DATA PRIVACY POLICY
Verus Petroleum UK Limited (the "Company")

1. INTRODUCTION

Every business like ours will process some level of personal data as part of the management of staff and dealings with business partners and other third party organisations. If we as a business allow our data privacy standards to slip, this can leave individuals vulnerable to identity theft, fraud, financial loss, and loss of confidentiality. It can also lead to serious reputational damage for the Company, and legal action being taken by individuals and the Information Commissioner's Office. Ultimately, the Company could face fines of up to €20,000,000 or 4% of annual worldwide turnover for a breach of data privacy legislation.

This data privacy policy enshrines key principles to ensure that personal data is processed lawfully, securely and in a way that instils confidence in Company procedures. All staff are expected to comply with this policy and any other Company guidelines, procedures and rules which are signposted in this policy, or which otherwise regulate our processing of personal data.

This policy applies to the processing of personal data by automated means as well as in manual files. However manual files which are not structured in accordance with any specific criteria are not covered.

Any failure to comply with this policy may result in disciplinary action for our employees, and termination of engagement for other Company personnel. This policy does not form part of any individual's contract of employment or engagement and may be amended by the Company at any time.

2. DEFINITIONS

In this data privacy policy:

"**Data Protection Officer**": means Colin Christie, Finance Director who is responsible for data protection matters within the Company, and who may be contacted on 01224 659122 or colin.christie@veruspetroleum.com

"**personal data**" means any information relating to an identified or identifiable natural person. "personal data" includes data which could be attributed to a living person if additional data was provided;

"**personal data breach**" means a breach of security leading to the accidental or unlawful destruction, loss alternation, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"**processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure

by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**sensitive personal data**" means any personal data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation.

"**staff**" means employees, workers, consultants, officers, independent contractors or any other individual providing their service or services to the Company.

3. KEY PRINCIPLES

As a data controller, the Company is responsible for upholding six key principles when processing the personal data of any individual, as set out below. The Company must be able to demonstrate its compliance with these principles when called upon.

(a) First Principle: Lawfulness, fairness and transparency

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

Lawfulness and fairness

Personal data should only be processed if there is a lawful ground for doing so. Lawful grounds which the Company will commonly rely on are where the processing is necessary for: (i) the performance of a contract with the individual (e.g. their employment contract); or (ii) compliance with the Company's legal obligations; or (iii) pursuing the Company's legitimate interests where these are not overridden by those of the individual. In certain limited circumstances, the individual's consent can provide a lawful ground for processing.

When the Company processes information regarding criminal convictions and offences or sensitive personal data (such as information about an employee's health) additional conditions apply.

If you have any questions regarding whether any processing (or proposed processing) of personal data complies with this first principle – these should be put to the Data Protection Officer in the first instance.

Transparency

The Company must make sure that when personal data is collected (either from the individual or from a third party), that certain specified pieces of information are provided to that individual including such matters as our contact details, the provenance of the personal data, the purpose and lawful basis of processing, retention periods and the individual's rights over their data. Information and communications regarding processing should be accessible and easy to understand in clear and plain language.

This notification to the individual is normally carried out by way of a Company "privacy notice", but there are certain situations when such notification is not required. For more details regarding the need for a privacy notice, its content and timing, please contact the Data Protection Officer.

(b) Second Principle: Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Careful consideration must be given to the question of whether processing for another purpose is compatible with the purpose for which the personal data was originally collected.

(c) Third Principle: Data minimisation

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

Staff must only process personal data to the extent required by their role, and must process it for a purpose compatible with that for which it was originally collected.

(d) Fourth Principle: Accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

All staff have a responsibility to make sure that they check their personal details (as maintained by the Company on any relevant server or filing system) on a regular basis to make sure they are up to date.

(e) Fifth Principle: Storage limitation

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed, taking into account any ongoing need for it, and our legal obligations. Please refer to our document retention policy.

