Privacy Policy

Policy name:	Privacy Policy		
Policy no.:	DT-101		
Date issued:	11/11/2016		
Approved by:	Mark Thrift		
Date reviewed:	13/02/2018	**Reviewed by:**	Mark Thrift

Policy outline

DataTrust respects the privacy of our clients, contractors, employees and suppliers. As such we have taken appropriate steps to comply with the *Australian Privacy Act of 1988*.

The following policy outlines our commitment to adhering to this Act.

Contents

What data do we collect?

DataTrust only collects data that is relevant to our business dealings. This includes resumes, contact names, business addresses, email and internet addresses, telephone and fax numbers.

DataTrust does collect and store the financial records of our dealings with clients, sub-contractors and suppliers.

DataTrust does collect financial information relating to credit references with regards to our clients and sub-contractors.

We do not collect personal or sensitive data regarding any employee or owner of any sub-contractor or client, unless this is specifically related to a work practice.

DataTrust collects and stores sensitive and personal information regarding employees. This includes addresses, telephone numbers, next of kin, employment references, financial details and police histories.

When do we destroy the data we collect?

DataTrust keeps records for a period of one full year in “active service”. Any paper-based records are stored in locked filing cabinets at our head office

DataTrust archives all legally required records after a period of one year. These are stored at our head office for a period of not less than seven years.

DataTrust destroys all non-legally required records after a period of one year by the means of a shredding machine on our premises.

How do we store the data we collect?

DataTrust stores all data related to clients or sub-contractors and employees in an electronic database. Backup hard copies of this data are kept in a locked filing cabinet at our head office.

How do we protect the information we store?

DataTrust electronic data is protected by a Watchguard Firebox firewall. This firewall is designed to prevent intrusion from unauthorised parties accessing information stored on the DataTrust network via the internet.

DataTrust virus protection is regularly updated to protect against the loss or corruption of data from a virus, and to prevent the installation of any virus that may provide unauthorised parties with a “back door” into our computer systems.

All authorised personnel require a password and a logon to access the DataTrust network. This applies to both internet access and onsite computer terminal access.

Logons for the DataTrust network can only be authorised via the DataTrust Systems Administrator. Only DataTrust permanent staff may apply for a logon to this network.

Security levels are set for each logon, so that non-essential staff cannot view details that are not relevant to their position.

DataTrust has a strict confidentiality agreement in place with all staff and sub-contractors. All staff and sub-contractors are aware of the principals of the *Privacy Act of 1988* and have a copy of this corporate Privacy Policy included in the Corporate Procedures Manual.

DataTrust staff or sub-contractors may not export any information regarding our clients for non-business purposes. This includes downloads to external or removable drives, photocopies, original hard copies, email (including attachments) or uploads to the internet. The only exception to this is if the information is required to complete a current job for a client.

DataTrust staff or sub-contractors may not give out any information regarding our clients via the telephone to non-authorised parties, unless directly related to a current business activity for a client.

DataTrust stores all hard copy or paper data in locked filing cabinets at our head office.

DataTrust has an extensive security system in place to further ensure the security of both electronic and hard copy information.

Who do we disclose information to?

DataTrust only discloses the business-relevant information collected by us to our suppliers and sub-contractors when requested for legitimate business purposes.

We do not under any circumstances pass on information relating to our clients to third parties for non-direct business-related reasons.

DataTrust reserves the right to pass on relevant details of current clients to prospective clients for purposes of site references, where the existing client has specifically authorised DataTrust to use this information for this purpose.

What must DataTrust do?

- DataTrust must abide by this corporate Privacy Policy.
- DataTrust must abide by the *Privacy Act of 1988*.

As a company, DataTrust must ensure that the information we store is accurate and up to date. If information is found to be incorrect, we must rectify this within a reasonable period of time.

We must only store information that is relevant to our business dealings with the client, sub-contractor, supplier or employee.

We must adequately protect the privacy of our clients, employees, suppliers and sub-contractors. This includes appropriate IT infrastructure, internal security measures and training for our staff.

We must disclose to any client, sub-contractor, employee or supplier the information that we hold about them.

DataTrust must make this policy available to anyone who asks for it.

We must disclose to whom we supply information, and specify what information has been provided to third parties. This must be approved by the client, employee, sub-contractor or supplier to whom the information applies.

We must undertake to train all staff to ensure that this Privacy Policy is understood and implemented in an appropriate and accurate manner. This must take place during induction training and is the responsibility of the Department Manager to implement and the responsibility of the Human Resources Manager to ensure occurs.

Responsibilities of DataTrust employees

- You must abide by this corporate Privacy Policy.
- You must abide by the *Privacy Act of 1988*.

You must not pass on information of any kind to unauthorised parties about any employee, client, sub-contractor or supplier of DataTrust without the organisation's or person's specific approval.

You must not store or collect personal data about any employee, client, sub-contractor or supplier of DataTrust.

If you wish to have personal information regarding yourself disclosed to a particular business or person you should approach your HR Officer.

You must not remove documents or information in any format from DataTrust premises unless it is specifically related to a business activity of DataTrust.

Dealing with complaints

If any client, employee, sub-contractor or supplier wishes to make a complaint regarding the information we hold about them, or our Privacy Policy, please address them to the Human Resources Department.

Sub-contractors

- All sub-contractors conducting work on DataTrust's behalf must sign a confidentiality agreement prior to carrying out work for the company.
- All sub-contractors must read and understand our Privacy Policy prior to beginning work on DataTrust's behalf.
- All sub-contractors are bound to abide by DataTrust Privacy Policy whist carrying out work on DataTrust's behalf.