INFORMATION AND RECORDS MANAGEMENT POLICY

Table of contents

Introduction

The establishment of an effective and efficient record-keeping environment ensures standardisation, protection and retrieval of information improving levels of quality customer service.

Good records management is a key component of good governance. Records are vital ingredients in the support of the organisation's ongoing business activities. Kingfisher Garden Centre is committed to managing its records in accordance with best practice standards and to fulfil its responsibilities under other Acts such as the *Freedom of Information Act 1991* and *Privacy Act 1988*, as well as fulfilling legal processes, such as discovery and subpoenas. Records may also be required by the Ombudsman, the courts, auditors and other people or bodies.

This model policy provides the procedural framework for Kingfisher Garden Centre to effectively fulfil its records management obligations and to meet the statutory requirements upon it.

Definitions

Accountability

The principle that individuals, organisations and the community are responsible for their actions and may be required to explain them to others (AS ISO 15489 International Standard on Records Management).

Archive

Those records that are appraised as having continuing or permanent value.

Employee

Includes persons employed by Kingfisher Garden Centre, trainees, work experience placements, independent consultants and contractors and other authorised personnel offered access to the Council's resources.

Dispose of

To dispose of an official record means to:

- destroy or abandon the record;
- carry out an act or process as a result of which it is no longer possible or reasonably practicable to reproduce the whole or a part of the information contained in the record; or

- transfer or deliver ownership or possession of or sell the record, or purport to do so,

but does not include to transfer or deliver the record to Kingfisher Garden Centre head office or between Kingfisher Garden Centre's stores.

Electronic records

Records communicated and maintained by means of electronic equipment.

Email

A service that enables people to exchange documents or messages in electronic form. It is a system in which people can send and receive messages through their computers. Each person has a designated mailbox that stores messages sent by other users. You may retrieve, read and forward or re-transmit messages from your mailbox.

Information asset

A body of information and knowledge that is organised and managed as a single entity, is valuable to the organisation and easily accessible to those who need it. Includes data, information, knowledge and records.

Normal administrative practice

Provides for the routine destruction of drafts, duplicates and publications, with the test that it is obvious that no information of more than transitory or temporary value to the organisation will be destroyed. Material that can be disposed of under normal administrative practice comprises items of a temporary or transitory nature created, acquired or collected by Kingfisher employees in the course of their official duties. Such material has no ongoing value and is not usually incorporated into the Council's record management system.

Record

A record means:

- anything on which there is writing or braille
- a map, plan, diagram or graph
- a drawing, pictorial or graphic work, or photograph
- anything from which images, sounds or writings can be reproduced with or without the aid of anything else
- anything on which information has been stored or recorded, either mechanically, magnetically, electronically, written, graphic or pictorial matter, or
- a disk, tape, film or other object that contains information or from which information may be reproduced (with or without the aid of another object or device).

Temporary records

A record is temporary in nature if it is of little or no continuing value to the organisation and only needs to be kept for a limited or short period of time, such as a few hours or a few days.

Policy aim

Record management

This policy aims to establish a framework for the implementation and maintenance of an appropriate records management system. Kingfisher operates in an accountable and community orientated environment and is committed to maintaining a records management system that meets its business needs as well as its legal and accountability requirements.

Information management

This procedure provides employees with their responsibilities to appropriately manage information (specifically records, data and information assets) which they may receive, create, use, store or dispose of within the organisation. This includes classifying information for appropriate protection and/or disclosure.

This procedure further enables the enhancement and integration of information management, empowers local decision-making, and increases capability to share information between other Kingfisher stores and our partners.

Policy scope

This document applies to all Kingfisher business, including electronic business. It concerns records which are created, collected, processed, used, archived, stored and disposed of in the conduct of official business. It applies to all Kingfisher employees.

Electronic communications which are relevant to the information gathering, policy formulation or decision-making processes of the organisation are part of the scope of this document. Electronic messages which document business activity should be printed, registered and placed on Kingfisher files until electronic records management procedures and practices are developed and implemented. All procedures and records management systems are to be consistent with this document.

