GENERAL DATA PROTECTION POLICY

Hughes and Salvidge Holdings Ltd (The Company), is registered under the Data Protection Act.

Statement of the Company Duties and Scope:

The Company is required to process relevant personal data regarding members of staff, applicants, sub-contractors, suppliers and customers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Data Protection Controller:

The Company has appointed a Data Protection Controller (DPC) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy. The Company recognises The General Data Protection Regulations (GDPR) and will comply with that directive as follows:

The Principles:

The Company shall so far as be reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Definitions:

- The Company is 'Hughes and Salvidge Holdings' and includes H&S Metals, Aasvogel, K&B Crushers and Valley Trading. It additionally covers subsidiaries and affiliated bodies where the Data Protection Act applies
- Data Subject, an individual who is the subject of the personal data

Personal Data:

Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for employment such as the member of staff's name and address and details for payment of salary or a staff attendance record and exam results. Personal data may also include sensitive personal data as defined in the Act.

Processing of Personal Data:

Consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data, and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent. If a staff member wishes to revoke or change consent they must agree a specific agreement on how their data is to be processed with the data processor.
The Company may, from time to time, be required to process sensitive personal data. Sensitive personal data includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings.

Rights of Access to Information:

Data subjects have the right of access to information held by the Company, subject to the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000. Any data subject wishing to access their personal data should put their request in writing to the DPC. The Company will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within 40 days for access to records and 21 days to provide a reply to an access to Data Protection Policy information request. The information will be imparted to the data subject as soon as is reasonably possible after it has come to the Companies attention and in compliance with the relevant Acts.

Exemptions:

Certain data is exempted from the provisions of the Data Protection Act which includes the following:

- National security and the prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or

imposed by law upon the Company, including Safeguarding and prevention of terrorism and radicalisation

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPC.

Accuracy:

The Company will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the data processor of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

Enforcement:

If an individual believes that the Company has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the member of staff should utilise the Company grievance procedure and should also notify the DPC.

Data Security:

The Company will take appropriate technical and organisational steps to ensure the security of personal data. All staff will be made aware of this policy and their duties under the Act. The Company and therefore all staff are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and be Data Protection Policy Lent encrypted when transported offsite. Other personal data may be for publication or limited publication within the Company, therefore having a lower requirement for data security.

Attention is also drawn to the existence of the IT Security Policy, which provides more specific information on digital data protection and best practice guides.

External Processors:

The Company must ensure that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this policy and the relevant legislation.

Secure Destruction:

When data held in accordance with this policy is destroyed as required by regulations or retention dates, it must be destroyed securely in accordance with best practice at the time of destruction.

Data Breaches:

Data breaches must be informed to the ISO within 72 hours or reasons must be given if there is a delay this will cover risks to data subjects which will include damage to reputation or financial loss.

Retention of Data:

The Company may retain data for differing periods of time for different purposes as required by statute or best practices, individual departments incorporate these retention times into the processes. Other statutory obligations, legal processes and enquiries may also necessitate the retention of certain data. The Company may store some data such as site files, photographs, medical history and accident/incidents indefinitely in its archive.

CCTV:

The Company owns and operates a CCTV network for the purposes of crime prevention and detection, and Safeguarding. This is static within the H&S Metals yards with mobile systems erected on sites where requested by the clients.

Signed: **Martyn Burnett, Managing Director**

Issue Date: 25th May 2018
Review date: January 2019