Company Policy – Customer Data Protection Policy

This policy provides information on how Scientific Services Ltd collects and processes your personal data when you use our services.

1. Important information and who we are

Scientific Services Ltd is the controller and responsible for your personal data.

We have appointed a data protection officer (DPO). If you have any questions about this data protection policy or our data protection practices, please contact the DPO.

Our full details are:

- Scientific Services Ltd, a company registered in England and Wales with company number: 04367494, whose registered office is The Fuel Depot, Scorrier, Redruth, Cornwall, TR16 5UT
- Our DPO is our Managing Director
- Email address: datacontroller@scientificservices.org
- Postal address: Scientific Services Ltd, The Fuel Depot, Scorrier, Redruth, Cornwall, TR16 5UT
- Telephone number: 01209 311350

2. The data we collect about you

- Information collected by us

  In the course of providing our services to you, we collect the following personal information when you provide it to us:

  - Your name, residential address and contact details
  - Card payment details

- Information collected from other sources

  We also obtain personal information from other sources as follows:

  - Many of our customers subcontract testing and surveying activities to us. They may provide your name, residential address and contact details subject to the work being undertaken.

3. How we use your personal data

We will only use your personal data for the purpose for which we collected it which include the following:

- To register you as a new customer.
- To provide our services to you.
- To manage your relationship with us.
- To improve our website, products/services, marketing or customer relationships.
- To recommend products or services which may be of interest to you.

4. How we share your personal data

We may share: -

- Your name, residential address and contact details

We may do so because: -

- It is essential for the operation of The Electronic Asbestos Management System (TEAMS) Client Portal. We store your information with them because this allows you access through the client portal. You are able to see all the information the portal holds on you. Please see more specific information on the operation of the TEAMS client portal below.
- We may be required to provide such information to sub-contractors (e.g. asbestos removal specialists) in order to, for example, receive quotations for services additional to or ancillary to our services or arrange the instruction of such services on your behalf.
- If required by applicable law, we may share personal information with Law Enforcement or other authorities, such as the Health & Safety Executive.
- We will not share your personal information with any other third party.

5. TEAMS Client Portal Specific Protection

The TEAMS Client Portal is hosted by Mark One Consultants Ltd, Unit 5-6, Bartlett Court, Sea King Road, Lynx Trading Estate, Yeovil, Somerset, BA20 2NZ. Mark One Consultants also act in the capacity of both TEAMS software developers and online security consultants.

The TEAMs Client Portal is hosted on a secure server and is accessed through a secure gateway, denoted by the 'https' URL prefix and the image of a padlock on the address bar.

Mark One Consultants and Scientific Services are signatories to a separate non-disclosure and confidentiality agreement which includes the TEAMS portal and servers.

User access is achieved by the named client representative requesting access, in writing and includes the following information:

- Name(s) of third party;
- Email address(es) of third party;
- Level of required access;
- Date access required from;
- Date access should be rescinded.

We will then set up the correct level of access and provide an individually generated password which is emailed directly to the named user.

It remains your responsibility to ensure that user details and access levels required are kept current and up to date and that you notify us if any access requires removal.

Authorised third party access

Only those persons with a valid username and password can access the portal, this includes the employees of Scientific Services Ltd and Mark One Consultants.

If third party access is required as requested by a client, this request must be received in writing and include the following information

- Name(s) of third party
- Email address(es) of third party
- Level of required access
- Date access required from
- Date access should be rescinded

6. How long your personal information will be kept

We will not retain your personal information for any longer than we feel is necessary.

In relation to any personal information held in the TEAMS Client Portal described above, data uploaded to the Client Portal by any party will be retained until such time as notice is received in writing from us that the data is no longer required.

In the event that you no longer wish to use our services, but do require continued access to the portal, the access and all responsibility for the data stored on the portal will transfer to you.

7. Reasons we can collect and use your personal information

We need all the categories of information listed above primarily to allow us to **perform our contract with you** and to enable us to **comply with legal obligations**. In some cases, we may use your personal information to **pursue legitimate interests of our own or those of third parties**, provided your interests and fundamental rights do not override those interests.

8. International transfers

We may transfer your personal information to external third parties based outside the European Economic Area (EEA), so their processing of your personal data will be outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring appropriate safeguards are implemented.

We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.

Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.

Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between Europe and the US.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

9. Your legal rights

Under the *General Data Protection Regulation,* you have a number of important rights free of charge. In summary, those include rights to:

- fair processing of information and transparency over how we use your use personal data
- access to your personal information and to certain other supplementary information that this Privacy Notice is already designed to address
- require us to correct any mistakes in your information which we hold
- require the erasure of personal information concerning you in certain situations
- receive the personal information concerning you which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to a third party in certain situations
- object at any time to processing of personal information concerning you for direct marketing
- object to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you
- object in certain other situations to our continued processing of your personal information
- otherwise restrict our processing of your personal information in certain circumstances

For further information on each of those rights, including the circumstances in which they apply, see the *Guidance from the UK Information Commissioner's Office (ICO) on individual's rights under the General Data Protection Regulation*.

If you would like to exercise any of those rights, please email, call or write to us – please see 'How to contact us' below.

10. Keeping your personal information secure

10.1 Data security

We will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

- Maintaining data security means making sure that:

a. only people who are authorised to use the information can access it, all data is password protected;

b. information is accurate and suitable for the purpose for which it is processed; and

c. authorised persons can access information if they need it for authorised purposes.

- By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

- Personal information must not be transferred to any person to process (e.g. while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

- Security procedures include:

a. Any desk or cupboard containing confidential information must be kept locked.

b. Computers should be locked with a strong password that is changed regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.

c. Data stored on CDs or memory sticks must be password protected and locked away securely when they are not being used.

d. The Data Protection Officer must approve of any cloud used to store data.

e. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

f. All servers containing sensitive personal data must be approved and protected by security software.

g. Servers containing personal data must be kept in a secure location, away from general office space.

h. Data should be regularly backed up in line with the Employer's back-up procedure.

- Telephone Precautions. Particular care must be taken by staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

a. the identity of any telephone caller must be verified before any personal information is disclosed;

b. if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;

c. do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the Data Protection Officer.

- Methods of disposal. Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

10.2 Data breaches

If we discover that there has been a breach of Staff personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

We will record all data breaches regardless of their effect in accordance with our Breach Response Policy.

If the breach is likely to result in a high risk to your rights and freedoms, we will tell affected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures it has taken.

11. Training

We will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy will receive additional training to help them understand their duties and how to comply with them.

12. How to complain

We hope that we can resolve any query or concern you raise about our use of your information.

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is the Information Commissioner who may be contacted at https://ico.org.uk/concerns/ or telephone.

13. How to contact us

Please contact us if you have any questions about this data protection policy or the information we hold about you. If you wish to contact us, please send an email to datacontroller@scientificservices.org, write to Scientific Services Ltd, The Fuel Depot, Scorrier, Redruth, Cornwall, TR16 5UT or call 01209 311350.

14. Do you need extra help?

If you would like this notice in another format (for example: audio, large print, braille) please contact us (see 'How to contact us' above).

15. Changes to this policy

This customer data protection policy was published on the 21.06.2019.