Data Protection Policy

CONTROLLED COPY			
Issued By	**Role**	**Version No**	**Date**
Matthew Helks	Director	1	20/6/19

PCS Asbestos Consultants, 2 Moor Lane, Highburton. Huddersfield. HD8 0QS

E:info@pcs-asbestos.co.uk
W:www.pcs-asbestos.co.uk
T: 01484 604920
F: 01484 604210

Registered office:- 2 Moor Lane, Huddersfield. HD8 0QS. Registered in England: 69999763

DATA PROTECTION POLICY

PCS Asbestos Consultants Limited (**PCS Asbestos**), as Data Controller, is committed to ensuring its compliance with the requirements of the law governing the management and storage of Personal Data (as defined below), which is set out in the UK's Data Protection Act 2018 and the EU's General Data Protection Regulation 2016 (**GDPR**). We recognise the importance of Personal Data to our business and the importance of respecting the privacy rights of individuals. This Data Protection Policy (**the Policy**) sets out the principles which we will apply to our Processing (as defined below) of Personal Data so that we not only safeguard one of our most valuable assets, but also Process Personal Data in accordance with applicable laws.

Compliance with the GDPR is overseen by the UK data protection regulator which is the Information Commissioner's Office (**ICO**). PCS Asbestos is accountable to the ICO for its data protection compliance.

This policy aims to protect and promote the data protection rights of individuals and of the business, by informing everyone working for the business of their data protection obligations and of the business procedures that must be followed in order to ensure compliance with GDPR. Information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

This policy covers all Personal Data and special categories of Personal Data, however Processed (on computers or manually). In the event that any staff process Personal Data through working at home, for example, this Guidance (as defined below) and all it entails applies equally to such data.

This Policy and the Guidance (which is set out in the following pages) applies to all staff (including managers), consultants and any third party that this policy has been communicated to, as it is the responsibility of all to assist PCS Asbestos in complying with its obligations as Data Controller. All members of staff should familiarise themselves with both this Policy and the Guidance and apply their provisions in relation to any Processing of Personal Data. Failure to comply with the GDPR, the Policy and the Guidance could amount to misconduct, which is a disciplinary matter, and could ultimately lead to summary dismissal. Serious breaches could also result in personal criminal liability.

For these reasons, it is important that all employees familiarise themselves with this Policy and the Guidance and attend any training sessions in respect of the care and handling of Personal Data.

This Policy and the Guidance may be amended from time to time to reflect any changes in practice or legislation. Matthew Helks, who is the business's Privacy Manager, and Sally Rhodes who is the Deputy Privacy Manager, are responsible for monitoring the business's compliance with this policy and any queries as to data protection procedures or requirements should be directed to the Privacy Manager.

This Policy has been approved by the management. It will be reviewed annually or as and when a change in the data protection regime requires it to be updated.

INTRODUCTION

This Guidance Note (**Guidance**) forms part of the Data Protection Policy and provides supplementary information to enable staff to better understand and comply with the Data Protection Policy.

PCS Asbestos, as Data Controller, is required to comply with the GDPR in respect of its Processing of Personal Data (such as information about our clients, employees and suppliers). Compliance with data protection legislation is the responsibility of all members of the business who process personal information and it is therefore important for all staff to familiarise themselves with both the Data Protection Policy and this Guidance and act in accordance with their content.

Any day-to-day data protection issues or any questions about the Policy or the Guidance should be raised with the Privacy Manager.

The GDPR is intended to protect the rights and privacy of individuals and to ensure that data about them is not processed without their knowledge and, wherever possible, is processed with their consent. Whilst the GDPR covers Personal Data relating to individuals, you should bear in mind that if you handle personal details of, for example, officers of companies, this will still constitute Personal Data and therefore be subject to the GDPR's requirements.

It should be noted that the business is authorised to process data connected to staff administration, advertising and marketing, keeping accounts and records, provision of legal services and data gathered by the GPS tracking devices which are installed in all company vehicles. Anyone who is, or intends Processing data for purposes not included in the business's entitlements should seek advice from the Privacy Manager.