Australian standards

The development of these procedures for record keeping is closely related to the *Australian Standard on Records Management (AS ISO 15489)*. Many of the definitions and methods of managing records have been based on the recommendations of the Standard.

Responsibility for policy

The general manager, operations manager, information technology manager and store ICT supervisors and administration staff have the responsibility for updating, disseminating and reviewing the policy. All managers have a duty of care to ensure the policy aims and strategies are implemented. All employees have a responsibility to abide by legislation and policy initiatives.

Records management

Mail management

Every employee is responsible for ensuring records that they generate and/or receive are properly captured onto official record-keeping systems.

All mail which is received (whether from within or outside the organisation), or which is sent (to an addressee within or outside the organisation), which records Kingfisher business, must be recorded and placed in the relevant organisational file.

Classification and file taxonomy

To ensure official records of Kingfisher Garden Centre are adequately managed and retrievable, all records are to be classified and placed in appropriate files titled in accordance with the corporate taxonomy. This will assist in the overall management of the records from the time of creation through their active life and to their final disposition.

Files and file creation

All official records of the organisation must be placed on official files. Employees may continue to use working files. However, no original Kingfisher records are to be placed on those working files.

Employees are not to place original records on personal working files at any time.

Version control

Document history and version control are used to record details of minor and major amendments and reviews to all organisational documentation. It is one method of ensuring documentation meets legislative requirements and organisational quality standards.

- All policies, procedures, forms, records, documents, resources are to be version controlled.
- Version control is to include as a minimum the version number, the month and year in the footer of a document.

- Policies, procedures and documents classified as confidential or restricted must include a version control history at the front of the document that outlines reasons for modifications.
- Employees are to use the most recent version available wherever possible.

Electronic records management

Employees are encouraged to generate and disseminate information in electronic formats to improve productivity and facilitate timely communication. Such electronic records form part of Kingfisher's records and will be subject to the same conditions as any other record format. Therefore, they must be managed and integrated into the record-keeping systems just as other record formats are.

All electronic record-keeping and storage systems should mimic the paper-based systems with directory structures that resemble the classification system.

Observance of confidentiality and privacy principles

All records created by an employee in the course of their duties must be managed in accordance with National Privacy Principles (NPP) and the organisation's privacy policy. Such records must not be divulged or released to unauthorised persons without authorisation from the employee's supervisor, direct manager or the human resources manager.

Employees are required to use discretion in regard to the release of information as such records may contain confidential information, for example, internal contact information or telephone numbers that are not normally publicly available. If in doubt, employees must consult their supervisor, direct manager or the office manager.

The office manager must be consulted in relation to the handling of sensitive information that may have institutional impact.

Administrative and corporate records

Administrative systems and/or corporate applications used by the organisation, for example, human resources information systems, risk management information systems and financial information systems, contain data that is required to be retained for evidentiary purposes.

The data contained in these systems are to be managed in a way that will ensure integrity of the records and enable access to these records in their original format as created for the period as required and set by approved disposal authorities.

Intentional and unauthorised destruction or erasure of data, or its corruption by alteration, insertion or deletion of information, or any other form of unauthorised alteration that impairs the usefulness or effectiveness of the data as a significant, legal or corporate record, is not permitted.

Software and hardware

Electronic records must be accessible at all times and the necessary software and hardware required to access electronic records must also be maintained. When electronic records are migrated to other systems the integrity of the record must be preserved.

Legal records

Legal records include agreements, contracts, memorandum of understanding, legal certificates, deeds and licences. Legal records are considered vital records to the organisation for the period of the title, licence, agreement or contract and a short period thereafter. Therefore the records must be protected and secured to ensure they are not lost, modified or damaged in any way, or accessed by unauthorised persons.

Employee records

Employee files must be maintained entirely by the Human Resources (HR) Department. All original records must be sent direct to HR for normal processing, registration and attachment to official employee files.

