Data Processing

We recognise that under the Data Protection Act 2018 (DPA) & the General Data Protection Regulation (GDPR), we are a data controller, and in some circumstances a data processor as well. The following sets out our contract with you regarding our activities as your data processor. If you would like to know more about the steps we take to protect your data as a data controller, please read our 'Terms of Website Use' available on home page of KAHSC Website.

We provide data processing services through our secure website, via email and by post. The table at the end of this section describes the core processing activities we carry out for you and describes some of the terms of this contract.

The **duration of the processing** we do for you is limited to the term of our contract with you. At the end of your contract, you must choose whether you want us to erase your data or return your data to you, and tell us in writing what you have decided. Your access to your data via our website will cease the day after your contract expires and we will mutually agree the method of any data return and a reasonable timescale within which it must happen. This does not affect your statutory rights over your data as the data controller and your data will be securely erased or returned to you as immediately as possible after suitably secure arrangements are agreed for the transfer. If you decide not to renew a contract with us, we will be sorry to lose a valued client and we strongly recommend advising us of your intention at least 14 days before your contract end to ensure seamless retention of full access to your data. Where there has been a problem with the provision of any data processing service, we will keep relevant data that belongs to you even after our contract has ended, but only in line with Article 9(2)(f) which outlines our right to a legal defence e.g. the period throughout which a claim relating to our processing of that data could be brought against us (6 years).

As the data controller you have the right to:

Control over the processing of your data

- We will only act on your written instructions. By agreeing to this contract you will have generally instructed us in writing to carry out processing activities for you as detailed in the table at the end of this section. We require further written expression of your instructions for non-routine and task specific processing before such processing can be carried out: for example, analysis of a wellbeing survey or review of specific documentation pending a visit from the Local Authority Fire Officer. This written instruction will usually be your email request for the work to be done. The only exception to this right to control the processing of your data is where another law requires us to do so without your consent e.g. providing it to the Police as part of a lawful investigation.
- We will only engage a new sub-processor of your data with your prior consent and under written contract.
- If our processor uses a sub-processor of their own, we will impose contractual terms on them which meet Article 28.3 of the GDPR and they will be fully liable to us in the processing of your data.
- If we make any changes to the ways in which we work with our existing sub-processors we will tell you about them before they take place and we will give you the opportunity to object.
- We undertake to ensure provision of continuous access to your data held online, except in limited circumstances entirely beyond our control: for example the reasonable duration of a service interruption caused by natural disaster affecting servers, or when your technical failure prevents you accessing your data even though we have maintained its availability i.e. your information is live and available online but you cannot access the internet.

Confidentiality

- Our employees, including temporary or agency staff are bound by their employment contracts to keep your data confidential and this duty reasonably extends beyond the term of their employment i.e. they cannot lawfully retain any of your data after they are no longer employed by us.
- We include such confidentiality clauses with any sub-processors we employ to process your data.

- We can identify the processing activities of any website user through our website access monitoring logs. Our employees and processors understand that anyone found to have carried out unauthorised or unlawful processing activities will be subject to disciplinary action and may be further subject to legal action or prosecution.

Security of your data processing

- Our e-mail server and e-mails are secure and protected by nationally recognised software - https, ESET Endpoint Security, virus checker etc.
- Our website, where most of the processing of your data is done, has an HTTPS and secure padlock in its address bar which indicates that it is secured with an SSL Certificate. There are many steps involving issuance and verification of a Certificate.
- We operate a strict user password policy in line with standard children's workforce policies on the use of Information Technology and data protection and we require all users to fully comply e.g. passwords should be suitably strong, not shared etc.
- We additionally secure your sensitive personal data on our website by restricting the number of users who can access it. We employ the technical measure of providing different levels of access to individual user accounts e.g. only users with accident administrator access enabled on their user account can see data associated with accident and incident records etc. The success of this technical measure will depend in part on the organisational measures you employ e.g. the number of users you authorise us to set up for you and the levels of access you request for them.
- In case a user should fail to log out of our secure access website, it has a time-out feature set at 30 minutes of inactivity, after which the user must re-enter their password to continue website access.
- Our website is backed up daily in the UK. Our document server is backed up daily, both manually and via the cloud.
- Our email system is not encrypted to protect personal data, so we employ other technical or organisational measures such as emailing password protected files, fax or other secure method as agreed with you on a case by case basis.
- We use the Royal Mail services to send personal data in properly sealed and addressed packages by post. Sensitive personal data is additionally protected by being addressed to the named individual it is meant for, being marked private and confidential, and by using a tracking service where necessary.

Assistance to meet your obligations to your data subjects under Chapter 3 of the GDPR.