In this Guidance, the following definitions are used:

Consent is agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controllers means the natural or legal person, public authority, agency or other body who alone or jointly with others, determine the purposes for which, and the manner in which, any Personal Data is processed. They have a responsibility to establish practices and policies in line with the GDPR. PCS Asbestos is the Data Controller of all Personal Data used in our business.

Data Processors include any person who processes Personal Data on behalf of a Data Controller. Employees of Data Controllers are excluded from this definition but it could include suppliers which handle Personal Data on our behalf.

Data Subjects (for the purpose of this policy) include all living, identified or identifiable individuals about whom PCS Asbestos holds Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data. This will include, and is not limited to, staff, clients, suppliers and business contacts.

Personal Data means data (however held) relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal Data can be factual (such as a name, address, date of birth or telephone number) or it can be an opinion (such as a performance appraisal). It will include passport or driving licence details. It also includes information that identifies the physical, physiological, genetic, mental, economic, cultural or social identity of a person. For the business's purposes, our clients are Data Subjects (other individual third parties that we hold Personal Data about are also likely to be Data Subjects)

Processing (or Process) is any activity that involves use of the Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation on or regarding the data including organising, accessing, amending, merging, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or making available Personal Data to third parties.

Special Categories of Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special Categories of Personal Data can only be processed under strict conditions and will usually require the express consent of the person concerned.

A. <u>Overall Policy Statement and detailed Guidance</u>

- All Data Subjects have rights with regard to how their personal information is handled. During the course of our activities we will store and process personal information which includes information about our staff and our clients and suppliers. We recognise the requirement to treat this information correctly and in a lawful manner.
- Personal information, which may be held on paper or on a computer, is subject to certain legal safeguards specified in the GDPR and other regulations. The GDPR imposes restrictions on how we may use that information.
- PCS Asbestos has to adhere to the data Processing principles around which the GDPR is based. These principles deal with handling, Processing, transportation, destruction and storage of personal information. It is essential that all staff adhere to these principles in performing their day-to-day duties. The principles require the business to ensure that all Personal Data and Special Categories of Personal Data:

    1. **is processed fairly and lawfully and in a transparent manner in relation to the subject;**
    2. **shall be obtained for specified, explicit and legitimate purposes and not processed in a way that is incompatible with these purposes;**
    3. **shall be adequate, relevant and not excessive in relation to the purpose it is held;**
    4. **shall be accurate and kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay;**
    5. **shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which it is processed;**
    6. **shall be processed in accordance with the individuals' rights; and**
    7. **shall be processed in a manner that ensures appropriate technical and organisational measures shall be taken against unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.**

Additionally, Personal Data shall not be transferred to a country or territory outside the European Economic Area unless: (1) that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data; (2) appropriate, approved standard contractual clauses are in place; (3) the Data Subject has given explicit consent; or (4) the transfer is necessary for a reason set out in the GDPR. If this is envisaged, speak to the Privacy Manager for further guidance before transferring any data.

The business must be able to demonstrate its compliance with the above principles (‘accountability’).

In order to process all Personal Data in a manner that is compliant with GDPR, PCS Asbestos will:

- observe fully the conditions regarding the fair collection and use of Personal Data;
- meet its obligations to specify the purposes for which Personal Data is used;
- collect and process appropriate Personal Data only;
- ensure the quality of Personal Data used;
- apply strict checks to determine the length of time Personal Data is held;
- ensure that the rights of individuals about whom the Personal Data is held can be fully exercised under applicable laws;
- take the appropriate technical and organisational security measures to safeguard Personal Data; and
- ensure that Personal Data is not transferred abroad without suitable safeguards.

To expand on the practical aspects of the principles:

Fair and lawful Processing

The GDPR is intended not to prevent the Processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. Establishing an instruction is lawful Processing of Personal Data and continued instruction is deemed acceptance of data Processing for the purposes of progressing a matter.

For Personal Data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the Data Subject has Consented to the Processing, that it is in connection with us delivering our services for the Data Subject or that the Processing is necessary for our legitimate interests, provided that processing for our legitimate interests does not adversely affect the interests or rights of Data Subjects. When Special Categories of Personal Data is being Processed, more than one condition must be met. In most cases, the Data Subject's explicit consent to the Processing of such data will be required.

