GBWCT POLICY

Document Number: **00.10.02**
Effective Date: **20/06/2023**
Last Review Date: **02/12/2022**
Next Review Date: **01/01/2027**
Status: **APPROVED**

DOCUMENT MANAGEMENT POLICY

This Policy establishes standards for document management across all of the Golden Bay Workcentre Trust's functions and operations, and for ensuring documents are created, maintained and disposed of appropriately, taking full account of operational needs.

1.0 Purpose

The GBWCT must ensure that documents created in relation to its operations are being managed and maintained appropriately. This policy sets out standards and definitions to enable staff to create documents that:

- Meet GBWCT internal requirements
- Enable the content of the document to be accessed, used and reused in a controlled and efficient manner
- Ensure the continuity of GBWCT operations in the event of staff absence or emergency circumstances
- Are compliant with all regulatory and statutory requirements
- Enable the defence of the rights and interests of the GBWCT, staff, clients, and its stakeholders
- Are capable of providing evidence of a decision or operational process
- Are kept and maintained and stored in the most economical way consistent with the above objectives

2.0 Scope

This policy applies to all members of the GBWCT and any individual creating or handling documents on behalf of GBWCT.

The policy applies to all documents held in any format, including (but not limited to):

- Letters (digital and hard copy)
- Emails
- Policies and guidance
- Meeting papers and minutes
- Reports

- Contracts
- Presentations
- Official communications
- Photographs
- Audio recordings (other than voicemail messages)
- Personnel files
- Client/student files
- Research data

Voicemail, text or instant messages do not constitute documents for the purposes of this policy, unless recorded or retained for specified purposes in accordance with legal requirements.

Storage of all other on-site digital files is managed via the *Storage of Digital Files* policy which specifies where files are to be stored electronically and the back-up process.

3.0 Roles and responsibilities

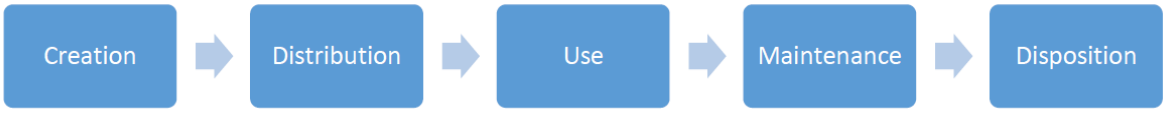
The General Manager is accountable for ensuring that the GBWCT has robust information management and security processes and procedures in place – this includes document management. The General Manager also has operational responsibility for this policy and ensuring that it complies with legal and regulatory requirements.

Individual staff are responsible for ensuring that any information assets they own are managed in accordance with this policy, and also for maintaining standards in relation to document management in their operational area.

All staff are responsible for creating and using documents in line with the terms of this policy.

4.0 Document lifecycle

All documents created have a "lifecycle" from creation through to disposition, as shown below:



It is important to understand this cycle and the various stages when creating and handling documents to ensure that they are managed effectively.

Creation
Documents that will represent formal, compliant and trusted communications or records must be well-designed from the point of creation, using relevant naming conventions and document templates when necessary. All staff must act responsibly, lawfully and professionally when creating documents relating to GBWCT activities and/or on GBWCT systems.

Distribution
When documents are transmitted or otherwise made available to those who need them and, upon receipt, are used in the conduct of GBWCT operations.

Use
Use takes place after a document has been distributed internally, and can generate business decisions, further actions, or serve other purposes.

Maintenance
While a document is in active use, it is vital that the content is maintained, accurate and available to those who require it at all times.

Disposition
The practice of handling information that is accessed less frequently or has reached its assigned retention periods. This could mean destruction of the document(s) or transfer to an archive until the assigned retention period is reached.

See appendix I for *GBWCT Records Retention Schedule* showing retention periods for various categories of information.

5.0 Document management practices

The below list sets out practices that must be adhered to when creating and handling documents on behalf of GBWCT:

- Documents must be clearly named (with date and version number if relevant) and stored in a structured manner (see next section)
- Duplicate copies of documents must not be created unnecessarily
- Wherever possible, documents must be shared from their source location rather than attaching documents to emails
- Key documents (that others may require access to) must be stored in an appropriate shared filestore, i.e. not personal filestores (including desktop or device filestores)

- Copies of documents, whether digital or hard copy, must only be taken offsite when necessary (encrypted and password-protected removable storage or remote access via a secure network connection must be used whenever possible)
- Digital copies of documents should never be emailed to a personal email account or stored on a personal cloud-based storage account
- Once a document is finalised, previous versions and drafts of documents should only be retained where entirely necessary e.g. for legal or audit purposes
- Final copies of formal documents (such as policies or minutes) must be saved in PDF format
- As standard practice, the filename and storage location should be included in the footer of the document

6.0 Naming conventions and folder structures

A naming convention is a collection of consistent rules followed in naming documents, which should allow users to work effectively, ensure that files can be easily accessed by all who require access and to ensure that individuals are referring to and working on the correct document. The use of consistent naming conventions will improve efficiency by allowing staff to quickly identify the nature of the information contained within a document when searching through an archive or filestore. For further information, please see relevant guidance on naming conventions.

