HAZARDOUS CONSULTING LTD DATA PROTECTION POLICY

Rational

Hazardous Consulting Ltd (HC) is committed to a policy of protecting the rights of individuals, clients and subcontractors in accordance with the General Data Protection Regulation (GDPR) May 2018. The new regulatory environment demands higher transparency and accountability in the way organisations manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use. The GDPR contains provisions that HC will need to be aware of as data controllers, including provisions intended to enhance the protection of personal data.

HC needs to hold information for the following purposes:

1. Compliance with legal requirements for example producing a set of accounts
2. Project management of contracts
3. Purchase of goods and services.

To comply with its legal obligations, including the obligations imposed on it by the GDPR, HC must ensure that any information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all employees of HC.

As a matter of best practice, any other companies and individuals working with HC who have access to personal information will be expected to read and comply with this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

This piece of legislation came in to force on 25th May 2018. The GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals, for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

Data Protection Principles

The legislations places a responsibility on us to process any personal data in accordance with eight principles:

1. **Process personal data fairly and lawfully.** HC will make all reasonable efforts to ensure that individuals who are the focus of the personal data are informed of the purposes of the processing, any disclosures to third parties that are envisaged, given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this process. We will ensure that the reason for which we collected the data originally is the only reason for which we process those data, unless the individual is informed of any additional processing before it takes place.

3. **Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.** We will not seek to collect any personal data which is not strictly to the purpose for which it was obtained. Forms for collecting data will be drafted with this in mind. If any relevant data are given by individuals, they will be destroyed immediately.

4. **Keep personal data accurate and, where necessary, up to data.** We will review and update all data on a regular basis. It is the responsibility of the individuals giving their person data to ensure that this is accurate, and individuals should notify us if data needs to be updated. It is our responsibility to ensure that any notification of change is noted and acted upon.

5. **Only keep personal data for as long as is necessary.** We will not retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means we will undertake a regular review of the information held and implement a weeding process. We will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (eg secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

All personal data will be deleted or destroyed by us after three years of no contact, unless it is needed for safeguarding purposes.

6. **Process personal data in accordance with the rights of the individual under the legislation.** Individuals have various rights under the legislation including a right to:

- Be informed upon request of all the information held about them within 30 days.
- Prevent the processing of their data for the purposes of direct marketing.
- Compensation if they can show that they have been caused damage by any contravention of the Act.
- The removal and correction of any inaccurate data about them.
- Be forgotten and removed from the database at their request as long as this is fair and reasonable.

We will only process personal data in accordance with individuals' rights.

7. **Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.** We will ensure that any personal data which we hold is kept securely and not disclosed to any unauthorised third parties. We will ensure that all personal data is accessible only to those who have a valid reason for using it. We will have in place appropriate security measures:

- Keeping all personal data in a secure location
- Password protecting personal data held electronically.
- Archiving personal data which are then kept securely.

In addition, we will put in place appropriate measures for the deletion of personal data – manual records will be shredded of as 'confidential waste'. Hard drives of redundant PCs will be wiped clean before disposal or if that is nor possible, destroyed physically. A log will be kept of the records destroyed.

8. **Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA).** This also applies to publishing information on the Internet – because transfer of data can include placing data on the website that can be accessed from outside the EEA – so we will always seek the consent of individuals before placing any personal data (including photographs) on our website.

Consent as a basis for processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. We understand consent to mean that the individual has been fully informed of the intended processing and has signified their agreement whilst being of a sound mind and without having any undue influence exerted upon them. Consent will not be inferred from the non-response to a communication.

Where an individual has consented to being contacted by HC, that persons consent will remain current until he/she advises us otherwise. However an individual can opt out by sending a letter to 4 Greenhead Tce, Chopwell, Newcastle upon Tyne NE17 7AH or an email to mark@hazardousconsulting.co.uk

Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to GDPR May 2018 and Data Protection Act 1998