A Data Subject provides Consent to Processing of their Personal Data if they clearly indicate agreement to the Processing either by a statement or positive action. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Evidence of Consent and records of all Consents should be kept so that the business can demonstrate compliance with Consent requirements.

Specific Consent should be obtained to use Personal Data on the internet as such data could be accessed worldwide and the final data principle outlined above may be breached.

Processing for specific and limited purposes

Personal Data may only be processed for the specific purposes notified to the Data Subject when the data was first collected or for any other purposes specifically permitted by the GDPR. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose and Consent obtained before any Processing occurs.

Adequate, relevant and non-excessive Processing

Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject. Any data which is not necessary for that purpose should not be collected in the first place. If you are in possession of excessive data, it should be immediately deleted or destroyed.

We must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the business's data retention guidelines.

Accurate data

Personal Data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and therefore you should check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out of date data should be destroyed or updated as appropriate. You should notify the business's Office Manager with regard to any of your own Personal Data which needs updating and you should also ensure that if any client or third party provides updated personal information, the update is acted upon without delay.

Timely Processing

Personal Data should not be kept longer than is necessary for the purpose, meaning that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is to be kept before being destroyed, contact the Privacy Manager.

Processing in line with Data Subject's rights

Data must be processed in line with Data Subjects' rights. Data Subjects have a right to:

- ask what information PCS Asbestos holds about them and why;
- request access to any personal data held about them by us;
- prevent the Processing of their data for direct marketing purposes;
- ask to have inaccurate data amended;
- prevent Processing that is likely to cause damage or distress to themselves or anyone else;
- if we have any, be informed of the mechanics of any automated decision-making process that will significantly affect them;
- not have significant decisions that will affect them taken solely on an automated process;
- sue for compensation if they suffer damage as a consequence of a contravention of data protection laws; and
- request the Information Commissioner (the regulatory authority on this subject) to assess whether any provision of applicable laws has been contravened.

Data Security

- To guard against the risk of unlawful or unauthorised Processing of Personal Data, or against the accidental loss of, or damage to, Personal Data, we will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own and identified risks. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.
- The GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data may only be transferred to a third party Data Processor if that third party agrees to comply with those procedures and policies, or if he puts in place adequate measures himself. As an example, you may wish to consider password protecting emails or documents being transmitted to third party recipients or if the email or document contains particularly delicate or Special Categories of Personal Data, confirming by telephone (i.e. separately) to the intended recipient what the password is. Ask IT for training if required.
- Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data. These are defined as follows:
  - **Confidentiality** means that only people who are authorised to use the data can access it. All staff are responsible for ensuring that any Personal Data which they hold is kept securely and that it is not disclosed to an unauthorised third party;
  - **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed;
  - **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on our central computer system instead of on individual PCs.
- Security procedures include:
  - **Passwords**. Computer and mobile phone passwords must be kept confidential.
  - **Entry controls**. Any unannounced stranger seen in entry-controlled areas or beyond “normal” visitor access areas should be politely challenged as to their purpose and their presence should be queried with the Operations Manager Steve Hoare.

- **Secure lockable desks and cupboards**. Such should be kept locked if they hold confidential information of any kind. Note that Personal Data is always considered confidential.
- **Methods of disposal**. Paper documents containing Personal Data, once no longer needed, should be placed in the shredding bins. Hard drives or any permitted memory sticks should be specifically erased before disposal and CD-ROMs should be physically destroyed when no longer required.
- **Equipment**. Staff should ensure that individual monitors do not show confidential information to passers-by or to any person to whom this policy does not apply and that they lock or log off from their PC when it is left unattended. Any portable devices should be encrypted when not in use and never left unattended.

The GDPR requires us to keep full and accurate records of all our data Processing activities. We must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents. These records should include clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

If you have any concerns about Processing Personal Data, please contact the Privacy Manager who will be happy to discuss matters with you.

B. Dealing with subject access requests and other disclosures

The GDPR gives rights to individuals in respect of the Personal Data organisations hold about them. Everyone must be familiar with these rights and adhere to the business's procedures to uphold these rights.

