****

**Data Protection Policy**

**Contents**

1. **Introduction page 1**
2. **Data Protection Principles page 1**
3. **Personal Information page 2**
4. **Legal Basis for Processing page 2**
5. **Sharing Personal Data page 2**
6. **Data Retention page 2**
7. **Individual Rights page 2**
8. **GDPR Breaches page 3**
9. **Further Information page 4**
10. **Related Policies page 5**
11. **Appendix 1 page 6**
12. **Introduction**

1.1 PEEK is committed to protection and respecting our team members and children, young people and families personal data. PEEK complies fully with the necessary requirements under the Data Protection Act 2018 and the EU General Data Protection Regulation (“GDPR”).

1.2 This policy sets out how PEEK handles the personal data of our participants and families, team members, board trustees, volunteers, stakeholders, funders, and other third parties.

1.3 Protecting the confidentiality of personal data is a critical responsibility that we take seriously at all times. If PEEK fails to comply with the relevant data protection law, then we may be subject to substantial sanctions, including potential fines of up to 4% of annual turnover, as well as significant reputational damage.

1.4 This policy applies to all team members, including temporary and sessional team members, volunteers and trustees. All should read, understand and comply with this policy. This policy sets out what PEEK expects from you to ensure that PEEK complies with the relevant data protection legislation. Any breach of this policy may result in disciplinary action.

1. **Data Protection Principles**

2.1 The data protection principles set out the main responsibilities which apply to PEEK when processing personal data in compliance with GDPR. These principles are:

* Fairness/transparency – PEEK only use or store personal data in a fair, lawful and transparent manner;
* Purpose limitation – PEEK only process personal data for specific stated purpose;
* Data minimisation – PEEK only collects and processes necessary personal data;
* Accuracy – PEEK ensures personal data is accurate and up to date;
* Storage limitation – PEEK only retains/stores personal data for as long as is necessary;
* Integrity and confidentiality – PEEK keeps personal data secure at all times.
1. **Personal Information**

3.1 PEEK processes a range of personal data. The categories of personal data can be summarised as follows:

* Participant and family details
* Team members details
* Volunteers including board members
* Stakeholders i.e. partner organisations, schools, etc.
* Funders
1. **Legal Basis for Processing**

4.1 When PEEK processes personal data, we must do so on the basis of one of the lawful grounds set out in the GDPR. The legal process is set out in our Privacy Policy.

4.2 Below are examples of some of the key personal data types we use and the legal bases on which they are processed:

|  |  |
| --- | --- |
| **Categories of Personal Data** | **Legal Basis for Processing** |
| Participant and families details | Legal Obligation  |
| Team members details  | Performance of a contract |
| Volunteers including board members  | Legal Obligation  |
| Stakeholders | Legal Obligation  |
| Funders  | Legal Obligation  |

4.3 Whenever PEEK processes personal data, it must be clear which legal basis is being relied on. All new data processing activities should be subject to a data protection privacy impact assessment.

1. **Sharing Personal Data**

5.1 PEEK does not share your personal information with any third parties unless there is a legal requirement to do so. Where appropriate, PEEK will notify the relevant person(s) if data has been shared.

1. **Data Retention**

6.1 PEEK only retains personal data for so long as it is necessary in connection with the purposes for which it was collected and in line with the Records Retention Policy.

1. **Individual Rights**

7.1 Under the GDPR, individuals have the right to make the following types of request regarding the personal data we have about them:

* Right of access (subject access requests) – the right to request a copy of the personal data PEEK has concerning an individual and supporting explaining how the personal data is used.
* Right of rectification – the right to request that PEEK rectify inaccurate personal data concerning and individual.
* Right of erasure (right to forgotten) – the right to request that PEEK erase all personal data concerning an individual.
* Right to restrict processing – the right to, in some situations, request PEEK do not use an individual’s personal data they have provided (e.g. if they believe it to be inaccurate).
* Right to object – the right to object to certain processing of his/her personal data (unless PEEK has overriding compelling legitimate grounds to continue processing) and the right to object to direct marketing.
* Rights relating to automated decision making – the right to object/opt-out of automated decision making that significantly affects an individual.
* Right to data portability – the right to, in some situations, request PEEK to port an individual’s data to the individual or a new provider in machine readable format.

In certain circumstances, PEEK will be exempt from responding to certain requests

Where you receive a communication from any individual which seeks to exercise any rights in relation to personal data, you must immediately notify Emma Hill, Head of Operations and follow instructions.

1. **GDPR Breaches**

8.1 PEEK has a duty to report data breaches to the Information Commissioner’s Office and in certain circumstances, to the individuals as well. This policy sets out how we will respond to data and cyber breaches. It applies in situation where there is an actual, potential or suspected data breach.

