Career Seekers Direct Ltd

Data Retention and Records Management Policy

1 Introduction

This Policy forms part of a suite of policies and procedures that support an information governance framework.

A record is defined in the Records Management British Standard BS ISO 15489 as “Information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business”. All records created and held by CSD, both paper and digital, (including email and information held in databases) are subject to this policy.

Records are both evidence of business activity and information assets. They can be distinguished from other information assets by their role as evidence in the transaction of business and by their reliance on metadata. Metadata for records is used to indicate and preserve context and apply appropriate rules for managing records.

Managing records encompasses the following:

a) creating and capturing records to meet requirements for evidence of business activity;
b) taking appropriate action to protect their authenticity, reliability, integrity and useability as their business context and requirements for their management change over time.

Reference to "business activity" or “business activities” is interpreted broadly to mean those activities that support the purposes of the organization's existence. Functions, activities, transactions and work processes are representations of particular forms of “business activity”

Increasingly, records are made and kept in digital environments, offering a range of opportunities for new kinds of use and reuse. Digital environments also allow greater flexibility in the implementation of records controls, within and between systems that manage records.

Records are an important asset to CSD and they require appropriate management for effective and efficient administration, for the discharge of CSD’s responsibilities and business, and for compliance with legislative requirements. Good management of records also helps staff in the performance of their duties by improving access to and organisation of relevant records, removing out of date or superseded records from CSD systems and reducing duplication of documents and data.

There are also several pieces of legislation which impact on the way in which CSD manages and uses information. Non-compliance with this legislation may result in financial and reputational penalties.

2 Purpose

CSD records are defined as those documents or data sets which arise from or facilitate the business carried out by CSD and which provide evidence of its transactions or activities.

This Policy aims to ensure that CSD, creates, maintains, retains, uses and properly disposes of those records which it requires for the conduct of its business and that they are managed in a manner commensurate with legal obligations and information requirements. It aims to ensure that records are available as assets to CSD and are capable of reuse in appropriate contexts. CSD acknowledges the legislative environment within which it operates, particularly in the context of this Policy, those pieces of legislation, related codes of practice and standards listed in the control box below. These all have implications for the way in which they are expected to use and keep records and apply records management standards.

This will be achieved through the implementation of controls and responsibilities including measures to ensure, support and enable:

- the delivery of CSD business including assurance that external data sources are safeguarded though appropriate controls and audit.
- legislative compliance - compliance with record keeping provisions in current legislation such as the Freedom of Information Act, data protection legislation and the Environmental Information Regulations.
- lifecycle management – records must be kept for an appropriate length of time and in an appropriate manner. They must be securely disposed of at the end of their lifecycle in accordance with policies, procedures and best practice and in accordance with CSD's Records Retention schedule.
- confidentiality – CSD's records must be protected from unauthorised access.
- integrity – the accuracy and completeness of CSD's records must be safeguarded and unauthorised amendment or destruction prevented.
- availability – CSD records must be available to authorised users in line with business requirements
- efficiency – CSD records must be available to authorised users in a form that ensures efficiency and ease of use.
- authentication – the identity of the persons accessing highly restricted and critical systems which permit the creation, amendment or deletion of CSD records must be recorded and verifiable.
- semi-current manual records (records which are not in regular use, but which have not yet reached their disposal date) will be managed, where appropriate, through CSD's record storage facilities

3 Scope

This Policy applies to:

- all CSD records and information processing, received or used via email, Teams chats or any other method of communication;
- all members of staff, as well as individuals conducting work at or for CSD and those who have access to CSD information (**"staff"**). This includes temporary, visiting, casual, voluntary and agency workers and suppliers (this list is not intended to be exhaustive);and
- all locations from which CSD related information is accessed including non CSD HQ locations.

4 Responsibilities and compliance framework

CSD has a corporate responsibility to maintain records of processing and its records management systems in accordance with the regulatory environment. This responsibility therefore extends to all staff who work with CSD records.
CSD recommend sharing links to documents within emails where and when possible rather than using attachments. Personal accounts, email accounts and non-CSD email accounts must not be used for storing primary CSD records.
Any emails and documents which are important and need to be kept must be stored elsewhere in an appropriate filing system relevant to their confidentiality or criticality; this could include shared email role accounts or SharePoint 365 Online.
Access to email and OneDrive accounts will be removed when a member of staff leaves CSD, and this access will not be reconstituted except under exceptional and limited circumstances.

CSD CEO is responsible for ensuring that records management within CSD is carried out in line with this Policy and established procedures. The CEO is responsible for providing policies, procedures, guidance and advice in support of this Policy, for training staff where necessary and for managing CSD's records.

5 Monitoring compliance

The information records management system is subject to internal monitoring and auditing throughout CSD, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement.

Reports on the matters related to this Policy will be provided to the CSD Governance meetings.

6 Review of Policy

This Policy will be reviewed at least annually or when significant changes are required.

Version amendment history

Version	Date	Reason for change
1.0	January 2024	Creation and approval by the CEO & Chair of Governance

Document control box	
Policy title:	Records Management Policy
Date approved:	January 2024
Approved by	Governance Committee
Version:	1.0
Supersedes:	NA
Previous review dates:	NA
Next review date:	January 2025
Related policies:	Data Protection Policy Information Security Policy Acceptable Use Policy
Related procedures:	Records Retention Schedule
Policy owner:	CSD CEO