DATA PROTECTION POLICY

1 Your Data Protection Responsibilities

1.1 Everyone has rights with regard to how their personal data is handled. Personal data is any information that a person can be identified from and about that person, such as a name, address, staff number, or location. During the course of our activities, Pinewood Group Limited, Pinewood Studios Limited and Shepperton Studios Limited (**we**, **us**, **our**) and together with their subsidiaries and associated companies (the **Group**) will collect, store and process personal data, and we recognise the need to treat it in an appropriate and lawful manner. This may include data we receive directly from those individuals (for example, when they complete forms on our website or give us their business cards) and data we receive from other sources (including, for example, clients, customers, business partners, tenants, contractors and others).

1.2 Personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation EU 2016/679 as incorporated and amended in the UK by section 3 of the European Union (Withdrawal) Act 2018, other data protection and privacy laws such as the European Commission Directive 95/46/EC, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, as may be updated or replaced from time to time (the **Data Laws**).

1.3 The correct treatment of personal data collected by Pinewood is of paramount importance and Pinewood seeks fully to support and adhere to the provisions of all Data Laws.

1.4 This policy sets out our rules on the data protection and the legal requirements that must be satisfied by us and those who work with us in relation to the obtaining, handling, recording, editing, revising, use, storage, transfer and destruction and other processing of such personal data. It forms part of our policies and procedures for demonstrating compliance with the Data Laws and supplements the Group's other policies relating to IT, data breaches and document retention and the Staff Privacy Notice (which sets out how the Group companies treat staff personal data).

1.5 This policy applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors, interns and volunteers (**Data Users**). All Data Users should familiarise themselves with this policy and comply with its terms when processing personal data on our behalf.

1.6 This policy does not form part of any employee's contract of employment and it may be amended at any time. Where appropriate, we shall notify changes by email and/or publish the updated version on our intranet and/or website.

1.7 Next Review Date: **June 2023**

2 Oversight and Compliance

The Group Board is responsible for ensuring compliance with the Data Laws and with this policy and has delegated day-to-day responsibility to the Legal Department. If you have any questions or concerns about the operation of this policy, please refer in the first instance to the Legal Department.

3 Data Protection Principles

3.1 All Data Users who process personal data under this policy must comply with the principles of the Data Laws. They provide that personal data must:

(a) be used in a way that makes it clear to individuals what is being done with their personal data, and is fair, reasonable and compliant with Data Laws;

(b) only be used in line with how we told the individual we would use it and not for any wider, incompatible purposes;

(c) be adequate, relevant and limited just to what to what we need it for;

(d) be accurate and, where necessary, kept up to date;

(e) not be kept for longer than we need it; and

(f) be kept secure.

3.2 In addition, when processing personal data we must bear in mind that individuals have certain rights to their personal data (for example, to access it or have it deleted) and that we must not send it to companies and people outside the EU without following certain procedures.

3.3 Each Group company must comply with these principles in respect of employee and customer data held by it and be able to demonstrate compliance (the accountability principle).

4 Fair and Lawful Processing

4.1 We must generally only process personal data if one or more of the lawful bases set out in the Data Laws apply.

4.2 This means that we will only process personal data if:

(a) the individual has given us their consent (we must ensure that the consent wording and mechanism for obtaining consent meet the requirements of the Data Laws);

(b) we need to process the personal data in order to perform a contract with the individual, or because they have asked us to take certain steps before entering into a contract (for example, we require contact details so we can deliver goods ordered);

(c) the processing is necessary to comply with the law (not including contractual obligations);

(d) the processing is necessary to protect someone's life;

(e) the processing is necessary to perform a task in the public interest or for our official functions; or

(f) the processing is necessary for our business' legitimate interest or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those interests.

4.3 If in doubt, Data Users should consult the Legal Department who can confirm which is the most appropriate to rely on. We should always record our reasoning for choosing a particular lawful basis, so we can explain ourselves if an individual complains or the data protection regulator (the ICO) asks us.

