individuals including customers, clients, suppliers, Personnel, applicants, website users, shareholders and other third parties in the course of their work with or for us. We rely on all members of Personnel whatever their seniority to help us meet our data protection obligations.

If you have access to Personal Data you must:

- only access data that you have authority to access and only for authorised purposes;
- not disclose data except to individuals who have appropriate authorisation (whether inside or outside the organisation);
- keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction). In particular, where applicable, you must lock your computer screens when not at your desk. You must lock drawers and filing cabinets and not leave paper with Personal Data lying about;
- not remove Personal Data, or devices containing or that can be used to access Personal Data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device and follow our policies relating to removable media devices and remote working.
- not store Personal Data on local drives or on personal devices that are used for work purposes;
- keep data secure when working from home;
- not save Personal Data to your own personal computers or other devices or send Personal Data to your personal email addresses;
- only use data for the specified lawful purpose for which it was obtained;
- regularly review and update Personal Data which you have to deal with for work;
- not make unnecessary copies of Personal Data and keep and dispose of any copies securely;
- shred and dispose securely of documents containing Personal Data when you have finished with it; and
- comply with all other aspects of this policy (each section has specific obligations that you need to comply with).

If you are unsure about anything to do with processing Personal Data, you should speak to Emma Loyns. You must always contact Emma Loyns in the following circumstances:

- if you become aware of an actual or potential Personal Data breach (Section 5 below);

- if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by us) (see Section 7 below);
- before you process any new type of Special Categories of Personal Data or process Special Categories of Personal Data in a new way (see Section 8 below);
- before you process any new type of Criminal Convictions Data or process such data in a new way (see Section 9)
- if you need to rely on consent and/or need to capture explicit consent or think you may have to do so (see Section 10 below);
- if you are unsure about the retention period for the Personal Data being processed (see Section 15 below);
- if you are unsure about what security or other measures you need to implement to protect Personal Data (see Section 16 below);
- if you are unsure on what basis to transfer Personal Data outside the UK (see Section 18 below);
- if you need any assistance dealing with any rights invoked by a Data Subject (see Sections 19 and 20);
- whenever you are engaging in a significant new, or change in, processing activity which is likely to require a DPIA (see Section 21 below) or plan to use Personal Data for purposes others than what it was collected for;
- if you plan to undertake any activities involving automated processing including profiling or Automated Decision Making (see Section 22 below);
- if you plan to introduce a new service provider or new service product offering;
- if you need help complying with applicable law when carrying out direct marketing activities (see Section 23 below);
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see Section 24 below); or
- if you carry out any new processing activity, to enable our record of processing to be updated (see section 25 below).

You are responsible for helping us keep your Personal Data up to date. You should let us know if any Personal Data held by us changes, for example if you move house, change your bank details or get married. You must also inform us if your mobile phone number changes.

Failing to observe any of requirements of this policy may amount to a disciplinary offence. Significant or deliberate breaches of this policy, such as accessing any Personal Data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to summary dismissal, or in the case of contractors, to contractual consequences including the immediate termination of engagement.

5. REPORTING PERSONAL DATA BREACHES

You must notify Emma Loyns immediately you become aware of any actual or potential breach of security which has or may lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed (a "**Personal Data Breach"**). You must notify Emma Loyns of any Personal Data Breach, however minor, caused either by you or anyone else.

Under applicable data protection legislation, we are responsible for notifying the applicable regulator (the Information Commissioner in the UK) without undue delay (within at the most 72 hours) of any Personal Data Breach which involves a risk to the right and freedoms of Data Subjects. It is therefore imperative that you notify Emma Loyns immediately you become aware of any such breach. This would include contacting Emma Loyns out of working hours, at weekends or holidays.

We are also responsible for

- notifying the Data Subject without undue delay in certain circumstances;
- notifying the processor or Controller of Personal Data in certain circumstances; and
- updating our Breach Register.

