Last reviewed: July 2024

Confidentiality Policy

1. Purpose

Our company confidentiality policy explains how we expect our employees to treat confidential information. Employees will unavoidably receive and handle personal and private information about participants, partners and our company. We want to make sure that this information is well-protected.

We must protect this information for two reasons. It may:

- Be legally binding (e.g. sensitive participant data).
- Constitute the backbone of our business, giving us a competitive advantage (e.g. business processes).

2. Scope

This policy affects all employees, including board members and volunteers, who may have access to confidential information.

3. Policy elements

Confidential and proprietary information is secret, valuable, expensive and/or easily replicated.

Common examples of confidential information are:

- Data of Customers/Partners/Suppliers
- Unpublished financial information
- Patents, formulas or new technologies
- Customer lists (existing and prospective)
- Data entrusted to our company by external parties
- Pricing/marketing and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives marked as confidential

Employees may have various levels of authorised access to confidential information.

What employees should do:

- Lock or secure confidential information at all times
- Shred confidential documents when they're no longer needed

- Only view confidential information on secure devices
- Only disclose information to other employees when it's necessary and authorised
- Keep confidential documents inside our company's premises unless it's absolutely necessary to move them
- Use participant initials instead of names when talking on the phone in public spaces wherever possible
- Use participant initials instead of names in emails
- Save accident and incident forms and daily reports in Dropbox, and don't send them by email
- Save Access Needs in Dropbox, and don't send by email where possible. If emailed, they must be password protected
- Keep printed copies of allergies / photo consent forms safe
- Gain consent to take photos of staff and participants – and stick to it
- Programme Leader must ensure that Find my iPhone is on at all times; this allows us to remotely wipe iPads if they're lost or stolen
- Report any breach to the CEO or Programmes Manager straight away

What employees shouldn't do:

- Use confidential information for any personal benefit or profit
- Disclose confidential information to anyone outside of our company
- Share data with anyone within PPA unless necessary and done securely
- Store data on personal computers / phones including photos and phone numbers
- Give anyone access to laptops or iPads outside of Purple Patch Arts.
- Accept completed access needs forms at Programmes unless pre-arranged. If this has been pre-arranged, type up onto drobox and return the form straight away

When employees stop working for our company, they're obliged to return any confidential files and delete them from their personal devices.

Confidentiality Measures

We'll take measures to ensure that confidential information is well protected. We'll:

- Store and lock paper documents
- Encrypt electronic information and safeguard databases
- Ask employees to sign non-compete and/or non-disclosure agreements (NDAs)
- Ask for authorization by senior management to allow employees to access certain confidential information

Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons. Examples are:

- If a regulatory body requests it as part of an investigation or audit
- If our company examines a venture or partnership that requires disclosing some information (within legal boundaries)

In such cases, employees involved should document their disclosure procedure and collect all needed authorisations. We're bound to avoid disclosing more information than needed.

4. Reporting Mechanisms

All staff are responsible for reporting any breaches or potential breaches of this policy to their Line Manager who will record the facts relating to the breach, its effects, and any remedial action taken. This information will be shared by Line Manager with the Chief Executive Officer, Fran Rodgers for further action, which includes - where appropriate - further investigation. In the event of a Serious Incident, a Serious Incident Report will be created by the Chief Executive Officer and shared with the Board of Trustees in accordance with the Serious Incident Policy.

5. Disciplinary Consequences

Employees who don't respect our confidentiality policy will face disciplinary and, possibly, legal action.

We'll investigate every breach of this policy. We'll terminate any employee who wilfully or regularly breaches our confidentiality guidelines for personal profit. We may also have to punish any unintentional breach of this policy depending on its frequency and seriousness. We'll terminate employees who repeatedly disregard this policy, even when they do so unintentionally.

This policy is binding even after separation of employment.

6. Review

This policy will be reviewed biennially.