These rights include:

- Right of information and access to confirm details about Personal Data that is being processed about them and to obtain a copy;
- Right to rectification of any inaccurate Personal Data;
- Right to erasure of Personal Data held about them (in certain circumstances);
- Right to restriction on the use of Personal Data held about them (in certain circumstances);
- Right to portability – right to receive data processed by automated means and have it transferred to another data controller;
- Right to object to the Processing of Personal Data; and
- Make a complaint to the regulatory authority, the Information Commissioner's Office.

A formal request from a Data Subject for information that we hold about them need not be in any particular format (and it could be verbal) but it should specify the information that the Data Subject requires. If you receive a request for Personal Data and require guidance as to whether it is a "subject access request", speak to the Privacy Manager. PCS Asbestos will require the Data Subject to provide evidence of their identity (so we are not disclosing to a third party). Any member of staff who receives a request should inform the Privacy Manager immediately who will assist. A request sent by email or fax is as valid as one sent in hard copy. Requests may also be validly made by means of social media. Note that information requested under a subject access request may not be fully disclosable as particular exemptions from disclosure may apply. Indeed, it may be that none of the information is disclosable. The Privacy Manager will advise as to what can be disclosed.

PCS Asbestos aims to comply with requests for access to personal information as quickly as possible, and, if we hold such information, will ensure that it is provided within **one month** of the request unless there is a proper reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

We must ensure that Personal Data is not disclosed to unauthorised third parties which includes family members, friends, government bodies and, in certain circumstances, the Police. All staff should exercise caution when asked to disclose Personal Data on an individual to a third party. Speak to the Privacy Manager if in doubt.

Personal Data may be legitimately disclosed where one of the following conditions applies:

- The individual has given their consent (e.g. consenting to us speaking to their adviser or other named third party);
- Where disclosure is in the legitimate interests of the business (e.g. disclosure to other staff members);
- Where the business is legally required to disclose the data.

The GDPR does not create a barrier to sharing information when it is necessary to protect the public as in such situation disclosing information would be permitted if it can be justified and is proportionate.

The GDPR contains some exemptions in respect of disclosures. If you are contacted by, for example:

- the Police; or
- any government department asking for information about clients,

you must not confirm or deny whether or not we hold information about a Data Subject straight away. You first of all need to consider the relevant facts and circumstances whether the request for disclosing such information is proportionate and justifies the granting of access to the relevant information.

The rights of individuals over their data can be restricted in certain circumstances and it may be that a specific exemption in the GDPR and the Data Protection Act 2018 might permit such disclosure. You should not disclose any information without speaking to the Privacy Manager first. The Privacy Manager will have to consider the availability of any exemptions on a case by case basis and consider if a failure to disclose the information would prejudice and compromise the alleged investigations before deciding whether or not to disclose.

Do not be afraid to ask for further information relating to the reasons for the requests as it is for the person making the request to satisfy you that disclosing the requested information is lawful.

If you receive a Production Order from the Police or an Order from a government department requiring information to be disclosed, contact the Privacy Manager.

C. <u>Providing information over the telephone</u>

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal or confidential information held by us. In particular they should:

- check the caller's identity to make sure that information is only given to a person who is entitled to it;
- suggest that the caller put their request in writing if they are not sure about the caller's identity or the purpose of the enquiry and where their identity cannot be checked;
- refer to the Privacy Manager for assistance in difficult situations. No-one should be pressured into disclosing personal information.

Every member of staff that holds information about identifiable living individuals has to comply with the GDPR in managing that information.

D. Retention and Disposal of Data

The business will not retain Personal Data for longer than necessary.