These obligations all have different deadlines for compliance, so notifying Emma Loyns as soon as you become aware of an actual or potential Personal Data Breach will allow us to comply with its various obligations.

If you become aware of an actual or potential Personal Data Breach, do not attempt to investigate the matter yourself. You should, however, preserve all evidence relating to the Personal Data Breach.

Clearly serious Personal Data Breaches such as leaving an unencrypted iPad with Personal Data on in a public space such as a cafe, would require you to contact Emma Loyns without any delay, even if it was out of working hours. However, even seemingly minor events would require you to notify Emma Loyns. For example if you become aware that an email containing Personal Data has been accidentally sent to the wrong email address this would also require you to notify.

6. DATA PROTECTION PRINCIPLES

We comply and anyone processing Personal Data on our behalf must comply with the principles set out in applicable data protection legislation. These provide that Personal Data must be:

- Processed lawfully and fairly and in a transparent manner (Lawfulness and Fairness - see section 7 and Transparency- see section 11 below).

- Collected for specified, explicit and legitimate purposes and processed in a manner consistent with such purposes (Purpose Limitation - see section 12 below).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation - see section 13 below).
- Accurate and, where necessary, kept up to date (Accuracy - see section 14 below).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Data Security - see section 16 below).
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests – see sections 19 and 20 below).

In addition, Personal Data must not be:

- Kept in a form which permits identification of Data Subjects for longer than necessary for the purpose (Storage Limitation - see section 15 below).
- Transferred to another country without appropriate safeguards being in place (International Data Transfers – see section 18 below).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability – see section 17 below).

Further details of these principles along with an explanation of our procedures for securing compliance with them are set out in the following sections in this policy.

7. LAWFULNESS AND FAIRNESS

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

Data protection legislation is not intended to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject.

We will comply with this principle and only process Personal Data fairly and lawfully for specified purposes. For Personal Data to be processed lawfully, it must be processed on the basis of one of the following six legal bases:

- the Data Subject has given his or her consent;
- the processing is necessary for the performance of a contract with the Data Subject or in order to take steps at the request of the Data Subject prior to entering into a contract;
- the processing is necessary for the compliance with a legal obligation to which we are subject;

- the processing is necessary to protect the Data Subject's vital interests;
- the processing is necessary for the performance of a task carried out in the public interest; or
- the processing is necessary for the purposes of our legitimate interests where such interests are not overridden because the processing prejudices the interests or fundamental rights and freedoms to Data Subjects.

When Special Categories of Personal Data or Criminal Convictions Data are being processed, additional legal bases and/or processing conditions must also be met (see sections 8 and 9 for more details).

You must consider and then document the legal basis being relied on for each processing activity before carrying out that activity.

8. SPECIAL CATEGORIES OF PERSONAL DATA

Special Categories of Personal Data require higher levels of protection. We can process such data only if we have a legal basis for processing (one of those set out in section 7 above) and one of the additional legal bases relating to Special Categories of Personal Data also applies (see below). We will identify and document the legal bases relied on for each processing activity.

Where we process Special Categories of Personal Data, we usually rely on the following additional legal bases, subject to any applicable conditions in each case:

- where such processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on us or the Data Subject in connection with employment, social security or social protection; or
- where the Data Subject has given their explicit written consent.

Subject to any applicable conditions in each case, we may also process Special Categories of Personal Data on other additional legal bases including:

- where it is necessary to protect the Data Subject's vital interests (or someone else's interests) and the Data Subject is not capable of giving their consent,
- where it is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- where the Data Subject has already made the information public;
- where it is necessary for archiving, scientific, historical research or statistical purposes and is in the public interest; or
- where it is necessary for reasons of substantial public interest and is necessary for the purposes of:

- insurance; or
- identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups with a view to enabling such equality to be promoted or maintained.

When collecting Special Categories of Personal Data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we will provide Data Subjects with a Privacy Notice, details of which are set out below in section 11.

