 **PULSAR® Data Protection Policy**

PULSAR® is the trading name of Praybourne Ltd. Registered in England No. 1421991. VAT Registration No. 378 2234 38

PULSAR®, Unit 2, Indurent Park, Norton Rd, Broomhall, Worcester, WR5 2QR UK

Tel: 01527 962012 | Email: sales@pulsaruk.com | Web: www.pulsaruk.com

**1. Introduction**

1.1 In the course of our activities Praybourne Limited trading as PULSAR® (“**the Company**”) collects, stores and processes Personal Data about:

* + 1. job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees; and
		2. third parties such as our customers and suppliers.

Data protection legislation imposes certain obligations on us and you relating to how we and you must handle Personal Data irrespective of whether such Personal Data is held on paper, on a computer or on other media.

1.2 In this Policy, Personal Data includes Personal Data which relates to any current, past or prospective job applicants, employees, workers, contractors, volunteers, interns, apprentices, former employees, customers, suppliers or any other person with which we or you have dealings.

1.3 We have prepared this Policy in order to inform you of our obligations under DP Legislation and your obligations as a Data User in respect of the obtaining, handling, processing, storage, transportation and destruction of Personal Data. Each of these activities constitutes “processing” of Personal Data under DP Legislation. This Policy informs you of our rules and procedures for processing Personal Data (for example, Personal Data of our job applicants, employees, workers, contractors, volunteers, interns, apprentices, former employees, customers and suppliers) and data security.

1.4 This Policy applies to all Data Users of the Company and should be read in conjunction with our IT, Communications and Systems Policy.

1.5 In this Policy:

1.5.1 “**Data User**” means those of our employees, workers, contractors, volunteers, interns and apprentices whose activities for the Company involve using Personal Data or accessing any part of the Company’s IT systems;

1.5.2 “**DP Legislation**” means the retained EU law version of the General Data Protection Regulation (EU) 2016/679 (as it forms part of the law of England and Wales), the Data Protection Act 2018, and all other data protection legislation having effect in the United Kingdom;

1.5.3 “**Personal Data**” means any information identifying an individual or information relating to an individual that can be identified (directly or indirectly) from that data alone or in combination with other identifiers in our possession or which we can reasonably access. Personal Data can be factual (for example, a name, postal address, email address, telephone number, location or date of birth) or an opinion about that individual's actions or behaviour; and

1.5.3 all references to the Company’s “**IT system**” are referring to the Company’s IT and telecommunications systems (including for the avoidance of doubt the Company’s email systems and online file storage system, and all cloud-based platforms used by the Company in connection with its business).

**2. The Law on** **Processing of Personal Data - the Key Provisions**

2.1 The main principles of DP Legislation are that Personal Data must be:

 processed fairly and lawfully and in a transparent manner;

 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

 accurate and up-to-date;

 kept only for as long as it is needed for the purpose for which it was collected; and

 processed in a way that ensures appropriate security of the Personal Data.

 We are required to demonstrate compliance with the above principles. In addition, Personal Data must be:

 processed in accordance with the rights of the individual to whom the Personal Data relates; and

 not transferred outside the United Kingdom or the European Economic Area unless adequate safeguards have been put in place to allow its export.

 Please see section 3 of this Policy below for further information about some of the above principles.

2.2 All of this means that we and you must take appropriate measures to ensure that Personal Data is kept secure and handled in accordance with the provisions of DP Legislation. You are responsible for ensuring that any Personal Data you provide to us is accurate and up-to-date and that you inform us of any changes to the Personal Data you have provided.

2.3 The person responsible for overseeing data protection compliance within the Company is Toni Nash (Credit Controller & HR) (tel: 01527 962012; email: toninash@pulsaruk.com). All new employees are required to undertake data protection training within their first month of joining us. Where appropriate, you will receive additional training in respect of our Personal Data handling and security procedures (e.g. if your role requires regular access to Personal Data).

2.4 Any queries relating to this Policy or the handling of Personal Data should be referred to Toni Nash.

2.5 If you consider that this Policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with Toni Nash.

**3. Data Protection Principles**

**Fair, Lawful and Transparent Processing**

3.1 The intention of DP Legislation is not to prevent the processing of Personal Data, but to ensure that it is processed fairly and without adversely affecting the rights of the individual to which the Personal Data relates. The individual must be informed about, among other things, the identity of the controller - i.e. Praybourne Limited trading as PULSAR® - along with the purposes for which the Personal Data is to be processed by us, and the identities or categories of anyone to whom the Personal Data may be disclosed or transferred. Such information must be provided through an appropriate privacy notice or fair processing notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that the individual can understand it.

