Data Protection Policy

Policy became operational on: 1st April 2018

Next Review Date: 31st March 2019

Introduction

Peter Gill's Rock Schools C.I.C. gathers and uses certain information about individuals.

Individuals include our members, employees, family members, suppliers, volunteers and people **Peter Gill's Rock Schools C.I.C.** has a relationship with or may need to contact. This Policy describes how personal data is collected, handled and stored to comply with the external data protection regulations.

This Data Protection Policy ensures **Peter Gill's Rock Schools C.I.C.**

• Complies with data protection law • Protects the rights of all members of **Peter Gill's Rock Schools C.I.C.** • Is open about how data is stored and processed • Protects itself from the risks of a data breach.

Data Protection Laws EU Global Data Protection Regulation (GDPR)

The GDPR is Europe's new framework for data protection laws and it replaces the previous 1995 Data Protection Directive, which current UK law is based upon. The legislation is designed to "harmonise" data privacy laws across Europe as well as give greater protection and rights to individuals. It's provisions in the UK is covered by a new Data Protection Bill.

The scope of the GDPR covers personal and sensitive personal data:

Personal Data Any information that can be used to directly or indirectly identify a person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Sensitive Personal Data Encompasses genetic data, information about religious and political views, sexual orientation for example.

Highlights

- Individuals have easier access to the data companies hold about them
- Fines regime in place for breaches
- Clear responsibility for organisations to obtain the consent of individuals they collect information about.
- Requirement to document why information is being collect and processed, descriptions of information held, how long it is kept for and descriptions of technical security measures that are in place.

Policy Scope This policy applies to:

- **Peter Gill's Rock Schools C.I.C.**
- All employees and volunteers of **Peter Gill's Rock Schools C.I.C.**

Data Protection Risks

This policy helps to protect **Peter Gill's Rock Schools C.I.C.** from data security risks, including:

- Breach 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 gain access to sensitive data.

Responsibilities

Everyone who works for or with **Peter Gill's Rock Schools C.I.C.** has responsibility for ensuring data is collected, stored and handled appropriately within the remit of their role. Everyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The company director Peter Gill is ultimately responsible for ensuring that legal obligations are met

General 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 is required to confidential information, individuals can request this by contacting the company director.

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

- Setting strong passwords to access the information.
- 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
- Be wary of emails that may not be genuine
- Only forward emails to family members /third parties if explicit consent has been given

- Don’t disclose information over the phone without verifying who you are talking to

- Never save files directly to personal laptops or other mobile devices like tablets or smartphones without password protected and consent given.

Data Storage

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 desk / 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 memory sticks, these should be kept locked away securely.

Data Use

- 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.

- Members information that is required by an employee, to be able to carry out their tasks should only be sent to a secure email address and password protected.

- Employees should not save copies of personal data to their own computers or company laptop hard drives without consent or password protection.

Data Accuracy

- The law requires **Peter Gill's Rock Schools C.I.C.** 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. Employees should not create any unnecessary additional data files.

- Employees should take every opportunity to ensure data is updated.

- **Peter Gill's Rock Schools C.I.C.** will have a clear and easy process for individuals to update the information held relating to them.

- Data should be updated as inaccuracies are discovered

Subject Access Requests (SAR)

All individuals who are the subject of personal data held by **Peter Gill's Rock Schools C.I.C.** 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 **Peter Gill's Rock Schools C.I.C.** requesting information specific to them, this is called a Subject Access Request (SAR). These must be responded to within one month of receipt and are free of charge. The company director must always verify the identity of anyone making a SAR before handing over any information.

Right to Erasure

The right to erasure states that in certain circumstances, an individual can submit a request to have personal information erased to prevent further processing of that data. The right to erasure applies when:

- The personal data is no longer necessary or relevant in relation to the purpose for which it was original collected.
- The individual specifically withdraws consent to processing (and if there is no other justification or legitimate interest for continued processing).
- Personal data has been unlawfully processed, in breach of the GDPR.
- The data must be erased in order to comply with legal obligations (for example, the deletion of certain data after a set period of time).

If one of the above conditions applies under this right to erasure, **Peter Gill's Rock Schools C.I.C.** has an obligation to delete and remove the data 'without undue delay' and specifically within a month unless specific circumstances apply. In instances where personal data has been shared with other third parties or made available in the public domain, the GDPR states that 'all reasonable steps' must be taken to inform other outlets of the request for erasure and require them to comply with deletion or removal.

The exceptions to the right to erasure and reasons to refuse to comply include:

- The right of freedom of expression and information

- Compliance with legal obligations or official authorities
- Public health reasons or the performance of a public interest task
- If needed for the exercise or defence of legal claims in some cases, the restriction of personal data may be more applicable, and this could be used an alternative option to erasure or in circumstances where data must be held in limbo pending legal challenges.

Disclosing data for other reasons

In certain circumstances, external bodies request data from **Peter Gill's Rock Schools C.I.C.**, which the company is legally required to comply with. Examples of this are: ▪ Office of National Statistics ▪ HMRC ▪ Department of Work and Pensions ▪ Government Equalities Office

In these circumstances **Peter Gill's Rock Schools C.I.C.** will disclose requested data. However, the company director will ensure the request is legitimate, seeking assistance from the Directors / legal advisers where necessary. We are also required to carry out Criminal Record checks as part of the terms of employment. The Disclosure and Barring service has a Code of practice regarding correct handling, which is adhered to. **Peter Gill's Rock Schools C.I.C.** are authorised to receive disclosure information, and it is a criminal offence to pass this information on to any other person or organisation. References that are sent from **Peter Gill's Rock Schools C.I.C.** are sent in confidence to the attention of the addressee only.

How long data is held for:

- Member Records - 3 years after the date the service provision ceased (Adults)
- Member Records - 25 years after the date the service provision ceased (Children)
- CVs of unsuccessful Applicants for Jobs 3 months
- Employee files 7 years after the date employment ceased
- Accounting transactions 7 years
- Criminal Record Disclosure information 6 months if the employee leaves or does not take up a position within the organisation

Data Breach

If a data breach occurs, please notify the Company Director immediately.

Providing Information

Peter Gill's Rock Schools C.I.C. 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.
- Members are required to read and sign the data consent forms.
- Members or employees who have a complaint about the way that the organisation keeps files about them, or who are refused access to files that they believe they should have access to, should be referred to the Data Protection Information Commissioner.

Additional Information

Eugdpr.org - EU GDPR website

ICO.org.uk – Information Commissioner's Office website.