Data Protection Policy, Guidelines & Procedures

Developed by:
Trevor Partridge MBCI, NEBOSH
(Director – 2 b continued Ltd.)

1) Context & Overview

Policy prepared by: **Trevor Partridge, Director 2 b continued Ltd., Risk Management Consultant**
Approved by: **Steve Place, Director, Gidden Place**
Approved on: **23.07.18**
Next review date: **01.07.19**

a) Introduction

At **Gidden Place**, dealing with information about people properly is vital. We need to gather and use certain information about individuals throughout our day to day operations, therefore, together, we must use Data, in accordance with individual's rights and our legal obligations.

This Policy:

- Explains why the above is of importance
- Applies to the main office of Gidden Place
- Applies to everyone across the company, including, employees, customers, contractors and other individuals we have a relationship with
- Describes how the Data is collected, handled and stored, to meet the Regulations and to comply with the law
- Follows good practice
- Protects the rights of employees, customers, contractors and other individuals we have a relationship with
- Endeavours to protect **Gidden Place** from the risk of a Data breach including:
    - Breaches of confidentiality
    - Failing to offer choice
    - Reputational damage.

It applies to all Data held by the company, relating to individuals, including:

- Names of individuals
- Postal addresses
- E-mail addresses
- Telephone numbers
- Plus, any other information relating to such individuals.

b) General Data Protection Regulations (GDPR)

Data protection laws are enforced in the UK by the Information Commissioners Office (ICO), who can investigate complaints, audit our use of Data, and take action against us for breaches of these laws. This can include fines, preventing us from using personal Data, which could prevent us from carrying on with our business. In addition, Directors may be subject to criminal prosecution. The impacts on our business therefore can be significant and must not be underestimated.

The Regulations are underpinned by general principles. Primarily they are that Data must:

- Be processed fairly and lawfully
- Be obtained only for specific lawful purpose
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Be protected in appropriate ways
- Not be transferred outside of the European Economic Area (EAA).

2) Roles & Responsibilities

Everyone who works for or with **Gidden Place** has responsibilities for ensuring Data is collected, stored and handled appropriately, and that everything they do is aligned to this Policy.

This Policy must be read, understood and signed by all employees.

Gidden Place have a legal responsibility as employers to ensure that employees are adequately trained in understanding the importance of complying with this Policy, as well as other related information on Data Protection.

The Directors are ultimately responsible for ensuring that **Gidden Place** meets its legal obligations.

Line Managers are responsible for ensuring all Data is retained, for as long as deemed appropriate and accurate

The Operations Director has been given ownership and responsibility to ensure compliance with the Regulations, including:

- Keeping Directors updated about compliance
- Reviewing procedures and Policy
- Arranging any training and awareness
- Handling questions or dealing with requests
- Ensuring all IT systems, including security software, firewalls and scans, used for Data storage, meets acceptable security standards, signed by **Premier Choice Internet**, to this end.
- Evaluating third party providers, including contractors, clients and IT service providers meet their legal obligations in Data Protection.

Employees are responsible for ensuring their own personal records are up to date, correct, consistent and relevant.

3) Employees Guidelines

a) General Guidelines

General guidelines and principles, for all employees to follow, are set out below. These principles form the basis for the training and awareness materials provided. For more details, a section has been added to the main index of the Employees Handbook.

1) The only people able to access data, covered by this Policy, should be those who need it for their work

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

3) **Gidden Place** will provide training and awareness materials to all employees to help them understand their responsibilities when handling Data. It is the responsibility of all employees to ensure they are fully aware of their responsibilities in respect of Data Protection

4) Employees should keep all Data secure, by taking sensible precautions, follow guidelines provided, and treat Data with respect

5) Strong passwords must be used, not shared and changed regularly

6) Personal Data must not be disclosed to unauthorised people, either within the company or externally

7) Data, for example employee details, the clarity database, e-mails, etc. should be regularly reviewed, mapped and updated. If no longer required, it should be deleted and disposed of. More details on Data storage locations, access rights and mapping can be found in a separate document.

8) Employees should request help from their line manager or the Operations Director, if they are unsure about any aspect of Data protection

9) When working with personal Data, it is the responsibility of all employees to ensure the screens of their PC's are always locked when left unattended

10) Data should never be transferred outside of the European Economic Area

11) Employees should be careful and mindful when clicking on an unsafe attachment or link.

b) Data Storage

These guidelines describe how and where Data should be safely stored. Questions about storing Data safely can be directed to the **Operations Director** and the appointed specialist 3rd parties including **Premier Choice Internet** and **2 b continued Ltd**.

1) When Data is stored, either on paper, electronically, or on removable media (CD, memory stick etc.) it should be kept in a secure place, where unauthorised people cannot see it or gain access to it, or may cause accidental deletion or may cause malicious hacking

2) When not required, any paper files should be kept in a locked drawer, filing cabinet, or safe. All keys for filing cabinets should be locked in the safe

3) Employees should make sure paper and printouts are not left where unauthorised people could see them, and desks should be cleared from all Data every night before finishing

4) Data printouts should be shredded daily and disposed of securely on a regular basis

5) Data should be stored on designated drives and servers, uploaded to an approved cloud computing service and/or backed up regularly and should never be saved directly to laptops or other mobile devices

6) Servers should be sited in a secure, locked location, and protected by approved and appropriate levels of security software including a firewall.

c) Data Accuracy

The Regulations requires **Gidden Place** to take reasonable steps to ensure Data is kept up to date and accurate.
It is the responsibility of all employees who work with Data to take such reasonable steps.

1) Data will be held in as few places as necessary

2) **Gidden Place** will make it easy for Data on employees to update their information, inform employees as to how the business holds their information and what the Data is used for

3) Data should be updated as inaccuracies are discovered

d) Employees access requests

Gidden Place aims to ensure all employees are aware their Data is being processed. To this end the company has a Privacy Notice, setting out how Data related to employees is used by the company, a version of which can be found on the website and included in the Employees Handbook.

All employees who are the subject of personal Data held by **Gidden Place** are entitled to:

1) Ask what information the company holds about them and why

2) Ask how to gain access to their Data

3) Be informed as to how to keep it up to date

4) Be informed as to how the company is meeting its Data protection obligations

4) Data Breaches

Data breaches arise in many ways, often by human error, and include for example:

- A lost laptop, smart device or paper file
- Loss of customers details
- Through giving personal details face to face, by telephone or e-mail to the wrong person
- Clicking an unsafe attachment or link, triggering a cyber-attack

If employees suspect there has been a Data Breach, this must be reported immediately, with full details, to the **Operations Director** who will inform the **Directors**.

In certain circumstances, the Regulations requires the company to disclose such Data Breaches.

Should this case arise, the company will call the Information Commissioners Office helpline on 0303 123 1113, who will record the breach and give advice as to what to do next.

Information required when contacting the helpline is as follows:

- What has happened;
- When and how the Data breach was found
- The people that have been or may be affected by the breach
- What the company is doing as a result of the breach
- Who should be contacted if more information is required and who else has been informed.

Any questions about this Policy, Guidelines and Procedures should be referred to the **Operations Director** and the appointed specialist 3rd parties including **Premier Choice Internet** and **2 b continued Ltd**.