Folder structures and names are also important in allowing the efficient retrieval of documents. The below principles must be followed when creating new folder structures:

- Folders must be clearly named by a relevant and meaningful subject area
- The names of individuals should only be used when creating a case file, i.e. not creating a personal folder in a shared filestore
- Top level folders must be kept to a minimum
- Ideally, file structures should not exceed six levels of subfolders
- Appropriate access levels must be assigned depending on necessity to access the documents contained within the folder

7.0 Information Classification

The GBWCT uses an information classification system which has five levels of security classification for different types of information, shown below with examples:

Classification	Definition
Public	**May be viewed by anyone, anywhere in the world:** • GBWCT Website • Social media posts • Newsletters • Publications (Annual Report etc) • Marketing and other promotional materials • Some organisational policies (i.e. complaints)
Open	**Available to all members of GBWCT staff** • General organisational information (i.e. staff handbook) • Organisational forms • Resources • Training material • Policy and procedures
Confidential	**Available only to authorised members of staff** • Client information • Information relating to specific teams and departments
Confidential & Sensitive	**Access is controlled and restricted to a small number of named members of staff and/or Trustees** • Personnel records • Complaints • Client information that could be damaging to the person/s concerned (i.e. child protection concerns, abuse, family violence, criminal offending, drug use etc)
Secret	**Known to only to a very small number of members of staff and/or Trustees** • Legal or criminal proceedings • Employment disputes • Information relating to "in committee" discussions held at Trust meetings

While it is not mandated that all documents and records are marked with the relevant classification, it is good practice to include the classification in the document header or footer, email subject and/or body, or stamp (on a hard copy), to ensure that users and recipients are aware of the potential sensitivity of the content.

Staff should consider the following questions and exercise their judgement in each case:

Does the document contain information that originated from an open and publicly-accessible source?	Provided the document contains information that was not obtained in breach of any confidentiality or secrecy obligation and is in the public domain, the document may be classified as open or public depending on the other questions to be considered below.
Does the document contain personal data?	Any information that may directly or indirectly identify an individual. Documents that contain personal data should be classified as Confidential.
Does the document contain special categories of personal data or personal data relating to sensitive issues such as a child protection concern, Mental Health, or criminal convictions and offences?	This information requires additional procedures to be followed and safeguards applied and should be classified as Strictly Confidential.
Does the document contain any information of commercial or competitive value for GBWCT or any other third party?	The document may contain commercially sensitive information or trade secrets relating to GBWCT or entrusted to GBWCT by a third party or information relating to GBWCT strategic plans and contract opportunities.
If the document was accidentally disclosed, or published in a public forum would it pose a risk to any individual(s) or GBWCT?	The document may contain information which would have an adverse impact on one or more individuals or groups within GBWCT, the organisation as a whole (including reputational harm) or GBWCT, clients, participants, staff, agents, suppliers or other partners.

8.0 Digital preservation

Where documents or records are either “born digital” or where hard copies are digitised, GBWCT will ensure that there are appropriate standards and guidance in place to ensure that records of permanent or continuing value remain accessible and preserve their integrity for as long as required, accounting for changes in IT software and hardware.

Adherence to these standards and guidance will safeguard the authenticity and integrity of digital materials in the long term and will allow the storage of digital materials safely through adoption of security mechanisms appropriate to each classification of material.

9.0 Storage of Hard Copy Files

The preferred storage arrangement for documents (hard copy) is manila folders and ring binders, labelled with year, main content, and stakeholder (if appropriate) identifying information and stored in locked file cabinets or locked offices or storage rooms.

Files stored in filing cabinets should also be kept in a rational manner, with suspension files clearly labelled, preferably alphabetically. This is to enable other staff to locate material when necessary.

Each staff member is responsible for their own filing, ideally in a rational, consistent system (e.g. all in ascending date order, or divided by topic, alphabetically by surname, etc.) that other authorised users such as the Manager can access intuitively.

Each person should review the files they are responsible for at least annually. They should retain current work, archive material that must be kept, and dispose of unwanted material according to the procedures outlined below.

10.0 Archiving

Inactive files (digital and hard copies) will be archived and accessible according to legislative and audit requirements.

The IT Administrator shall retrieve documents from the backups or provide restore functions in the case of major system breakdown.

