CLIENT DATAPOLICY

OVERVIEW

Top Blokes Foundation (The Company) is committed to providing the highest level achievable in the quality of our all products and services in accordance with the client's requirements and the applicable statutory, regulatory and industry requirements.

Top Blokes Foundation recognises the importance of secure management of IT systems as a vital part of sound business operation. The company aims to ensure that all client information is kept secure and confidential. At times, client information may need to be shared with a third party. The policy outlines the process for when this is required.

This policy applies to all employees of the Company who use computer systems or work with documents or information that concerns clients, suppliers or any other partner for whom the organisation has collected information in the normal course of the business.

OPERATION

In so far as this policy imposes any obligations on the Company, those obligations are not contractual and do not give rise to any contractual rights. To the extent that this policy describes benefits and entitlements for employees, they are discretionary in nature and are also not intended to be contractual. The terms and conditions of employment that are intended to be contractual are set out in an employee's written employment contract.

The Company may unilaterally introduce, vary, remove or replace this policy at any time

THIRD PARTY ACCESS TO CLIENT INFORMATION

Top Blokes Foundation aims to ensure that all client information is kept secure and confidential. At times, client information may need to be shared with a third party. For all instances where this is required, employees, volunteers and contractors must obtain the client's consent prior to sharing their information with the third party.

When inviting a third party to access a client's data, in any form, you must receive written authorisation from the client before allowing access. When you have the clients' authorisation, in writing through a formal consent process. Any kind of information relating to a client's affairs must be protected by you and any administrative staff; whether that information is personal, or business related or financial.

You may not release any information to a third party without specific authority from the client. In addition, you are most likely to be bound by the Privacy Act 1988. The Act is relevant for almost all businesses. The Company simply assumes that the privacy principles apply to us.

CONFIDENTIAL PHYSICAL FILE STORAGE IN WORKSPACES

Physical records and files stored in workspaces should primarily be those still required for ongoing use by employees, volunteers and contractors in the workspace. Only records or files in active use should be kept on desks. All other records in workspaces should be stored securely in filing cabinets, drawers, cupboards or in other secure storage facilities. In general, records are stored in workspaces because ongoing access to them is required.

REMOTE CONFIDENTIAL PHYSICAL FILE STORAGE & DISPOSAL

Employees, volunteers and contractors must keep all confidential physical files secure at all times. Confidential documents and paperwork should be stored securely and/or disposed of appropriately to ensure confidentiality.

DATA STORAGE & DISPOSAL

Client data is digitally stored though our third party programs such as Salesforce, SocialSuite and Dropbox. All third party platforms have the highest security settings applied for login and access. All data collected in Salesforce and Socialsuite is stored in servers within Australia. Client Data that is deleted from digital systems is immediately disposed of from third party servers.

CLIENTS AND WEBSITE VISITORS

Top Blokes Foundation respects the right to privacy and is committed to safeguarding the privacy of our clients and website visitors. We adhere to the Australian Privacy Principles contained in the Privacy Act 1988 (Cth Australia).

BREACH OF POLICY

Any breach of this policy will be dealt with in accordance with the company's Discipline and Termination Policy and may result in disciplinary action up to and including termination of employment contract. In addition, unlawful or illegal use of the Company's internet or email systems may constitute a civil or criminal offence for which you could be personally liable.

REVIEW

The Company may unilaterally introduce, review, vary, remove or replace this policy at any time.

OTHER POLICIES

Employees, volunteers and contractors are encouraged to read this policy in conjunction with other relevant Company policies, including:

- Code of Conduct
- Discipline & Termination Policy
- Information Security and Management Policy