(f) Sixth Principle: Integrity and Confidentiality

Personal data must be processed in a manner that ensures appropriate security is in place to protect it, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Measures may include such steps as encryption and pseudonymisation of personal data where appropriate. Staff must comply with cyber security measures as described in our IT End User policy. Staff should be wary of any party requesting personal data and appropriate identity checks must be carried out before any request is actioned.

Any third party who processes personal data under the Company's instructions, or in the course of providing services, must be party to a written contract with the Company which provides adequate safeguards for the protection of personal data, and which is compliant with this policy and local data privacy laws.

4. DATA PROTECTION BY DESIGN AND DEFAULT

Data protection should be at the heart of everything we do.

This means the Company should implement appropriate technical and organisational measures which are designed to implement the six data protection principles above in an effective manner and to integrate the necessary safeguards into processing so as to protect the rights of individuals over their personal data. This implementation must be done at the time both when the Company is determining the methods of processing, and at the time of processing itself. Due consideration must be given to the circumstances behind the processing, the technology available, the cost of implementation of protective measures, and the size of the risk posed to individuals by our processing activities.

The Company should also ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

Where a type of processing (in particular using new technologies), is likely to result in a high risk to individuals, the Company shall prior to the processing carry out an assessment of the impact of the envisaged processing operations on the processing of personal data.

5. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Any transfer of personal data (which is undergoing processing or is intended for processing after transfer) to a country outside the European Economic Area or to an international organisation shall only be carried out if appropriate safeguards are in place, such as by putting in place standard data protection clauses approved by the European Commission or by the use of binding corporate rules.

6. RECORDS, AUDIT AND TRAINING

The Company shall maintain records of processing activities under its responsibility (including but not limited to records of consents to processing provided by individuals), and shall ensure that any third party processing data on its behalf does the same. The Company shall carry out regular tests to assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of processing. Appropriate levels of training shall be provided to staff on data protection matters.

7. DATA SUBJECT RIGHTS

All individuals (including staff and members of the public) have rights in relation to any personal data which we might be processing about them, as set out below.

- **Transparency** – Individuals have the right to receive certain specified information when we collect data from them or from a third party (see First Principle above).
- **Right of access** – Individuals have the right to obtain confirmation from us as to whether we are processing their personal data, together with confirmation as to other matters relating to the data and their rights over it.
- **Right of rectification** – Individuals have the right to obtain the rectification of inaccurate personal data, or to have imcomplete data completed.
- **Right to erasure and restriction** – In certain situations, individuals have the right to obtain from us the erasure of their personal data and/or the restriction of its processing.

- **Right to data portability** – In certain limited situations, individuals have the right to receive their personal data (which they have already provided to us) in a structured, commonly used and machine-readable format, and have it transmitted to another data controller.

- **Right to object** – Individuals have the right to object to the processing of their personal data in certain circumstances (including for the purposes of direct marketing).

- **Right to avoid automated decision-making** – Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them.

- **Right to withdraw consent** – Individuals have the right to withdraw consent where it has previously been provided to the Company.

These rights of the individual must be balanced against the rights of the Company to reject a request (in whole or in part) on certain lawful grounds, and to charge a fee where permitted to do so.

If you wish to exercise any of these rights, or if you become aware of such a request as part of your role, you should contact the Data Protection Officer or Human Resources. Appropriate identity checks should be carried out on the individual making the request.

8. PERSONAL DATA BREACH

During the course of our operations, staff may discover that a personal data breach has occurred. If this happens, staff must contact the Data Protection Officer as soon as possible and should preserve all relevant evidence. The Data Protection Representative shall be responsible for deciding what, if any, action should be taken in response to the breach including measures to mitigate its impact and whether to notify the Information Commissioner's Office or relevant individuals who may be affected.

9. QUESTIONS

Queries regarding any aspect of this policy should be directed to the Data Protection Officer whose contact details may be found on the first page of this policy.