DATA PROTECTION (GDPR) POLICY

Introduction

WPG needs to gather, store and use information on people to be able to carry out it's business functions. These can include employees, clients and suppliers and other people WPG has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored in order to meet WPG Data Protection Policy and comply with data protection legislation including GDPR General Data Protection Regulation (EU) 2016/679.

Purpose and scope of Policy

This Data Protection Policy ensures WPG:

- Complies with data protection law and follows good practice
- Protects the privacy rights of employees, clients and suppliers
- Is open about how it stores and processes individual's data
- Identifies roles and responsibilities
- Protects itself from the risks of a data breach

This Policy applies to all permanent and temporary employees of the Company (including any of its intermediaries, subsidiaries or associated companies). It also applies to any individual or corporate entity associated with the Company or who performs functions in relation to, or for and on behalf of, the Company, including, but not limited to, directors, agency workers, casual workers, contractors, consultants, seconded staff, agents, suppliers and sponsors ("associated persons"). All employees and associated persons are expected to adhere to the principles set out in this Policy.

Legal obligations

The UK legislation on which this Policy is based is the UK Data Protection Act 1998, GDPR General Data Protection Regulation (EU) 2016/679 and associated UK legislation to enact GDPR General Data Protection Regulation (EU) 2016/679.

At the time of writing this policy the GDPR General Data Protection Regulation was not fully enacted. This policy will be updated if changes are required when this bill becomes enshrined in law.

Data Protection Principles

The data protection legislation is underpinned by eight important principles. These principles 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 longer than necessary
6. Be processed in accordance with the rights of the 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.

Policy Scope

This policy applies to

- All WPG employees
- All contractors, suppliers and other people working on behalf of WPG

It applies to all data that the company holds relating to identifiable individuals. This can include

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- All personal details held in employee HR records
- All personal data contained within business documents
- Personal data provided to WPG by clients and suppliers

Data Protection Risks

This policy helps to protect WPG from data security risks including:

- Breaches of confidentiality
  For example data being given out inappropriately
- Reputational Damage
  Due to data breach

Roles and Responsibilities

Everyone who works for or with WPG has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure 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 WPG meets it's legal obligations

- Data Protection officer, due to its size and nature of it's business WPG does not have a dedicated DPO, this role will be fulfilled by the Managing Director. The Data Protection Officer is responsible for:

- Keeping the board updated about data protection risks and issues
- Reviewing all data protection procedures and related policies
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from employees and anyone else covered by this policy
- Dealing with requests from individuals to see the data WPG holds about them (also called Subject Access Requests)
- Checking and approving any contracts or agreements with third parties that may handle WPG data

- The IT Manager is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
  - Performing regular checks and scans to ensure security hardware and software is functioning properly
  - Evaluating and third-party services the company is considering using to store or process data

- The Marketing Manager is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters
  - Working with other employees to ensure marketing initiatives abide by data protection principles
  - Addressing and data protection queries from journalists or media outlets

General Employee Guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Data must not be shared informally. When access to personal data is required employees must request it from the appropriate manager
- Employees must keep all personal data secure, by taking sensible precautions such as
  - Use strong passwords
  - Do not share passwords
  - Do not disclose personal data to unauthorized people either within WPG or externally
  - Review and update personal data regularly. Securely delete and dispose of personal data that is no longer required
  - Employees are to request assistance from their line manager or the data protection officer if they are unsure of how data protection applies to any data they are responsible for.

Data Storage

Questions about storing data securely should be directed to the IT manager or the data protection officer.

- Data stored on paper must be kept in a secure location such as a locked drawer or cupboard where unauthorized people cannot see it.
- Employees must ensure printouts of personal data are not left on unattended printers
- Data printouts must be shredded and securely disposed of when no longer required

Electronic data must be protected from unauthorized 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 this should be kept locked securely when it is not in use
- Data should only be stored on designated drives and servers and should only be uploaded to an approved secure cloud service
- Data should be backed up regularly. These backups should be tested regularly and securely stored off site
- All servers and computers containing data should be protected by approved security software including a firewall

Data Use

WPG needs to use personal data to be able to conduct its business, this data must be protected as follows when it is in use

- Personal data should never be transferred outside of the EEA
- Personal data should not be shared informally
- Personal data must never be saved to employees personal devices
- Sending personal data via email should be kept to a minimum and only WPG email systems should be used
- When working with personal data especially sensitive personal data, employees should ensure their screens are locked when left unattended

Purposes for which Personal Data may be held

Personal data relating to employees may be collected primarily for the purposes of

- recruitment, promotion, training, redeployment and/or career development;
- administration and payment of wages;
- calculation and administration of benefits including pensions;
- disciplinary or performance management purposes;
- performance review;

- recording of communication with employees and their representatives;
- compliance with legislation;
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and
- staffing levels and career planning.

The Company considers that the following personal data falls within the categories set out above:

- personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ***gender, sexual orientation, disability***, ethnic origin and nationality will also be deemed as relevant;
- references and CVs;
- emergency contact details;
- notes on discussions between management and the employee;
- appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment;
- training records;
- salary, benefits and bank/building society details; and
- absence and sickness information.

Employees or potential employees will be advised by the Company of the personal data which has been obtained or retained, its source, and the purposes for which the personal data may be used or to whom it will be disclosed.

The Company will review the nature of the information being collected and held on an annual basis to ensure there is a sound business reason for requiring the information to be retained.

Personal Data held for Equal Opportunities Monitoring Purposes

Where personal data obtained about candidates for the purposes of Equal Opportunities monitoring must be kept secure and only used for such purposes. If this data is published it must be anonymised.

Data Accuracy

WPG must 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 ensure data is updated accurately.
WPG will provide a process whereby employees can keep their personal data updated
The marketing manager is responsible for ensuring marketing lists are kept up to date and if necessary to check them against industry suppression files.

Subject Access Requests

All individuals who WPG hold data on them are entitled to:

- Ask what information the company holds on them and why

- Ask to see a copy of that data
- Be informed as to how they keep that data updated
- Be informed how WPG is meeting its data protection obligations

Individuals may contact WPG requesting a copy of this information, this is referred to as a Subject Access Request or SAR. WPG will process SARs in line with the UK Information Commissioners Office (ICO) SAR guidelines.

Disclosing Data for other Reasons

In some circumstances the legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. In those circumstances WPG will disclose the requested data. All requests and disclosures must go through WPG data protection officer who will ensure the request is legitimate. When necessary the DPO may seek advice from the board and legal advisers.