5 Sensitive Personal Data and Criminal Checks

5.1 Some of the information we hold as a business is particularly sensitive and we must be aware that special rules apply to it.

5.2 This includes information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, or an individual's genetic data, biometric data (where it uniquely identifies them), or about their health, sex life or sexual orientation (**special categories of personal data**).

5.3 We will generally not collect and use such data unless the individual has given us explicit consent (for example, confirmed in writing that they agree to us holding it) or we need it in order to fulfil our obligations as an employer.

5.4 Likewise, we can only carry out criminal record checks in certain limited circumstances.

5.5 Where it is necessary to process such information, Data Users should consult the Legal Department to ensure the correct compliance steps are taken.

6 Consent

6.1 Sometimes we will need consent to use someone's personal data, for example if we are sending them marketing emails, or disclosing special categories of personal data to a third party. Where we need consent, we will ensure our consent wording and mechanisms for obtaining and recording consents comply with the Data Laws.

6.2 Where we rely on consent for processing special categories of personal data, we will ensure that it is explicit (expressly confirmed in words rather than by any other positive action).

6.3 Whenever we request consent for processing, we will:

(a) present the request for consent in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language;

(b) not use pre-ticked opt-in boxes;

(c) not make services conditional on consent to the processing of personal data that is not necessary for the performance of that contract (for example, marketing);

(d) keep records of consent obtained so we can provide evidence if required;

(e) enable individuals to withdraw their consent at any time. Data Users should consult with the Legal Department if they receive a notification that an individual wishes to withdraw his or her consent.

6.4 We must be mindful when relying on consent to process children's personal data, particularly where providing online services to children under the age of 13, that we may need to obtain parental or guardian consent. Data Users should consult the Legal Department in relation to

any processing of children's personal data to ensure that relevant compliance steps are addressed.

7 Processing for Limited Purposes

7.1 Personal data may only be processed for the specific purposes notified to the individual when the data was first collected or for any other purposes specifically permitted by the Data Laws.

7.2 This means, broadly, that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, we will inform the individual of the new purpose before any processing occurs.

8 Notifying Individuals (Privacy Notices)

8.1 In order to satisfy the transparency requirements under the Data Laws, when collecting personal data directly from individuals, we will ensure that they receive appropriate information about how we will use their data.

8.2 We will inform them of the following:

(a) our name, the relevant contact for data protection queries and (where applicable) our representative in the EU;

(b) why we are processing their personal data and the lawful basis that applies (for example, consent or legitimate interests);

(c) if we are processing the personal data on the basis of our or a third party's legitimate interests, we must explain what those interests are;

(d) anyone we with whom we will share the personal data (either their name or a general description of them) – this includes any suppliers to whom we may pass the data;

(e) details of transfers of the data outside the EU and safeguards we have put in place (for example, contractual clauses);

(f) how long we plan to retain the personal data or the criteria used to determine the retention period bearing in mind our Data Retention Policy;

(g) their rights (see *Individual Rights* below);

(h) if they have given us consent, that they have the right to withdraw the consent at any time;

(i) their right to lodge a complaint with a supervisory authority;

(j) whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the data; and

(k) the existence of any automated decision-making which could have a legal or similar significant effect for the individual, and information about how decisions are made, the significance and the consequences.

8.3 If we receive personal data about an individual indirectly (for example, via third parties), we will provide the individual with the information in paragraph 8.2 above, as well as details of the categories of personal data we are processing and where we got it from (for example, whether it came from a public source), as soon as possible.

8.4 If we later need to use that personal data for a different or new purpose, we will tell the individual beforehand.

8.5 This information is normally given by way of a 'privacy notice' or 'fair processing notice'. There are some limited exceptions to this notice requirement. If in doubt as to whether a notice should be given, Data Users should contact the Legal Department who can confirm and provide the appropriate wording.

9 Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate and out-of-date data.

