SECURE DOCUMENT CONTROL POLICY

POLICY STATEMENT
It is the policy of the Golden Bay Workcentre Trust to manage storage of its paper and electronic documents and data to ensure privacy, security and safe storage of all records.

The Golden Bay Workcentre Trust's electronic filing system is designed to facilitate the safe and efficient storage of electronic files and is regularly revised and updated as necessary. The system administrator and the Manager have access to all drives and folders. Other staff have limited password controlled access that enables them to create, save or view documents according to their portfolio of work.

1. **Electronic Databases:**

   Wherever possible, existing databases such as the student management system or online services, such as ART and TEC Workspace should be used as the location to collect, store and retrieve data. These databases are password protected and backed up by our approved I.T. personnel either here at the Workcentre or by the relevant government agency in the case of on-line databases.

2. **Electronic non-database data:**

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

3. **Storage of printed materials:**

   3.1 The preferred storage arrangement for documents 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 storage rooms.

   3.2 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.

   3.3 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.

   3.4 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.

4. **Inactive files**

4.1 Inactive files will be archived and accessible according to legislative and audit requirements.

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

4.3 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.

Examples of some retention requirements:

- Financial records:
  - Records that may be required by IRD: **7 years**
  - Contract agreements with funding agencies: **7 years**

- Documentation required for moderation:
  - Learners' assessment materials: **10 years**
  - Learning resources: **3 years**
  - Evidence that self-assessment activity is being carried out: **4 years**

5. **Disposing of unwanted documents and data**

5.1 Staff shall not delete emails. The system administrator archives all the emails, and in the event of any of these being required, e.g. as evidence in legal situations, they can be retrieved on request.

5.2 No one should delete a document created by another user without consulting them/or the system administrator.

5.3 Unneeded printed documentation with content that is commercially sensitive, confidential, or subject to privacy legislation, may only be disposed of in the shredding bin, or preferably 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.

5.4 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.