Privacy notice

Data protection company policy - GDPR

Introduction

Joyner PA Ltd and Joyner PA (Cymru) Ltd also known as the Joyner Group (the "Company") needs to gather and use certain information about individuals. This can include clients, suppliers, business contacts, employees, contractors and other people the organisation has a relationship with or may need to contact.

We are committed to maintaining the privacy of every individual we hold data on. We will never share individual data with a third party or external agencies without express permission from the individual in question.

Although we do not collect any personal data through our website we do analyse traffic, using Google Analytics as our third-party provider, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website.

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

The Company and its directors will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of The General Data Protection Regulations (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016, the two-year transition period and the application date of 25 May 2018 of the Data Protection Act 1998.

Why this policy exists

To ensure the Company:

- Complies with data protection law and follows good practice
- Protects the rights of staff, clients and partners
- Is open about how it stores and processes individual's data

- Protects itself from the risks of a data breach

Data protection law

The act describes how organisations, including the Company, 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:

- Be processed fairly and lawfully
- Be obtained for specific and lawful purposes
- Be adequate, relevant, not excessive
- Be accurate and, where necessary up to date
- Not be kept for longer than necessary
- Be processed in accordance with the rights of data subjects
- Appropriate measures must be taken against unauthorised and unlawful processing of data or accidental loss – be protected in appropriate ways
- Not be transferred to a country outside the EEA unless that country has adequate protection for the rights of data subjects

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of the Company
- All staff and volunteers of the Company
- All contractors, suppliers and other people working on behalf of the Company

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. This can include:

- Names of individuals
- Postal address
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals, such as sensitive personal data, meaning personal data consisting of information as to:

  - The racial or ethnic origin of the data subject
  - Their political opinions
  - Their religious beliefs or other beliefs of a similar nature
  - Whether they are a member of a trade union
  - Their physical or mental health or condition
  - Their sexual life
  - The commission or alleged commission by them of any offence
  - Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

Data protection risks

This policy helps to protect the Company 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, the Company has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal 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 Company meets its legal obligations
- The Company is not required to appoint a data protection officer (DPO) under the regulations, however, the directors shall undertake that the same duties and responsibilities apply, in so far as the board of directors deem appropriate, had we been required to appoint a DPO

- The **managing director, or other director nominated by him,** is responsible for:

  - Keeping the board updated about data protection responsibilities, risks and issues
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule
  - Arranging data protection training and advice for people covered by this policy, in so far as is deemed necessary
  - Handling data protection questions from staff and anyone else covered by this policy
  - Dealing with requests from individuals to see the data the Company 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 **Company office manager** (and any outsourced **IT services company** where appointed) 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 any third-party services the Company is considering using to store or process data. For instance, cloud computing services

- The **Company directors** are responsible for:

  - Approving any data protection statements attached to communications such as emails and letters
  - Addressing any data protection queries from journalists or media outlets, like magazines and newspapers
  - Where necessary, working with other staff to ensure any 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 manager
- The **Company will provide training** to all employees, in so far as is deemed appropriate by the directors, to help them understand their responsibilities when handling data

- 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 manager or a Company director if they are unsure about any aspect of data protection

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the office manager or a Company director.

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:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**
- 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

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 service**
- 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 good 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 Company 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**
- Personal data should **never be transferred outside 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 Company to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort the Company should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept 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 clients' details when they call
- The Company will make it **easy for data subjects to update the information** the Company holds about them
- Data should be **updated as inaccuracies are discovered.** For instance, if a Client can no longer be reached on their stored telephone number, it should be removed from the database

Subject access requests

All individuals who are the subject of personal data held by the Company 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 a director of the Company who will aim to provide the relevant data within 14days. Such requests should be headed 'subject access request'. In some circumstances it may not be possible to release the information about the subject to them e.g. if it contains personal data about another person.

The director 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 Company will disclose the requested data. However, the director will ensure the request is legitimate, seeking assistance from the board and from the Company's legal advisors where necessary.

Providing information

The Company 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

Policy approved by:

Title: Managing director **Date:** 1st November 2023