- We provide accident & incident and personnel training records. Data input to the online accident & incident reporting system & approval system can be exported by you at any time into a pdf summary which can be printed or saved to an electronic device. Statistical summary data from both systems and from the Training Records And Calendar (TRAC) system can be exported by you at any time into a spreadsheet. It can be filtered by personal or location data but you can also freely pseudonymize all exported data by deleting columns containing names. This data can also be printed or saved to an electronic device. Providing your data in these easy to access formats, which you control the creation of, should help you comply with any Subject Access Request you receive independently and without our direct assistance.
- We will update any of your personal data that we process within 5 working days of receipt of the written request e.g. the new married name of an employee.
- Where your data subject is entitled to object to processing, we will stop processing their data within 3 working days of the receipt of your written request to do so. It is your responsibility to ensure that your data subject has this right before you ask us to erase any data. Personal data which has been permanently erased from our website or office servers will not normally be recoverable.

Audit and inspect

- We undertake to tell you, as soon as is reasonably practicable, that an instruction you have given us is not compliant with the GDPR or a related data protection law. This does not extend to your requests for us to erase data which arise as a result of your compliance with a request from your

data subject to erasure of their data where we cannot reasonably be expected to know how you determined their right to be lawful.

- This contract performs the key function of our undertaking to provide you with the information necessary to show that we are both meeting our obligations regarding the processing your data under Article 28 of the GDPR. We will also provide any necessary supplementary information that you request and can submit to your reasonable audit requirements to ensure this if desired. You must set out such requirements to us in writing in a timely manner.

As the data controller your obligations are to:

- Provide us with accurate personal data and all necessary corrections in a timely manner compliant with the GDPR.
- Employ appropriate technical and organisational security measures when providing us with personal data and when using personal data covered by the GDPR and this contract for the processing of it.
- Only request user access to our website for employers and employees at a level commensurate with their work tasks and responsibilities, and with due regard to the requirement under the GDPR to restrict access to personal data i.e. have the fewest possible users who are authorised and enabled to access the accident & incident reporting system which contains sensitive health data.
- Respond promptly to the annual data correction request where we provide you with the data we hold regarding your authorised users and you provide your updated and accurate written instruction regarding the continued access to data that you require.
- Require your users of our website to comply with strict password security measures e.g. length, complexity, not shared etc. and to take appropriate action regarding any breaches.
- Advise us as immediately as possible of the need to remove any relevant security access i.e. to your data on our website, from individuals who no longer have any legal right or your authority to have such access e.g. employees who have left your employment.
- Ensure your users of our website understand their responsibilities with regard to the DPA and the GDPR. Anyone found to have carried out unauthorised or unlawful processing activities must be made aware that they will subject to disciplinary action by you and may be further subject to legal action or prosecution.
- Inform us as immediately as possible if we need to assist you to comply with a Subject Access Request.
- Inform us as immediately as possible if we need to stop processing the personal data of any of your data subjects.
- Ask us to stop processing the personal data of any of your data subjects only after you have established to your own satisfaction that your request is compliant, not only with the GDPR but with other applicable laws or legal rights e.g. a data subject had no legal right to request all record of an accident be destroyed because it conflicts with the right to a legal defence.
- Understand that our duty to assist you in meeting your obligations to your data subjects under Chapter 3 of the GDPR is limited by the nature of the processing we do for you and the information available to us.
- Inform us in a timely manner of your requirement for us to erase or return your data to you at the end of your contract with us.
- Pay the full costs of any extraordinary measures required to recover erased data where you have failed to ensure that you had the lawful right to ask us to erase it, but we did so as per your written instructions and you later requested recovery of it e.g. the hiring of a data salvage expert.

Kym Allan, Health & Safety Consultants Ltd. Processing Activities Summary

The subject matter	The nature of the processing	The purpose of the processing	The types of personal data processed	The categories of data subjects about whom data is processed
Accident and incident data	An online recording and reporting system.	Secure storage and sharing of accident & incident data, notifying HSE of reportable incidents on your behalf, data analysis for trends, and the provision of relevant advice.	Personal data e.g. name, date of birth, address, contact details, location. Sensitive personal data e.g. injuries, medical needs, first aid treatment.	Employees, volunteers, contractors, other lawful & unlawful visitors, witnesses, and affected members of the public e.g. the occupants of another vehicle etc.
Personnel training data	An online recording and reporting system.	Secure, storage, sharing and transfer of personnel training, to enable you to monitor staff training & volunteer competence, and to generate a reminder about expiring training.	Personal data e.g. name, qualification, performance, candidate number, location, and trainer identification numbers & names.	Employees, volunteers and training providers.
Your documentation e.g. policies, procedures	Reviews on request only.	The updating or improvement of the documentation you give us expressly for that purpose.	Names, location and contact details.	Employees and occasionally external personnel e.g. named contractors,