Employee files are confidential and duplicate employee files are not to be created within departments, work sectors or offices. Where employee files do exist in other internal filing systems, the records should only be duplicates of forms (such as leave forms) and they must not contain any personal information about employees. There must also be adequate security of these files to ensure no unauthorised usage.

Records storage

Records must be stored in conditions that ensure that they are readily accessible and retrievable for the length of time they are retained.

- Records should be stored in conditions that take into account their physical characteristics, sensitivity, retention period and expected access rate.
- The physical environment should be clean and free from dust.
- Records should never be exposed to direct sunlight and should be kept away from other sources of direct light and heat as much as possible.
- The physical area must be free from insects and rodents.
- There should be a minimal risk of damage from natural disaster such as fire, water and mould.
- It should be possible to retrieve records accurately and in a time period appropriate to the urgency of the retrieval request.
- Adequate security must be provided to protect confidential or restricted information. All official records must be stored in such a way as to minimise the potential for unauthorised access.

All record storage facilities used by the organisation must comply with Kingfisher Workplace Health and Safety policies as well as associated legislation.

Retention of records

Records cannot be disposed of prior to the expiration of the appropriate retention period. However, there is no requirement for organisational records to be destroyed as soon as the minimum retention period expires.

Retention and expiration dates are based on the *Australian Records Retention Manual* (2011 edition) and legislation specific to the state or territory the business unit is operating in.

Record retention periods

- Audit – retain for 7 years
- Monitoring and control documents (e.g., inventory, financial) – retain for at least 10 years
- Acquisition of assets (including contracts, purchase arrangements) – retain permanently
- Policies and procedures – retain for 10 years after they have been superseded
- Reports (including statistical and financial) – retain for 10 years
- Routine correspondence – retain for 2 years

Archiving of records

Records that should be archived have been appraised as having continuing value, but are no longer required for current use and so have been selected for preservation. This may be permanent preservation or for a specific period of time to meet legislative requirements or as specified in section *7.12 Retention of records*. This process should be undertaken at least on a yearly basis.

- Only inactive records should be archived.
- Records must be evaluated prior to archiving to determine ongoing value to the organisation.
- Electronic records to be archived should be stored in an appropriately designated archive file within the relevant information management system.
- Paper-based records must be placed in archive storage boxes and labelled with contents, time period the records relate to, destruction date (if applicable) and any specific details that aid record recovery at a later date.
- Each department must keep an Archive Inventory Record for both electronic and paper-based records outlining details of all archived records, including their location and box number (for paper-based records).

Disposal of records

A list of records due for destruction must be created and approved by the office manager before any records are destroyed. Records must be destroyed adequately so that they may not be recreated in any form, and confidentiality of the records must be maintained throughout the destruction process.

Records that are ready to be disposed of must go through the following procedures.

- The department or general manager of the area responsible for the records must approve and 'sign-off' on the destruction.
- The office manager must approve and oversee the destruction.
- Electronic records must be destroyed in a way that they are not recoverable once the destruction has taken place, such as data shredding.
- Hard-copy records must be destroyed internally by shredding or through an approved contractor by pulping, shredding or incineration.

Information management

Creation and use of information

Information in an employee's care, such as documents, records, data and information assets, must be managed appropriately.

- Any information that is classed as a record must follow the record-keeping requirements in Section 5 of this policy. This includes any object that provides evidence of a business decision, transaction or activity or is received in the course of business.
- When preparing information for publication (whether print or online, for public or internal websites), ensure that Kingfisher Garden Centre owns the copyright or, where applicable, has obtained specific consent of the copyright owner for publication.
- When creating documents, include metadata such as date of creation, status, version, purpose and contact, including business unit if appropriate, to assist in any future retrieval and release of information.
- Within emails add a signature block (e.g., name, position, business unit or region, contact phone number) using the layout defined in the Kingfisher Administrative Policy.

Management of information assets

Information owners and custodians must develop and implement processes to manage information assets through their life cycle, including adherence to intellectual property, right to information and all other legislative and regulatory obligations, including the following.

