Dairy Australia

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

For internal Dairy Australia use and distribution only.

Once printed, this is an uncontrolled document.

Approved April 2023

Document Control

Version #	Reviewed By	Date	Endorsed By	Date	Approved By	Date	Summary of Change
01	IT Manager	Oct 2013	IT Manager	Oct 2013	IT Manager	Oct 2013	Original Policy
02	GM BOP	August 2020	ARMC	August 2020	Board	September 2020	Major update
03	GM BOP	April 2023	LT	April 23	MD	May 2023	• clarified that all data, not just email can be tracked and stored, • removed reference to mobile access requiring approval and clarify that it's subject to the MDM • Addition of point to confirm transfer of unencrypted sensitive information is prohibited • Minor updates to several points to improve wording • Added clarification that HR is also responsible for monitoring training module
Document Steward							**IT Manager**
Document Owner							**General Manager, BOP**

Related Documents
IT Acceptable Use Procedure
IT Security Policy
IT Security Procedures
Code of Conduct
Social Media Policy
Social Media Procedure
Review Requirements
This document is next due for review in April 2024 by the General Manager BOP
Controlled Document Location
https://dairyaustralia.sharepoint.com/SitePages/documenthub.aspx

Contents

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

1 Purpose

The purpose of this policy is to articulate the principles for ensuring that Dairy Australia's information technology resources are used in a legal, ethical, secure and responsible manner.

2 Scope

This policy applies to all Dairy Australia employeesincluding fixed term, casual, Dairy Australia directors and contractors and all parties who access Dairy Australia's information technology infrastructure, hereinafter defined as 'users'.

This procedure must be read in conjunction with the *Information Technology Acceptable Use Procedure,* the *Information Technology Security Policy* and the *Information Technology Security Procedure.*

3 Policy Statement

Dairy Australia's Information Technology (IT) resources must be used in a lawful, ethical, secure and responsible manner, and in accordance with the IT Acceptable Use Procedures, IT Security Policy and Procedures, other applicable Dairy Australia policies, and any additional terms of use that may apply to particular software or services.

Dairy Australia provides IT resources to its staff and other authorised users, for the purpose of conducting activities in the normal course of business. Some reasonable non-commercial personal use is allowed, but as a privilege and not a right, and if that privilege is abused it will be treated as a breach of this Policy.

4 Policy Principals

- Users must not knowingly use or attempt to use Dairy Australia's IT resources for unlawful, offensive or otherwise improper activities including but not limited to:
    - harming (whether physically, financially or otherwise) another person or company
    - damaging another person's property or services, networks or facilities
    - contravening any law or regulation
    - placing Dairy Australia in contravention (or at risk of being in contravention) of any law or regulation
    - contacting a minor who is not known to the user, without the consent of that minor's parent or guardian

- enabling a minor to obtain access to inappropriate material
- harassing, menacing or stalking any person
- unlawfully discriminating against any person
- unlawfully vilifying any person
- storing, publishing or disseminating any obscene material (including child pornography)
- publishing or disseminating any defamatory material
- infringing any person's legal rights, including rights relating to intellectual property, fair trading, confidential information and trade secrets
- contravening any law relating to privacy
- engaging in the practice known as 'spamming' or altering the contents of an electronic message for the purpose of hiding, obscuring or deleting the source of the message or making the message appear to come from someone other than you
- creating or knowingly disseminating any virus, trojan, worm, cancelbot, time bomb, hacking tool, or other harmful component
- granting any person unauthorized access to or control over any service, network, facility or equipment
- engaging in a denial of service attack or the practice known as 'flooding', or
- defeating any security measure or usage limit imposed by Dairy Australia.

- Users must not in any way divulge, copy, release, sell, loan, alter or destroy any sensitive information without approval from the relevant General Manager.
- IT resources are provided for use in business activities. Some reasonable non-commercial personal use may be allowed, but as a privilege and not a right, and if that privilege is abused it will be treated as a breach of this Policy.
- Dairy Australia may, at any time and without prior notice monitor activity on Dairy Australia's IT systems. Users should also ensure that they alert the IT Manager if they become aware of any misuse of Dairy Australia's IT systems. In addition, data stored, transferred or email sent and received using Dairy Australia IT systems will be subject to tracking or long-term storage (e.g. Legal hold or Journaling).
- Information stored on IT facilities, whether owned or operated by Dairy Australia, remains the sole property of Dairy Australia.
- Accounts for use on Dairy Australia IT systems will be created as required and depending on the required use may require additional approvals or justification before they are created in accordance with the IT Security Policy and IT Security Procedure.
- Users must take all reasonable steps to protect their Dairy Australia issued account from unauthorised use including but not limited to not reusing passwords, writing them down, sending them via email, storing them in plain text or sharing logon details with other people.
- Users must never share logon details (username and or passwords) with anyone including co-workers.
- Accounts may be suspended if it is suspected that the account is compromised, or if the account is unused for an extended period of time. Users and managers are responsible for ensuring the IT department are notified when staff leave. The IT department will also perform reviews and suspend inactive accounts on a regular basis.

