Confidentiality and Information Security Statement

Porchlight uses third party suppliers in the course of operations. Third parties fall into various categories with differing levels of access to personal information, and different impacts upon the information security system.

Providers agree that they will not access Porchlight data unless required to do so. Where a provider is responsible for an IT system for which they have administration rights it is understood that in the course of providing support to the charity they may be required to have access to the data which is held on the system they operate.

Confidentiality

Porchlight work in compliance with the Data Protection Act 2018. In signing a contract with Porchlight, The Provider agrees by extension to uphold the same code of conduct and comply with legal requirements on confidentiality of personal identifiable information. Adequate security controls are to be maintained at all times to protect the information of Porchlight's clients and employees.

Data Processing

The Provider shall keep personal data secure and shall:

- Implement appropriate technical measures to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration and disclosure.
- Notify Porchlight immediately if at any time The Provider suspects or has reason to believe that personal data has or may have become corrupted, lost or degraded in any way or for any reason and inform Porchlight of the remedial action the contractor proposes to take.

Confidentiality and non-disclosure

The Provider shall:

- Treat as confidential all information which may be derived from or be obtained in the course of the contract or which may come into the possession of the contractor or an employee or sub-contractor of the contractor as a result of or in connection with the contract; and
- Provide all necessary precautions to ensure that all such information is treated as confidential by the contractor, their employees or sub-contractors; and
- Ensure that they, their employees and sub-contractors are aware of the provisions of the Data Protection Act 2018 and that any personal information obtained from the organisation shall not be disclosed or used in any unlawful manner; and
- Indemnify the organisation against any loss arising under the Data Protection Act 2018 caused by any action, authorised or unauthorised, taken by himself, his employees or sub-contractors.

"Confidential information" means any information of a confidential or secret nature relating to any and all aspects of the business of Porchlight including but not limited to information about staff/service users and their friends/relatives, personnel data, financial information, budgets, reports, business plans, strategies, know-how, data, research, processes, procedures and programs, client/customer information, pricing, sales and marketing plans and details of past or proposed transactions whether or not written or computer generated or expressed in material form.

In the course of your work in the organisation, you may have access to see or hear confidential information. Unless acting on the instructions of an authorised staff member

within the organisation, on no account should such information be divulged or discussed except in the performance of your normal duties.

To disclose or otherwise use confidential information without proper authorisation would be a breach of confidence, which will also constitute a breach of contract and may lead to termination of your contract with the organisation. Depending on the severity, a breach could also result in a criminal prosecution or civil proceedings for damages under the Data Protection Act 2018.

The Provider shall sign and adhere to this statement and any additional confidentiality and non-disclosure agreements as laid out by Porchlight.

Incident reporting mechanisms
In the case of any suspected incidents involving personal data, the Compliance Manager of Porchlight is to be informed immediately. An incident is classified as any occurrence in which the confidentiality, integrity and/or availability of personal data is compromised.

Incidents also include any suspected foul play with regards to but not limited to; Porchlight's digitally held records; suspected or actual unauthorised access to The Providers offices or The Providers server sites.

Information transfer
The Provider and Porchlight shall agree how information is to be transferred in a safe and secure manner.

Supply chain management
If during the course of business The Provider uses sub-contractors, and these sub-contractors have access to Porchlight's information or information systems, The Provider must:

- Inform Porchlight of the details of any such arrangement before the sub-contractor is given access
- Propagate Porchlight's security requirements throughout the supply chain once approval has been given

Audit and monitoring
Porchlight carry out routine audits on all parts of their information security management system. This extends to third party organisations who have access to Porchlight's information and systems. Porchlight may from time to time request to audit supplier processes and controls directly related to Porchlight operations.