- **Clients**: Data for clients is retained indefinitely in order to comply with legal and regulatory requirements as we are dealing with hazardous waste which our records for our clients' properties may be relied upon indefinitely.
- **Enquiries**: Data relating to client enquiries is retained for 3 years in order to offer a high level of client service.
- **Staff**: PCS Asbestos will create a personnel file for each member of staff and will keep this for the duration of employment and for a minimum of 1 year after a staff member leaves employment. After 1 year, we will review the personnel file and delete any personal data that we do not need. We will retain the following personal data for the following periods of time:

Data	Period of Retention
Data confirming payments due to you. For example, your contract of employment and any information about salary or benefits.	6 years after you leave your employment
Data relating to taxes, National Insurance contributions and other charges paid in relation to you.	7 years after you leave your employment
Data relating to any accidents or injuries at work or injuries or illnesses which such symptoms may occur later on in life.	100 years after you leave your employment in order to assist us in reviewing and potentially defending any claims as a result of symptoms of injuries or illness arising later in life.
Data relating to any references given in relation to you.	1 year after the date of the reference

- **Recruitment Records**: Information relating to unsuccessful applicants will be kept for up to 2 years from receipt of their application to aid in the recruitment process.
- **Disposal of Records**: all Personal Data must be disposed of in a way that protects the rights and privacy of Data Subjects (e.g. shredding).

E. Publication of Information

The business publishes a number of items that includes Personal Data and will continue to do so. These include:

- Internal telephone directory
- Staff information/photographs on the firm's website
- Information including photographs in newsletters, tender applications and so on.

F. Direct Marketing

Before any electronic direct marketing is undertaken, it must be clear that the people to be contacted have Consented to receive such marketing and that a valid, up to date, consent notice is held on file. There is a limited exception for existing clients known as "soft opt in" – this allows us to send marketing texts or emails if we have obtained contact details in the course of providing

services to that person, the messages are marketing similar services, and we gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

For marketing by post, we are able to send postal marketing to our clients regarding new products or services, in reliance on our “legitimate interests” – we generally do not need consent to this type of mailing but we will always need to offer clients an opt-out.

The right to object to direct marketing must be explicitly offered to the Data Subject. A Data Subject’s objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

G. Tracking Devices

To assist with the location and security of company property, we have installed GPS tracking devices, via Crystal Ball Vehicle Tracking Systems, into all company vehicles. Any personal data collected via our vehicle tracking devices will only be stored for a period of up to 12 weeks as Crystal Ball Vehicle Tracking Systems then archive the data for 7 years which we can then access if considered necessary.

Privacy By Design and Data Protection Impact Assessments (DPIAs)

Privacy by Design involves using appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles. Privacy by Design is an ongoing measure.

Data Privacy Impact Assessments (DPIA) involve using tools and assessments to identify and reduce risks of a data Processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

DPIAs will be carried out when introducing, or making significant changes to, systems or projects involving the Processing of Personal Data. DPIAs are required to identify data protection risks and to assess the impact of these risks, as well as to determine appropriate action to prevent or mitigate the impact of these risks.

This means thinking about whether we are likely to breach the GDPR and what the consequences might be, if we use Personal Data in a particular way. It is also about deciding whether there is anything that we can do to stop or minimise the chances of potential problems identified, from happening.

DPIAs will be undertaken by the Privacy Manager and Management.

Breaches

A data protection breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Everybody working for PCS Asbestos has a duty to report any actual or suspected data protection breach without delay to the Privacy Manager or, in their absence, their line manager.

Breaches will be reported to the ICO by the Privacy Manager without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, unless, we are able to demonstrate that the Personal Data breach is unlikely to result in a risk to the rights and freedom of Data Subjects. Where there is a high risk to the rights and freedoms of individuals, we must also notify the affected individuals.

The Privacy Manager will maintain a central register of the details of any data protection breaches.

Complaints

Complaints relating to breaches of the GDPR and/or complaints that an individual's Personal Data is not being processed in line with the data protection principles should be referred to the Privacy Manager without delay.

Penalties

It is important that everyone understands the implications for the business if we fail to meet our data protection obligations. Failure to comply could result in:

- Criminal and civil action
- Personal accountability and liability
- Suspension/withdrawal of the right to process Personal Data by the ICO which would impact on our ability to do business
- Loss of confidence in the integrity of our systems and procedures
- Irreparable damage to our reputation

Breaches can have serious consequences. PCS Asbestos could be fined up to 20,000,000 Euros, or up to 4% of annual turnover of the preceding financial year, whichever is the higher and depending on the breach.

This Guidance has been approved by Management. It will be reviewed annually or as and when a change in the data protection regime requires it to be updated.

This Policy was reviewed by Privacy Manager and introduced on **[**DATE**]**.