Key documentation has requirements as to the duration for which it must be kept. Do not dispose of any documentation if it is required to be kept for a specified period of time that has not yet been reached (see *GBWCT Records Retention Schedule)*. These documents and records should be stored in the physical archives located in the main office loft (the mezzanine floor above the back office). The main office is to remain locked at all times when no staff are present to preserve the security of these records.

Archived files should be held in standard file boxes, labelled, and stored correctly by year. White file boxes should contain general records for eventual destruction. Red file boxes should contain information that is to be kept and stored permanently.

11.0 Destruction

All documents must be subject to action proscribed in GBWCT Records Retention Schedule, which may be destroyed at the end of the assigned retention period unless such period has been suspended on learning of an actual or reasonably anticipated claim, audit, investigation, subpoena or litigation asserted or filed by or against GBWCT.

No one should delete a document created by another user without consulting them/or the General Manager.

Unneeded printed documentation with content that is commercially sensitive, confidential, or subject to privacy legislation and does not need to be kept may only be disposed of in the shredding bin, or secured and shredded/disposed of by a professional agency engaged to do so. This includes financial records, documents that identify an individual such as performance records or learner personal records, or that identify the Trust such as draft contracts etc.

Other scrap paper should be disposed of in the paper recycling bin or wastepaper baskets. This may include any documentation that is publicly available (e.g. on the intranet, noticeboards, standard letter drafts etc.), or would not put the Golden Bay Workcentre Trust at risk or be misused if picked up casually.

Management personnel should periodically determine whether any documents under their control should be destroyed in accordance with the *Records Retention Schedule*.

12.0 Related Documents

GBWCT has a number of existing policies and procedures that have relevance to document and records management, as below, and staff must be aware of their content:

00.08.03 Internet Access Policy 2021

00.16.01 Policy Framework and Guidelines 2021

01.09.02 Storage of Digital Files 2020

01.11.02 Confidentiality Policy 2021

01.13.01 Privacy Policy 2021

All documents processed on behalf of the GBWCT must comply with the various legislation relevant to information governance and security.

GBWCT Records Retention Schedule

Item	Retention time
Accounting records	not less than 10 completed accounting periods and the current accounting period
Agreements with architects, builders etc	6 years after completion of the contract
All trust deeds and rules	Permanently
Annual reports	Permanently
Annual returns	Permanently
Application for jobs - unsuccessful	up to 1 year
Auditor's reports	Permanently
Bank statements	7 years
Board committee minutes	not less than 10 years
Board minutes	not less than 10 years
Books of accounts giving information sufficient to comply with Companies Act 1993	Permanently
Certificates and other documents of title	Permanently
Cheques, bills of exchange and other negotiable instruments	7 years
Constitution of the company	master copy to be kept permanently
Contracts with agents	6 years after expiry
Contracts with purchasing agencies	6 years after expiry
Contracts with suppliers	6 years after expiry
Deeds of title	Permanently
Drivers' log books	7 years after completion
Employment agreements/Employment contracts	Permanently
Expense accounts and petty cash	10 years
Financial statements	not less than 10 completed accounting periods
H&S Incident / Accident books	Permanently
Instructions to banks	7 years
Insurance policies	10 years
Interests register	master copy to be kept permanently
Investment records	Permanently
Lease agreements	12 years after lease has terminated and all terminal queries (e.g. dilapidations) settled
Licensing agreements	6 years after expiry
Major agreements of historical significance	Permanently
Notification of change of address	1 year
Patent agreements with staff	16 years after employment ceases
Payrolls	12 years
Periodic accountancy reports, eg. to Board	file copies for 7 years
Personal record of organisations management staff	permanently for historical purposes
Policies	Permanently
Published accounts (including annual reports)	signed copy permanently
Reports and opinions	16 years
Salary register	up to 5 years

Salary revision schedules	up to 5 years
Staff personal records	7 years after employment ceases
Subscription records	3 years after cessation of membership
Tax returns	Permanently
Taxation returns and books	Permanently
Time sheets and piece work records	2 years
Training records/list of attendances	6 years
Trustees' minute book	Permanently
Vehicle maintenance records	7 years after vehicle disposed of
Vehicle mileage records	7 years after vehicle disposed of
Wage records (including overtime details)	7 years

**source: Governance NZ – Good Governance Guide https://www.governancenz.org/Category?Action=View&Category_id=194*

Books of account giving information sufficient to comply with the Companies Act 1993 and Financial Reporting Act 1993 - not less than 10 completed accounting periods and the then current accounting period of the company

Financial Statements and Group Financial Statements required by the Companies Act 1993 or the Financial Reporting Act 1993 - not less than 10 completed accounting periods and otherwise as above

A record of all goods and services supplied by and to that registered person showing the goods and services, and the suppliers or their agents, in sufficient detail to enable these to be readily identified by the Commissioner - 7 years

All relevant invoices, tax invoices and credit and debit notes and GST return adjustments - 7 years