- Where a higher level of access is required to a system to perform administrative functions a separate Administration account will be provided to relevant staff. These administrative accounts must not be used for day to day activities under any circumstances.
- All access to Dairy Australia systems from mobile (phone & tablet) devices will be subject to management via the Dairy Australia Mobile Device Management (MDM) system.
- Users must take all steps necessary to keep IT devices secure including not leaving devices in a visible location, whether that be an office, car or elsewhere, or overnight in a locked car.
- Users must comply with the Delegation of Authority in relation to procurement of IT hardware, software, and/or IT services being approved by the IT Manager which includes signing up for unauthorised or non-approved software-as-a-service (SaaS) or cloud based solutions.
- Users must make every effort to ensure they do not knowingly or unknowingly compromise the security of the Dairy Australia IT systems, or introduce security threats to the Dairy Australia IT systems by ensuring they are familiar with the IT Cyber Security guidelines (published on the IT support page on DairyHub).
- Users must ensure that their device (computer, mobile, etc.) screens are locked when they are left unattended. In addition, Dairy Australia will where appropriate implement policies on devices to enforce these requirements.
- Repeated loss or damage of devices may result in users being required to fund repairs or replacement devices.
- Users must not install any software whether licensed, free or otherwise on Dairy Australia's devices without IT approval, nor circumvent the IT security measures that prevent staff from doing so
- Users must ensure that all data is stored and shared using only systems, approved and provided by Dairy Australia. Storage of Dairy Australia data on non-Dairy Australia devices, or non-approved cloud storage services is prohibited without prior approval from the IT Manager.
- Sharing of sensitive data via unencrypted email or other unencrypted transfer methods is prohibited.
- Users must not send Dairy Australia data to their own, or other users' personal email addresses
- Users working with media, social media and blogs must comply with Dairy Australia's *Media* and *Social Media Policies* and *Procedures*
- Dairy Australia reserves the right to record, delete, block, quarantine, copy, use and take possession of all communications or data passing through IT facilities and pass on the information to external organisations where legally obliged to do so or in cases of possible breach of Dairy Australia's policies or procedures.
- Users are expected to report actual or suspected breaches of this Policy or other security incidents that may be a threat to the security of Dairy Australia IT to the relevant Manager, General Manager or to the IT Manager as soon as they become aware and in a timely manner
- At any time, Dairy Australia may implement technology controls to audit, log or block activity that contravenes this policy.

5 Roles and Responsibilities

The table below documents the responsibilities of all roles involved in the acceptable use of IT resources.

Role	Responsibilities
Dairy Australia information technology users	• Are responsible for all activities originating from accounts and devices provide by Dairy Australia • Use Dairy Australia's IT resources in accordance with this Policy including appropriately securing any IT accounts and devices provided to prevent unauthorised use, theft, or loss. • Report any activities considered likely to breach this Policy or compromise sensitive information to the relevant Manager, General Manager or to the IT Manager.
IT Manager	• Implement appropriate information security controls and processes
Managing Director / General Managers / Regional Managers	• Ensure the IT Acceptable Use Policy and Procedure are implemented within area of control • Ensure appropriate action is taken when the IT Acceptable Use Policy and Procedure are breached
Contract Owners	Any agreement where a third party requires the following access must include references to the third party adhering to the Dairy Australia IT Acceptable Use Policy, IT Acceptable Use Procedure, IT Security policy, and IT Security Procedure: • creation of accounts (user or administrative), or use of Service Accounts that are hosted within a system managed by Dairy Australia • access to the Dairy Australia IT network (wired, wireless, remote access or any other means of access) • access to any Dairy Australia systems (cloud, hosted or otherwise) for the purposes of performing administrative, configuration or development work • access to documents shared by Dairy Australia using approved sharing methods is not applicable – refer to the IT Acceptable Usage Policy and Procedure for information on approved sharing methods The Agreement must state that any third-party supplier not complying with these policies could have actions taken against them including but not limited to termination of contract.
Human Resources	• Provide training to all employees and contractors to raise awareness and understanding of the IT Acceptable Use Policy and Procedures • Ensure all employees and contractors review and acknowledge the IT Acceptable Use policy and procedure and undertake the IT security training online module on an annual basis • Provide reports to the GM BOP on training completion rates

6 Compliance and Assurance

- The GM BOP must ensure appropriate monitoring compliance processes are in place for this Policy

- Breaches of this Policy should be recorded as an incident

7 Review

In line with Dairy Australia's Policy Governance Policy, this policy is scheduled for review every two years or more frequently if appropriate.