PRIVACY & CONFIDENTIALITY

Policy No & Version	2.04 – V1.3
Policy Folder	Governance & Operational Management
Document Owner	CEO
Release date	11/10/2022

POLICY

In compliance with the Privacy Act 1988 McCall requires employees (board members, staff, contractors, consultants, volunteers and students) to respect and maintain the confidentiality of individuals and the organisation's business at all times.

Employees may from time to time have access to information that is confidential to McCall and/or other agencies that have dealings with McCall, which is be remain confidential at all times.

Confidential information includes but is not limited to the following:

- participant personal information
- participant & staff contact information
- personal information provided by staff or about staff in the course of performance reviews, leave applications, supervision sessions or similar discussions
- information about any internal dispute or grievance
- business conducted in board, management and staff meetings, other than that identified as being for public discussion
- any confidential and proprietary information concerning financial transactions, competitive tenders or expressions of interest or any other organisational plans or activities identified by the board and management team of McCall.

PROCEDURE

- Sign a Confidentiality Agreement.
- Retain all confidential information in the strictest confidence and not disclose any confidential information to any person other than for purposes directly related to your position at McCall.
- Not use any confidential information which you have acquired in relation to the activities of McCall for your own interests or the interests or purposes of others not associated with McCall.
- Not make copies of any confidential information for any other reason other than those essential to and directly related to your position and responsibilities with McCall.
- Upon the request, and in any event upon the cessation of your engagement or employment with McCall to return or destroy materials containing confidential information in your possession.
- Not hold any confidential information including photos on your own personal device without the consent of your supervisor.
- Documentation provided to participants must clearly outline the organisations obligations on what information we obtain, disclose and retain in accordance with all relevant legislations.
- This will not prevent an individual from:
  - disclosing information to proper authorities in relation to concerns about improper conduct, breaches of laws or breaches of duty of care
  - providing access for external reviewers to non-identified information for the purposes of formal audit processes
  - making a formal complaint to appropriate authorities about an aspect of the organisation's operation

- disclosing information that they may be required to disclose by any court or regulatory body or under applicable law

NOTIFICATION OF ELIGIBLE DATA BREACHES

- A data breach occurs when personal information that McCall holds is subject to unauthorised access or disclosure or is lost.
- Personal information is information about an identified individual, or an individual who is reasonably identifiable. This includes information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identified' as a result.
- A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.
- Under the Notifiable Data Breaches (NDB) scheme, McCall will notify affected individuals and the Australian Information Commissioner about eligible data breaches.
- An eligible data breach occurs when the following criteria are met:
  - there is unauthorised access to or disclosure of personal information held by McCall (or information is lost in circumstances where unauthorised access or disclosure is likely to occur)
  - this is likely to result in serious harm to any of the individuals to whom the information relates
  - McCall has been unable to prevent the likely risk of serious harm with remedial action
- Staff to report any data breach to their manager and complete an Incident Report within 24 hours of becoming aware of the breach.
- All data breaches to be reported to the CEO and managed in accordance with the Australian Government: Office of the Australian Information Commissioner (OAIC): Data breach preparation and response guide.
- Any data breach involving participants will the notified to the NDIS Commission as a reportable incident in accordance with the NDIS (Incident Management and Reportable Incidents) Rules 2018.

BREACH OF THE POLICY

- Failure to comply with the requirements contained in this policy will lead to disciplinary action, which may include, but is not limited to, termination of an employee's employment or engagement of a contractor's services.