You must take special care when processing Special Categories of Personal Data. You must identify and document the legal bases for processing before processing such data. Before processing any new type of Special Categories of Personal Data or processing existing Special Categories of Personal Data in a new way, you should contact Emma Loyns to seek advice.

9. CRIMINAL CONVICTIONS DATA

Criminal Convictions Data is a class of data with its own special protection and rules for processing.

We can process such data only if we have a legal basis for processing (one of those set out in section 7 above) and one of the specific processing conditions relating to Criminal Convictions Data applies (see below). We will identify and document the legal basis and specific processing condition relied on for each processing activity.

Where we process Criminal Convictions Data, we will usually rely on the processing condition that such processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on us or the Data Subject in connection with employment, social security or social protection.

We may also process Criminal Convictions Data on other processing conditions including:

- if the Data Subject has given their explicit written consent;
- where it is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) or where it is necessary for obtaining legal advice or for the purpose of establishing, exercising or defending legal rights;
- where it is necessary when a court or tribunal is acting in its judicial capacity;
- where the Data Subject has already made the information public;
- where it is necessary for the prevention or detection of an unlawful act; or
- where it is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement (a requirement imposed by legislation or a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity) which involves a person taking steps to establish whether

another person has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct.

When collecting Criminal Convictions Data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we will provide Data Subjects with a Privacy Notice, details of which are set out below in section 11.

You must take special care when processing such data. You must identify and document the legal basis for processing together with the processing condition before processing such data. Before processing any new type of Criminal Convictions Data or processing existing Criminal Convictions Data in a new way, you should contact Emma Loyns to seek advice.

10. CONSENT

For most uses of Personal Data, we will not rely on consent in order to process the Personal Data. However, in limited circumstances, we may seek to rely on consent.

If you wish to rely on consent for processing any Personal Data, you must first speak to Emma Loyns to establish if another legal basis would be more appropriate.

If you are seeking consent from anyone to processing you should be aware that a Data Subject consents to processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

If we are unable to rely on another legal basis of processing, explicit consent (consent which requires a very clear and specific statement, not just action) may be required for processing Special Categories of Personal Data, for Automated Decision Making, Criminal Convictions Data and for cross border data transfers.

You will need to evidence consent captured and keep records of all consents so that we can demonstrate compliance with consent requirements.

11. TRANSPARENCY

Personal Data must be processed in a transparent manner in relation to the Data Subject.

We will comply with this principle and will be transparent about the way we collect and process Personal Data. Personnel can find out detailed information from the Internal Privacy Notice. This notice sets out:

- the identity and contact details of the Controller (us);
- the specific types of Personal Data we process (including Special Categories of Personal Data);
- the sources of such data;
- the legal bases for processing;
- the purposes of processing;
- the legitimate interests pursued by us;
- recipients of such data;
- details of any overseas transfers;
- data retention information;
- details of any Automated Decision Making; and
- Personnel rights

Clients, customers, suppliers and other external third parties can find out how we collect and process their Personal Data by reading the External Privacy Notice.

Whenever Personal Data is collected directly from Data Subjects you must provide the Data Subject with the relevant Privacy Notice when the Data Subject first provides the Personal Data or as soon as possible thereafter. When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with the relevant Privacy Notice as soon as possible after collecting/receiving the data and no later than the time of the first communication with them.

12. PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be processed in any manner incompatible with those purposes.

We will comply with this principle and will inform Data Subjects what those legitimate purposes are in a published Privacy Notice. If we use Personal Data for a new compatible purpose then we will inform the Data Subject first.

If you wish to use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained, you must contact Emma Loyns.

13. DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We will comply with this principle and will ensure that we do not collect excessive data. We will only collect and disclose the minimum Personal Data required for the purpose for which the data is collected or disclosed. We will ensure that the Personal Data collected is adequate and relevant for the intended purposes.