3.2 In order for Personal Data to be processed lawfully, certain conditions have to be met. These may include, amongst other things, requirements that the individual has consented to the processing, or that the processing is necessary to comply with a legal or contractual obligation, or is necessary for the legitimate interest of the controller or the party to whom the Personal Data is disclosed. The processing of Personal Data concerning criminal convictions or special categories of Personal Data (which includes Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data and data concerning health or data concerning an individual’s sex life or sexual orientation) is prohibited unless certain additional conditions are met. In most cases the individual's explicit consent to the processing of such Personal Data will be required.

 Personal data relating to children should only be collected when specifically authorised by Toni Nash.

**Processing for Limited Purposes**

3.3 Personal Data may only be processed for the specific purposes notified to the individual when the Personal Data was first collected or for any other purposes specifically permitted by DP Legislation. This means 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 Personal Data is processed, the individual must be informed of the new purpose before any processing occurs.

**Adequate, Relevant and Non-Excessive Processing**

3.4 Personal Data should only be collected to the extent that it is required for the specific purpose notified to the individual. Any Personal Data which is not necessary for that purpose should not be collected.

**Accurate Data**

3.5 Personal Data must be accurate and kept up to date. Personal Data which is incorrect or misleading is not accurate and steps should be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Personal Data should be destroyed.

**Timely Processing**

3.6 Personal Data should not be kept for longer than is necessary for the purpose it was collected. This means that Personal Data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain Personal Data is likely to be kept before being destroyed or reviewed, please contact Toni Nash.

**Data Security**

3.7 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss, destruction or damage to, Personal Data.

3.8 DP Legislation requires 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. Personal Data may only be transferred to a third party data processor if we have carried out due diligence on the processor and the processor agrees to comply with those procedures and policies, or puts in place adequate measures itself. In addition, when appointing a processor we must ensure that appropriate contractual arrangements are in place and that any disclosure of personal data is appropriate in the circumstances. Any third party data processing or other third party data sharing arrangements must be approved by Toni Nash.

3.9 Maintaining information security means guaranteeing the confidentiality, integrity and availability of Personal Data, as follows:

3.9.1 "confidentiality” means that only people who are authorised to use the information can access it. **Personal Data is always considered confidential**;

3.9.2 "integrity” means that Personal Data should be accurate and suitable for the purpose for which it is processed; and

3.9.3 "availability” means that authorised users should only be able to access the information if they need it for authorised purposes. Personal Data should be stored in our IT systems and not on individual devices.

3.10 Security procedures include (but are not limited to):

3.10.1 Entry controls - any stranger seen in entry-controlled areas should be reported.

3.10.2 Secure lockable desks and cupboards - desks and cupboards should be kept locked if they hold confidential information of any kind. Keys for accessing such areas should not be left unattended at any time.

3.10.3 Methods of disposal - paper documents containing confidential information should be shredded or appropriately destroyed.

3.10.4 Records containing personal data (such as employees’ and customers’ details) which are stored electronically must be password protected. Hard copies should not be created unless needed in exceptional circumstances (in which case the hard copy should be stored securely when not in use - e.g. locked away or securely concealed in an upstairs room - and should be securely disposed of as soon as it is no longer required). Only authorised Data Users will be permitted access.

3.10.5 Equipment - Data Users must ensure that their devices do not show confidential information to passers-by and that they lock (via password) or log out of their device when it is left unattended or not in use (and all parts of our IT System should be logged out of at the end of the work day).

3.10.6 Data minimisation - we periodically review the Personal Data we hold. Any Personal Data which we no longer need, or which is held outside the retention periods detailed in our Data Retention Policy, will be disposed of.

3.10.7 Anonymisation/pseudonymisation - where appropriate, Personal Data should be anonymised or pseudonymised.

3.10.8 Encryption - Data Users must ensure that any Personal Data is encrypted before being transferred electronically from the Company’s IT system.