**8.2**  **What constitutes a breach?**

A data breach occurs where there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Examples of a breach involving the loss of personal data could include loss of a PEEK laptop containing personal information; loss of paper copies of personal data.

**8.3 What should you do if you think a personal data breach has occurred?**

If you think a personal data breach has occurred or is likely to occur you must **act immediately** and contact the Head of Operations and notify your line manager. This should be treated as a priority. An email with the details of the potential breach should be sent along with a telephone call to ensure the email has been read and acknowledged.

The information in the email should include the following details to the extent you know them:

1. Details of the actual, potential or suspected breach and how it occurred or may occur
2. If a breach has occurred, the time and data that the breach was discovered and if the incident is ongoing
3. The types of data breached e.g. participant details, staff details
4. The number of individuals the information relates to
5. What steps have been taken or proposed to take to address the breach or potential breach

In no circumstances should you delay reporting the breach if you do not have all the information.

**8.4 Investigation**

The Head of Operations will make an initial determination of whether or not there has been a data breach after considering the facts provided. If it is likely there has been a breach, the Head of Operations will notify the Chief Executive and they will coordinate an investigation.

The investigation should include the following:

1. When did the breach occur?
2. What is the nature of the breach?
3. What is the source of the breach?
4. What categories and numbers of individuals and data records are subject to the breach?
5. What are the likely consequences of the breach?
6. What is the severity of the potential impact of the breach on the individuals concerned?
7. What steps can be put in place to mitigate the impact and stop any further breaches?

8.5 Any investigation should be completed within 24hours.

8.6 A written record should be kept of the investigation even if the incident is not a breach.

**8.7 Report to the Information Commissioner’s Office**

PEEK should notify the ICO once it is aware of a data breach that is likely to results in **a risk** to rights and freedoms of individuals. This should be done within 72 hours of discovering the breach and is the responsibility of the Head of Operations.

**8.8 Notification to individuals**

PEEK should notify individuals once it is aware of a data breach that is likely to result in a **high risk** to their rights and freedoms of individuals.

This should be done following any investigation and is likely to take place over the phone, face to face or via letter.

**8.9 Record Keeping**

PEEK will maintain any documentation of all personal data breaches including decisions taking during the investigation.

**8.10 Further Information**

If you have questions regarding this policy, please contact PEEK’s designated Data Protection Officer – the Head of Operations.

**8.11 Changes to the policy**

This policy may be changed from time to time and you will be notified. The policy will be reviewed annually.

1. **Further information**

If you have any further queries or concerns regarding data protection, please contact:

the Head of Operations (emma@peekproject.co.uk)

1. **Related Policies**
* Employee Handbook
* Records Retention Policy
* Disciplinary Policy
* Child Protection and Safe Guarding Policy

Date Approved:

Approved by:

Next Review Date:

Possibilities for Each and Every Kid PEEK

The Legacy Hub

301 Springfield Road

Glasgow

G40 3LJ

Email: info@peekproject.co.uk

Website: www.peekproject.org.uk

Charity No: SC030814 Company No: 273784

**Appendix 1**

**Data Protection Breach**

|  |
| --- |
| **Practical Steps*** **Do** contact the Head of Operations with any data protection/privacy concerns, issues or queries.
* **Do not** ignore correspondence from individuals which relates to, or which may relate to personal data.
* **Do** notify the Head of Operations immediately if a communication is identified as being a request to exercise data protection rights.
* **Do** remain vigilant and check whether personal data is being stored securely. ALL Child Protection paperwork should be place in a sealed envelope and passed to the Child Protection Officer (Head of People and Programmes).
* **Do not** copy data or store personal data outside of the PEEK systems unless this is strictly necessary.
* **Do** ensure any portable hardware you use for work purposed is password protected and the contents are encrypted.
* **Do** ensure personal data sent via your PEEK email, or otherwise, is protected.
* **Do** ensure any personal data extracted from the systems and stored locally is stored securely and subject to password protection and encryption.
* **Do not** discuss confidential matters or details about particular individuals unless this is necessary for the purpose of your role.
* **Do** remain vigilant and notify your line manager on discovery of anything suspicious/unusual regarding the way in which their systems are functioning.
* **Do not** ignore any incidents/suspected incidents.
* **Do** implement the processes set out in the data breach policy.
* **Do not** store PEEK Participants personal data in personal folders unless strictly necessary.
* **Do** regularly delete personal data from your personal folders, if you are unsure what can be deleted contact the Head of Operations.
* **Do** check PEEK forms are FULLY completed by parents/carers before it is input to the systems.
* **Do** inform Head of Operations if any of your own personal data is out of date or inaccurate
* **Do** ensure all PEEK paperwork is securely stored off site through lockable (Padlock or coded) boxes/rucksacks.
 |