- Identifying the information security classification of the information asset to apply controls to manage, store, process or transmit the information assets.
- Providing access to information to employees based on sensitivity due to legislative, policy, standards, commercial or privacy reasons.
- Processing, transferring or releasing information assets according to the handling practices listed in Sections 5 and 7 of this policy.
- Maintaining created records in an authorised record-keeping system, where appropriate.
- Incorporating a metadata scheme where the information asset is an ICT business system.
- Making sure any intellectual property, including copyright, is appropriately identified and labelled.
- Reviewing the information asset annually, whether available publicly or internal, to ensure it is relevant, accurate and that the quality and integrity is being maintained.
- Storing and maintaining information assets, including archiving and the undertaking of integrity checks of data, to ensure data has not been modified without authorisation or accidentally corrupted.
- Reviewing and updating business continuity and disaster recovery plans regularly to reflect current processes and contacts, and to ensure required equipment is readily available.

Security of information and records

Security levels

All new files must establish the relevant security level of that file at the time of creation. A clear identification of who can and cannot have access to the file must be provided with the application for a new file. Any and all requests for restricted access or confidential files must be checked for authorisation and if a person making the request is not listed as authorised, access must not be given.

Kingfisher security levels are:

- **Public:** Information authorised to be made publicly available, or able to be released to the public.
- **Non-confidential:** Non-sensitive information that is created or received within Kingfisher, is used internally, and comprises the bulk of the information used within the organisation.

- **Confidential:** Sensitive and confidential information that is created or received within Kingfisher. Access must be restricted to authorised persons on a 'need to know' basis. If released inappropriately, it might cause limited damage to the organisation or other individuals.
- **Restricted access:** Very sensitive and confidential information where unauthorised and/or premature disclosure might cause damage to one or more parties.

Electronic records must be protected from unauthorised access at all times. Access restrictions created for hard-copy records also apply to electronic records.

Management of information security

When managing this information, employees that create, process or handle information must:

- ensure that electronic documents that have been classified confidential or restricted have their information security classification clearly displayed on the front page as a watermark and in the header or footer
- ensure that any changes to the classification applied that results in a lowering of the information security classification will be made through a formal approval process that involves the author and/or information custodian
- ensure that classification applied to an information item will not be changed whilst that item is being transferred to another location or between ICT business systems
- ensure information classified as protected that is stored in mobile devices (e.g., CDs, DVDs, USB devices, hard drives, SD cards) is destroyed or not used for other purposes without being securely wiped or rendered unusable
- ensure that when using the information security classification it does not limit the legislation under which the department operates
- take reasonable precautions to protect information based on their information security classification against unauthorised access, illegal or unauthorised use, disclosure, modification, duplication, disruption and/or destruction.

Password security

Your Kingfisher information system password is the main way to protect access to your data. It is therefore important that you pick a good password. It needs to be hard for crackers to break, difficult to guess (especially if someone knows you) and changed periodically in case someone does get to know your password over time.

Your IT account password must:

- be at least eight characters long
- contain at least one upper-case letter and at least one lower-case letter
- contain at least one number or punctuation character
- include only characters supported on standard Kingfisher technology
- not be a dictionary word
- be changed every 12 months.

Backup of electronic information and knowledge

All electronic files kept in Kingfisher information and knowledge management systems must be backed up every night to an external hard drive.

It is the responsibility of each store's IT supervisor to complete backup processes. When the IT supervisor is absent from the workplace, responsibility for completing backup processes is delegated firstly to the finance manager and then the assistant store manager.

The backup must be clearly labelled with date and time of backup and retained for one week. All files stored on the external hard drive must be completely erased before the drive can be reused for backup processes.

Audit and review

All record systems may be subject to audit and review to ensure compliance with legislative requirements and with the requirement of this policy.

To accommodate changes in legislation, technologies, programs and resources available to Kingfisher this policy is to be reviewed on a biennial basis.