

# TE PĀTAKA KŌRERO

## Content Storage



### WHĀINGA

To ensure that the content that is shared into the Pātaka system is stored securely and protected from being lost

### HOW IS THE CONTENT STORED IN THE PĀTAKA?

The Pātaka system has the ability to connect to multiple storage locations. This means you can choose where you want the content that is uploaded to be stored. This could be:

- locally (e.g. on your computer hard-drive) - meaning access to your content requires your computer,
- on the internet (e.g. in one of your other secure accounts like YouTube or Vimeo) - where your content is secured through your log-ons to those accounts, and/or
- in external storage (e.g. the Pātaka data centre facility) where access can be defined as you upload your content.

## Content Upload



### WHĀINGA

To allow content creators to upload, manage and define how their content is described, accessed and protected within the Pātaka system.

### HOW IS THE CONTENT MANAGED AND UPLOADED IN THE PĀTAKA?

This is the administration centre of the Pātaka system, where you can upload content. There are three key components of how users/groups can upload and manage the content they put into the Pātaka system. This includes:

- the ability to describe what you are uploading so that when you (or others you allow access) want to find it again they/you can (i.e. metadata),
- the ability to define who has access to your content, and how that will occur, and
- where you want your content to be stored (see Secure Storage for examples) once in the Pātaka system.

When uploading your content you can also determine additional layers of security (see Content Security) to protect your content.

## Content Security

### WHĀINGA

To provide extra layers of security in both the Pātaka system (encryption and anti-virus) and physical storage (your computer and your archive) of the content that is uploaded into the Pātaka system.

### WHAT ARE THESE SECURITY MECHANISMS?

#### Encryption

Encryption is a process that keeps your content safe by scrambling the data when it is uploaded before it is sent to where it is stored.

The only way to unscramble the content when trying to retrieve it from the storage place is by having an Encryption Key that only your log on will have available unless you choose to share with others.

#### Anti-virus

Anti-virus is a computer software (e.g. Norton Anti-virus) that provides protection from computer or internet-based viruses that could infect your computer or storage.

This is included in the Pātaka system, but your anti-virus should be up to date on your computer too!

#### Archiving

It is always good practice to keep a back up copy of the content that you create and upload. While the Pātaka system doesn't archive for you, we suggest that this is part of your content safety protocol.

A physical back up in another location might come in handy if something catastrophic happens (e.g. a natural disaster that destroys the data center).

## Content Access & Synthesis



### WHĀINGA

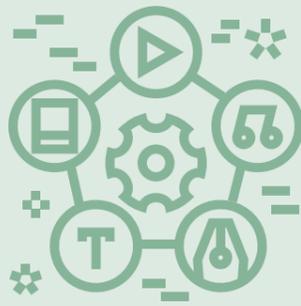
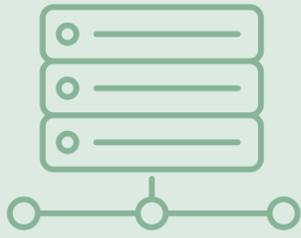
To enable all content you have uploaded to be accessible to you and others, and support you to see the information you have access to in a way that makes sense when you look for it.

### HOW IS THE CONTENT ACCESSED AND SYNTHESISED IN THE PĀTAKA?

The Pātaka system is intended to enable you to store your content safely, but also help you and others to access content stored in the Pātaka system. It enables people to network amongst each other and retrieve content in ways that are useful (e.g. spatial mapping of content and themed collections).

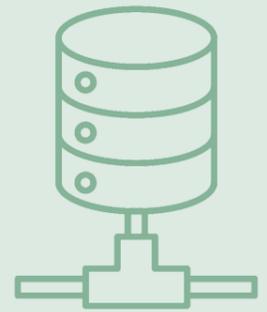
## LOCAL STORAGE

Users/groups private/personal data storage used to save and store a copy of the content uploaded to the Pātaka system



## REFERENCE:

A unique identifier that links to a resource on the internet (e.g. to a person's YouTube or Vimeo content already stored in their account)



## DATA CENTRE

External to the users/groups storage options. This is a facility purpose built to house data for the Pātaka system



## ENCRYPTION

Encoding of content to be stored requiring a key to access and de-code the content before viewing.



## ANTI-VIRUS

Software programs used to scan for, detect, delete and prevent infection from viruses in the system. This protects both the administering device as well as the storage space



## MANAGING CONTENT

User/group defined location and security mechanisms for content being stored



## USER DEFINED CONTENT

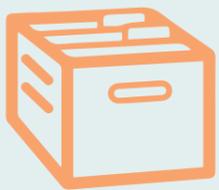
User/group defined descriptions and information (metadata) about content that is uploaded



## USER DEFINED CONTENT

## ARCHIVING

User/group archiving of content in a second safe storage location (e.g. harddrive, a second computer)



## MANAGING ACCESS

User/group defined access to content, both how content is accessed and who can access content that is uploaded



## SYNTHESIS OF CONTENT

Mechanisms to synthesise all content accessible to user (e.g. spatial synthesis)



## CONNECTING TO CONTENT CREATORS

Ability to seek permission for access directly from the content creators, and network with others using the Pātaka System



## CONTENT ACCESS & SYNTHESIS

## CONNECTING TO CONTENT

Users able to view individual pieces of content through search functions.