10 Minimal Processing and Data Retention

10.1 We will not collect excess personal data or retain data for longer than we need it. This means:

(a) we will only collect personal data to the extent that it is required for the specific purpose notified to the individual;

(b) we will not keep personal data longer than is necessary for the purpose for which it was collected; and

(c) we will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required, in line with our Data Retention Policy.

10.2 We will implement appropriate technical and organisational measures for ensuring that our systems allow us to do this.

10.3 We will also ensure that personal data is not automatically made accessible to an indefinite number of people and that access is limited appropriately.

11 Direct Marketing

11.1 Data Users involved with direct marketing should be aware that particular rules apply when sending electronic marketing to individuals (e.g. by SMS, email and where we call to sell services) and that we are required to comply with these rules.

11.2 This includes **any** advertising or marketing material targeted at a particular individual, including invitations to our events.

11.3 Where an individual hands us a business card, we will:

(a) ask them whether they are happy for us to keep in touch and send them invitations about events by email which may interest them;

(b) send their details to the Sales team and/or Marketing team to store centrally in our client relationship manager (**CRM**) system and marketing distribution database; and

(c) send an email shortly afterwards, acknowledging our meeting with them and saying that we will send them updates we think they may be interested in and that they can tell us at any time if they no longer want updates.

11.4 Unless:

(a) an individual has specifically signed up to receive marketing from us by email;

(b) an individual has given us their business card in the situation described above;

(c) we have an existing business relationship with them in relation to the services being marketed and gave them the opportunity to opt out of email marketing when we collected their details; or

(d) it is a business contact with a corporate email address (but not a sole trader or partnership),

we will not send any email marketing unless this has been specifically approved by the Legal Department.

11.5 Individuals have the right to ask us to stop us sending them marketing at any time. We will abide by any such request and notify the IT, Sales and Marketing teams whenever an individual opts out of receiving marketing, so they can update the CRM system and Marketing database accordingly.

11.6 Please contact the Legal Department for advice on direct marketing before starting any new direct marketing activity.

12 Individual Rights

12.1 We will observe and process all personal data in line with individuals' rights under the Data Laws, in particular the individual's rights to:

(a) request access to any personal data held about them and other supplementary information (see *dealing with subject access requests* below);

(b) have inaccurate or incomplete personal data corrected;

(c) object to us profiling them or sending marketing to them;

(d) withdraw their consent at any time;

(e) have their personal data erased from our systems;

(f) 'block' or suppress our use of their personal data;

(g) not to be subject to automated decisions (i.e. decisions made solely on a computer without human intervention) which produce legal effects or similarly significantly affect them, unless they have consented or another exception applies; and

(h) receive their data in a portable form.

12.2 Data Users should forward any requests or complaints received from individuals in respect of their personal data immediately to the Legal Department so that they can be dealt with within any mandatory legal timescales.

13 Data Protection Procedures

13.1 As part of the accountability principle, we are required to:

(a) keep records of processing we carry out;

(b) integrate privacy measures and security controls into our processing activities ('data protection by design and default');

(c) carry out a data protection impact assessment if our use of personal data is likely to result in high risk for the rights and freedoms of individuals; and

(d) ensure our systems have appropriate functionality to allow us to fulfil an requests made by individuals (for example, for access to their data).

13.2 The Legal Department should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are followed.

14 Data Security

14.1 We will ensure that appropriate measures are taken to keep data secure. Individuals may apply to the courts for compensation if they have suffered damage from such a loss and we may incur large fines if we are in breach of the Data Laws. You can also be liable personally for fines or imprisonment if you steal or recklessly misuse personal data.

14.2 The Data Laws require us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

14.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

14.4 Security procedures include:

(a) **Entry controls.** Any unfamiliar person seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind (personal data is always considered confidential).

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed or wiped when they are no longer required.

(d) **Equipment.** Data Users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

14.5 Generally, to keep personal data secure you must not disclose personal data - in writing or verbally - to anyone not authorised to receive it, whether internal or external, and whether within or outside the workplace.