3.10.9 Non UK/EEA Transfers - Personal Data must never be transferred outside the United Kingdom or European Economic Area without specific authorisation from Toni Nash.

3.10.10 We have secure operating procedures in place to control the use of our IT systems (which includes home and mobile working).

**Processing in Line With the Rights of Individuals**

3.11 Personal Data must be processed in line with individuals' rights. Individuals must be provided with information regarding the processing of their Personal Data and (subject to limited exemptions) have a right to:

3.11.1 request access to any Personal Data held about them by a data controller (including but not limited to Personal Data held within their personnel file); and

3.11.2 rectification of inaccurate Personal Data.

 In certain circumstances, individuals may also have the right:

3.11.3 to erasure of Personal Data;

3.11.4 of data portability (i.e. to request the transfer of Personal Data to another party);

3.11.5 to object to the processing of Personal Data concerning him or her (including to prevent the processing of their Personal Data for direct marketing purposes);

3.11.6 not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her; and/or

3.11.7 to restrict the processing of Personal Data (for example to ask to suspend the processing of Personal Data to establish its accuracy or the reasons for processing it).

3.12 Any new proposed processing activities in relation to Personal Data (including the introduction of new systems used to store Personal Data) must (prior to implementation) be subject to a Data Protection Impact Assessment (supervised by Toni Nash) to assess and appropriately resolve any risks in relation to the implementation of such new activities.

**4. What Data Users can and cannot do with Personal Data of others**

4.1 All information (including but not limited to Personal Data) relating to our job applicants, employees, workers, contractors, volunteers, interns, apprentices, former employees, customers, suppliers and any other person with whom we or you, in your role as a Data User, have dealings is confidential information and belongs to the Company.

4.2 You must not access such information unless we have given you permission to do so.

4.3 Information about our job applicants, employees, workers, contractors, volunteers, interns, apprentices, former employees, customers, suppliers and any other individual who has dealings with us must not be disclosed to any third party or to the person to whom it relates except in accordance with this Policy and our authorised procedures. For example, you must never assume that it is acceptable for a husband to be given Personal Data about his wife; they may be estranged or simply wish to keep their affairs separate**. In the event that you receive a request from a third party for disclosure of, or to inspect, Personal Data relating to any individual (including but not limited to job applicants, employees, workers, contractors, volunteers, interns, apprentices, former employees, or third parties such as customers or suppliers) you should refer the request to Toni Nash immediately**. You should make such a referral in all cases and should not respond to the request regardless of the identity of the requestor (including where the requestor is the police or any other government agency or public authority) as we have a set procedure for responding to such requests that must be followed.

4.4 Subject to paragraph 4.3 above, if you are in any doubt as to the identity of an individual, you must verify his or her identity before disclosing Personal Data to him or her. In any event, you should never give any Personal Data to anybody over the telephone regardless of the identity of the person making the request.

4.5 You may only share Personal Data with other employees of the Company if the recipient has a job-related need to know the information.

4.6 When making electronic records of Personal Data you must save them in the relevant areas of our IT system and not locally on the device’s hard drive. Manual records must be stored in a secure filing system.

4.7 Personal cloud based services such as OneDrive or Dropbox must not be used by Data Users to store or transmit Personal Data.

4.8 You must ensure that, in respect of each device used by you to access any part of the Company’s IT systems:

(a) you maintain the device’s original operating system and promptly install all updates and security patches upon them becoming available;

(b) you use an up-to-date anti-virus program and perform regular virus scans on such device;

(c) you immediately erase any Personal Data that is inadvertently downloaded to such device and ensure that no Personal Data has been inadvertently backed up locally to such device or to any personal cloud-based storage services when you have backed up such device. You must immediately delete any such backups that are inadvertently created; and

(d) you must not use such device to access any part of our IT systems using publically available Wi-Fi (such as Wi-Fi on public transport or in cafes).

4.9 Hard copies of information should not be taken from our electronic filing systems unless absolutely necessary and where they are taken they must be kept in a secure location.

4.10 You must not leave information relating to our job applicants, employees, workers, contractors, volunteers, interns, apprentices, former employees, customers or suppliers in open view where others can see it. For example, electronic devices at locations where people other than sufficiently authorised Data Users can see them should not be left unattended. The screen should not be visible to any third party except as required to carry out the transaction in question.

