PDSI Group Data Protection policy

Policy prepared by:	Brad Bamfield
Version	1.0
Approved by board	30th May 2018
Policy became operational on	30th May 2018
Next review date	1st August 2018

Introduction

This policy is adopted by PDSI Ltd and all its subsidiaries including Initiate Consultants Ltd, Profile Construction Consultants Ltd, Queensborough Project management Ltd, JS Projects Ltd and Complete Construction Management Ltd, collectively referred to in this Policy as "The PDSI Group" and it must always be applied by our, employees, sub-consultants and suppliers.

The PDSI Group needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the PDSI Group's data protection standards — and to comply with the law.

It is the responsibility of every member of staff to tell their line manager of any actual or potential issues that may affect the implementation of this policy. If no action is taken, then they must escalate the issue to the Chief Executive Officer.

Failure to act on information that could affect this Policy may be considered a disciplinary offence.

Why this policy exists

This data protection policy ensures the PDSI Group:

- Complies with data protection law and follows best practice
- Protects the rights of staff, customers and partners
- Is open about how we store and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations — including the PDSI Group — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, Risks and Responsibilities Policy scope

This policy applies to:

- The parent company PDSI Ltd
- All subsidiaries of PDSI Ltd
- All staff and volunteers of any PDSI Group company
- All contractors, suppliers and other people working on behalf of any company within the PDSI Group
- It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:
- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other information relating to individuals

Data protection risks

This policy helps to protect the PDSI Group from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with in the PDSI Group has appropriate responsibility for ensuring data is collected, stored and handled appropriately.

Each person and team that handles personal information and data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that the PDSI Group meets its legal obligations.
- The Chief Executive, Terry Chapman, is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, annually.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data the PDSI Group holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The PDSI Group Subsidiary Directors are responsible for:
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - The Administration Director, Brad Bamfield, is responsible for:
    - Ensuring all systems, services and equipment used for storing data meets acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    - Ensuring and approving any data protection statements attached to communications such as emails and letters and tenders comply with the policy and the law.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff guidelines

The only people able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

The PDSI Group will provide GDPR and Cyber Security requires all staff to complete GDPR and Cyber Security training to help them understand their responsibilities when handling data. This training will be repeated annually to ensure all staff are kept up to date.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Protection

Protecting data is of paramount importance to The PDSI Group and their Clients and is formed of several components.

- Corporate
- Personal
- Hardware and software
- Human

Corporate

The PDSI Group is committed to keeping is business at the point of "best practice" with regard to security of data.

The PDSI Group has achieved Cyber Essentials certification,

Certificate number 9951510267859178

more details of the scheme here
https://www.cyberessentials.ncsc.gov.uk/

The PDSI Group will review all aspects of Cyber Security annually and which includes a systems vulnerability test as part of Cyber Essentials annual re-assessment.

Personal

All employees, sub-consultants and suppliers have responsibility to ensure the equipment they use is compliant with eth PDSI Group requirements. They must inform

their line manager as soon as they become aware of a non-conformity and ensure it is remedied.

Use of equipment such as laptops and smart phones when not ion a PDSI Group office must comply with this Policy and public internet access points, such as coffee shops, must never be used without access through our VPN (virtual private network).

Hardware and Software

The PDSI Group is committed to ensuring best practise with regard to the hardware we install and the software suppliers we use.

Our hardware is reviewed annually as part of our Cyber Essentials re-assement.

Our software is only sourced from reputable suppliers who have comparable Data Security policies.

Cloud storage and back up protocols are GDPR compliant.

Human

The most important link in the security chain is the individual who must apply the processes with knowledge and understanding.

The PDSI Group will provide annual training for all employees to ensure skills are up to date.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- The PDSI Group operates a clear desk policy where all documents, papers, files or other media must be securely locked away at the end of each working day.
- When not required, the paper or files should be kept in a locked drawer or filing cabinet. Filing trays must be emptied at the end of every working day.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- All shredded paper waste must be securely disposed through a specialised and approved service and not mixed with general rubbish.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.

- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to the PDSI Group unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT Support team can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires The PDSI Group_to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- The PDSI Group will make it easy for data subjects to update the information we hold about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

- It is the Directors of each subsidiary responsibility to ensure marketing databases are checked against industry suppression files every six months.

Breach of Security

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the PDIS Group will promptly assess the risk to people's rights and freedoms and report the breach to the Information Commissioner's Office, ICO, (more information on the ICO website).

Subject access requests

All individuals who are the subject of personal data held by The PDSI Group are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at datarequest@pdsiconsult.com. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10.00 per subject access request and we reserve the right to increase the charge for repeat or frivolous requests. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, The PDSI Group will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

The PDSI Group aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. Which is publicly available on our web sites and for employees through our SharePoint intranet.

Signed by

Terry Chapman

PDSI Group CEO