You may only collect and/or process Personal Data if your job requires it. You must not process Personal Data for any reason unrelated to your job or the task that has been assigned to you. You must not collect excessive data.

14. ACCURACY

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will comply with this principle and ensure that the Personal Data we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

You must also ensure that the Personal Data you use or hold in the course of your work is accurate, complete, kept up to date and relevant to the purpose for which it was collected. You must check the accuracy of any Personal Data at the point of collection (where you are involved in such collection) and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data which you are responsible for.

15. STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We will comply with this principle. We will maintain retention policies and procedures to ensure Personal Data is deleted or rendered permanently anonymous a reasonable time after it is no

longer required for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than is needed for the purposes for which we originally collected it or for the purpose of satisfying any legal, accounting or reporting requirements.

You must take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require. This includes requiring third parties to delete such data where applicable.

16. DATA SECURITY

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will comply with this principle. We have developed, implemented and will maintain technical and organisational measures to ensure a level of security appropriate to the risks we face in relation the processing of Personal Data.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement to maintain the security of all Personal Data from the point of collection to the point of destruction.

You must exercise particular care in protecting Special Categories of Personal Data from loss and unauthorised access, use or disclosure.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- *Confidentiality* means that only people who have a need to know and are authorised to use the Personal Data can access it.
- *Integrity* means that Personal Data is accurate and suitable for the purpose for which it is processed.
- *Availability* means that authorised users are able to access the Personal Data when they need it for authorised purposes.

17. ACCOUNTABILITY

We are responsible for, and must be able to demonstrate, compliance with the data protection principles. We have adequate resources and controls in place to ensure and to document compliance with applicable data protection legislation including:

- nominating a person who has responsibility for data protection issues;
- completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects (see Section 21) and consulting the Information Commissioner if appropriate;
- where appropriate regularly training Personnel on applicable data protection legislation, this policy, related policies and data protection matters including, for example, Data Subject's rights, consent, legal bases, Data Protection Impact Assessments and Personal Data Breaches. We will maintain a record of training attendance by Personnel;
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to improve compliance;
- ensuring that records are kept of all Personal Data processing activities, and that these are provided to the Information Commissioner on request; and
- having internal processes to ensure that Personal Data is only collected, used or handled in a way that is compliant with data protection law.

18. INTERNATIONAL DATA TRANSFERS

Data protection legislation in the UK restricts data transfers to countries outside of the UK in order to ensure that the level of data protection afforded to individuals is not undermined. Transferring data for these purposes means not only transmitting or sending data from one country to another, but also viewing or accessing data in a different country from the country in which it originated.

You must not transfer Personal Data outside the UK without the express written permission of Emma Loyns.

19. DATA SUBJECTS' RIGHTS

Data Subjects have a number of rights in connection with the processing of their Personal Data, subject to certain conditions set out in applicable data protection legislation, including the right to:

- Request access to their Personal Data (commonly known as a "data subject access request"). This enables them to receive a copy of the Personal Data we hold about them and to check that we are lawfully processing it (see Section 20 for more details).
- Request correction of the Personal Data that we hold about them. This enables them to have incomplete or inaccurate data we hold about them corrected.
- Request the erasure of their Personal Data. This enables them to ask us to delete or remove Personal Data where there is no good reason for us continuing to process it.

- Ask us to stop processing Personal Data where we are relying on a legitimate interest and there is something about their particular situation which makes them want to object to processing on this ground. They can also prevent our use of their Personal Data for direct marketing purposes.
- Request the restriction of processing of their Personal Data. This enables them to ask us to suspend the processing of Personal Data about them, for example if they want us to establish its accuracy or the reason for processing it.
- Request the transfer of their Personal Data to another party.
- Lodge a complaint regarding the processing of their data with the Information Commissioner's Office.
- Request a copy of an agreement under which Personal Data is transferred outside the UK.
- Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms.

If you want to review, verify, correct or request erasure of your Personal Data, object to the processing of your Personal Data, or request that we transfer a copy of your Personal Data to another party, please contact Emma Loyns in writing.