4.11 Information must not be copied manually or onto an electronic storage device (such as a portable hard drive, USB drive, CD-ROM, DVD-ROM or MP3 player) except as specifically authorised by Toni Nash*.* In the event that any information is copied onto any such device it must be encrypted before being removed from the premises and the transportation of such device must be authorised by Toni Nash, logged and inventoried. Any electronic storage devices that are no longer required must be handed over to our IT department so that they can arrange for the relevant device to be wiped or destroyed as appropriate.

4.12 If you use a laptop, tablet computer or other hand-held device away from our premises you must take appropriate additional precautions to safeguard the security of Personal Data. Such precautions include but are not limited to keeping the device either with you or in a secure location at all times. Documents, laptops, tablet computers and other devices containing Personal Data should never be left unattended in vehicles (even when the vehicle is parked at your home). In the event that any such document or device is lost or stolen, or you believe that it may have been accessed by an unauthorised person or otherwise compromised, you must report it to Toni Nash.

4.13 In the event that we provide you with a mobile telephone, laptop, tablet computer or other electronic device, you shall only use such a device in accordance with our instructions and you shall not use such a device for any unauthorised purpose.

4.14 You must not send or copy any confidential information relating to the Company (including but not limited to Personal Data relating to our job applicants, employees, workers, contractors, volunteers, interns, apprentices, former employees, customers or suppliers) to any third party without specific authorisation from Toni Nash (unless otherwise in accordance with our standard procedures)*.* This includes sending or copying information to any non-Company email address and any device or system not owned and operated by the Company.

4.15 You must comply with our confidential waste disposal procedures (such as shredding) and ensure that confidential documents are not simply disposed of with the non-confidential waste.

4.16 Any request or complaint from an individual regarding personal data that we hold about them, and any other correspondence of the nature referred to in paragraphs 3.11.1 to 3.11.7 above, must be dealt with in accordance with this Policy. Any Data User who receives a request or complaint (whether in writing or otherwise) should forward it to Toni Nash immediately and not respond directly to the request.

**5. Post**

All post received at our premises, whether or not marked strictly private and confidential and/or for the attention of an individual employee, may be opened and inspected prior to distribution. You should be mindful of this if you ask for personal items or correspondence to be delivered to our premises.

**6. Data Retention**

6.1 We will only retain Personal Data for as long as we need it for the purpose for which it was collected. Whilst taking into consideration our legal obligations, we will on an ongoing basis: review the length of time we retain Personal Data for; consider the purpose or purposes for which we hold the Personal Data for in deciding whether (and for how long) to retain it; securely delete Personal Data that is no longer needed for such purpose or purposes; and update, archive or securely delete information if it goes out of date. For further information on retention periods please contact Toni Nash.

6.2 Any movement of records to a different location to which it is normally held must be recorded in order that such record can be easily retrieved at any time.

6.3 Any migration of records containing Personal Data to a new location or to a new platform must (prior to implementation) be subject to a Data Protection Impact Assessment (supervised by Toni Nash) to assess and appropriately resolve any risks in relation to the migration of such records.

**7. What you should do if you discover a data protection breach**

If you become aware that:

7.1 a device previously used to access any of our IT systems has been lost or stolen, or if you believe that any such device may have been accessed by an unauthorised person or otherwise compromised;

7.2 there has been unauthorised access to any element of our IT systems, premises or any other location where Personal Data is stored;

7.3 any Personal Data has been disclosed or accessed in error;

7.4 there is an IT threat (for example, if you have received a phishing email); or

7.5 Personal Data has been compromised in any other way,

you must report the incident toToni Nash immediately. In some circumstances we may be required to report the breach to the Information Commissioner’s Office and the individual(s) concerned. The Company will record all reported data breaches regardless of their effect.

**8. General**

8.1 This Policy does not form part of any contract and it may be amended by us at any time. Any changes will be notified to you in writing.

8.2 If you are found to be in breach of the terms of this Policy you may be subject to disciplinary action (which, in serious cases, or in cases of repeated breach, may result in dismissal). If you are in any doubt about the terms of this Policy or have any questions about data handling, data security, monitoring or communications, please ask Toni Nash for further guidance.

8.3 We will continue to review the effectiveness of this Policy to ensure it is achieving its stated objectives.