14.6 In addition to this policy, Data Users must comply with our Information Security Policy, which sets out further information about how we keep personal data and other information secure.

15 Data Breaches

15.1 We have specific obligations to report any breach of security involving personal data to the data protection regulator, the ICO. If you suspect a breach, you should comply with our Data Breach Response Policy.

15.2 Data Users should notify the Data Breach team and/or the Legal Department immediately of any breaches of security which lead or could lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data – for example loss of a laptop or paper file, or sending an email to the wrong recipient. This will allow us to:

(a) investigate the failure and take remedial steps if necessary; and

(b) make any applicable notifications within the mandatory legal timescales.

The Notification form is available on the Group intranet. See the Data Breach Response Policy for more information.

16 Third Parties

16.1 We will only use processors (for example, sub-contractors) who:

(a) can assure us they meet the standards (including security standards) required by the Data Laws; and

(b) agree to comply with our procedures and policies, or agree to put in place adequate measures themselves.

16.2 A written contract must be put in place with certain mandatory clauses prescribed by the Data Laws. We have standard contracts that can be used, which can be obtained from the Legal Department.

17 Sending Personal Data Overseas

17.1 We may be asked to transfer personal data to third parties which are located overseas or international organisations or to sub-contractors based overseas.

17.2 The Data Laws impose restrictions on the transfer of personal data outside the EEA, to third countries or international organisations. Where we need to send someone's personal

data we hold outside the EEA or make it accessible to people outside the EEA, we will need to follow certain procedures.

17.3 Data Users should not transfer personal data overseas or to international organisations without first consulting the Legal Department, who can ensure that the correct procedures are in place.

18 Sharing of Personal Data

18.1 From time to time a Group company may be asked to share personal data we hold:

(a) with other members of the Group;

(b) with external providers, such as pension, insurance and occupational health providers;

(c) with a third party in the event that we, our business, or substantially all of its assets are acquired by such third party (in which case personal data about customers will be one of the transferred assets); or

(d) in order to comply with legal obligations, or in order to enforce or apply a contract with an individual or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

18.2 We will only share such information if we have a lawful basis and ensure we comply with any other relevant policies.

18.3 Where Data Users receive such requests, they should contact the Legal Department for assistance. Where appropriate, the relevant Group company or companies should enter into a data sharing agreement setting out their respective rights and obligations.

18.4 We may share personal data with processors in accordance with the terms of this policy (see *Third Parties* above).

19 Dealing with Requests from Individuals

19.1 Individuals may make a formal request for information we hold about them or other requests (for example, for portable data).

19.2 Data Users who receive a written request should forward it to the Legal Department immediately. If the request is made by telephone, Data Users should take steps to verify the caller's identity and where their identity cannot be checked, suggest that the caller put their request in writing. Data Users should not be bullied into disclosing information and should also forward such requests to the Legal Department.

19.3 Where a request for information is made in electronic form, we will need to provide the information in electronic form where possible, unless otherwise requested by the individual.

19.4 We will deal with requests for information and any other requests without undue delay. Within one month of a request for information, we will either:

(a) provide the information to the individual;

(b) if the complexity or number of requests requires, extend the response period by up to a further two months and inform the individual of such extension; or

(c) not action the information request, and inform the individual of the reason for not taking action and of the possibility for lodging a complaint or seeking a judicial remedy.

19.5 If requests are manifestly unfounded or excessive (particularly if they are repetitive), we may charge a reasonable fee to carry out the request or refuse to action the request but we must record our reasoning. Otherwise, initial requests will be dealt with free of charge, and we may consider charging a reasonable fee for further requests. The Legal Department can advise on whether a fee may or may not be charged in each case.

20 Consequences of Failing to Comply

The Group takes compliance with this policy very seriously. Failure to comply puts both Data Users and the Group at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, up to and including dismissal.