If you receive a request from a Data Subject to exercise any of the rights set out above, you must immediately forward this to Emma Loyns.

20. SUBJECT ACCESS REQUESTS

When we receive a data subject access request, we are under an obligation to respond without undue delay. It is essential therefore for you to immediately forward any data subject access request to Emma Loyns. This could be any request from a Data Subject for confirmation that their data is being processed, access to their Personal Data or access to other supplementary information (such as the information set out in the Privacy Notices). You should not respond to a data subject access request yourself without first consulting Emma Loyns.

If you wish to make a data subject access request please do so in writing and send it to Emma Loyns.

21. DATA PROTECTION IMPACT ASSESSMENTS

Where a type of processing is likely to result in a high risk to the rights and freedoms of any individuals a DPIA must be carried out. A DPIA is an assessment used to identify and reduce the risks of a data processing activity.

DPIA should be conducted when implementing new projects or changing current systems involving the processing of Personal Data including in particular:

- The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated processing including profiling and Automated Decision Making;
- large scale processing of Special Categories of Personal Data; or
- large scale, systematic monitoring of a publicly accessible area.

If you consider that a DPIA may be required, you must contact Emma Loyns and Emma Loyns will discuss whether a DPIA is required.

22. AUTOMATED DECISION MAKING

We do not currently carry out any ADM.

23. MARKETING

We are subject to certain rules and privacy laws when marketing to our customers/clients.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer/client opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

You must comply with our guidelines on direct marketing to customers/clients.

24. DISCLOSURE AND SHARING OF PERSONAL DATA

Controllers can only in certain legitimate circumstances share Personal Data with third parties where certain safeguards and contractual arrangements have been put in place.

You must be careful when sharing any Personal Data with any third parties. You should speak to Emma Loyns if you are:

- sharing any new type of Personal Data with an existing third party;
- sharing the same Personal Data but with a new third party;
- changing the way you share Personal Data with a third party.

If in any doubt, speak to Emma Loyns in advance.

Set out below are some examples of the conditions that will be applicable when sharing Personal Data with third parties:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions;
- a fully executed written contract that contains approved third party clauses has been obtained.

Further conditions may also be applicable.

25. RECORD KEEPING

Data protection legislation requires us to keep full and accurate records of all our data processing activities.

In the case of Special Categories of Personal Data and Criminal Convictions Data, these records should also include which legal bases are relied on, which processing conditions are relied on and whether the Personal Data is retained and erased in accordance with the policy and if not, the reasons for not following this policy.

You must notify Emma Loyns if you carry out any new processing activity (anything other than the core business activities that we are already aware of) so that we can keep the record of processing up to date.

26. REVIEW AND CHANGES TO THIS POLICY

The policy will be retained where we process Special Categories of Personal Data and Criminal Convictions Data and for a period of at least six months after we stop carrying out such processing.

A copy of this policy will be provided to the Information Commissioner on request and free of charge.

This policy is reviewed from time to time. We reserve the right to change this policy at any time without notice to you. Please check back regularly to obtain the latest copy of this policy. We last revised this policy on 26 March 2025.

27. DEFINITIONS

ADM / Automated Decision Making: when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with applicable data protection legislation.

Criminal Convictions Data: Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

DPIA (Data Privacy Impact Assessment): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programmes involving the processing of Personal Data.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Specific examples of the types of Personal Data that we process are set out in detail in the:

External Privacy Notice at www.thetinytreehouse.co.uk; and

Internal Privacy Notice (a hard copy of which has been provided to you. Further copies are available on request).

Personnel: all employees, workers, consultants, contractors, secondees, agency workers, directors, members and others working for or with us (referred to also as ("**you**", "**your**"));

Special Categories of Personal Data: any of the following:

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- data concerning sexual orientation or health;
- biometric data for purpose of uniquely identifying a natural person; or
- genetic data.