Information Technology Acceptable Usage Policy

Policy Control		Document Reference	POL-ICT-0002
Owner	ICT	**Revision Number**	2.0
Date Reviewed	23/03/2017	**Review Period**	12 Month(s)
Next Review Date	23/03/2018	**Applies To**	All LiveBetter

1. Purpose

The purpose of this policy is to:

a) Protect LiveBetter from damage of liability arising from the use of its information technology resources contrary to the acceptable uses outlined in this policy
b) To ensure that all persons who use LiveBetter's information technology resources are aware of information security threats and concerns
c) To reduce the risk of theft, fraud, and misuse of information

2. Scope

This policy applies to all users of LiveBetter's information technology resources including staff, volunteers, and third-party contractors.

This policy is governed by the Information Security Policy. This policy forms part of LiveBetter's Information Security Management Framework which outlines LiveBetter's approach to managing information security.

3. Controlled Document Definitions

Term	Definition
Policy	A "Policy" document outlines principles, rules and guidelines formulated or adopted by the organisation.
Procedure	A "Procedure" document determines all major decisions, actions and defines high level activities that are required to take place within set boundaries.
Instruction	An "Instruction" document provides step by step instructions on how to complete a task or activity. The document can be a stand-alone document or may relate to a procedure and / or a policy.
Form	A formatted document (electronic or paper) containing blank fields that users can fill in with data/information. Completed forms become records.

4. Definitions

Term	Definition
Android	Android is a smart mobile phone and tablet operating system
Aspire	A helpdesk ticket and request tracking system used by Diamond IT
Broadcast Email	A broadcast email is an email sent to many recipients.
Chain Letter Email	A chain letter email consists of a message that attempts to convince the recipient to forward the email onto many recipients.
CIMS	CareWest Incident Management System – A subsystem of NetSuite that allows users to submit incidents via a publicly accessible form available via the links section of the LiveBetter Intranet. Incidents can then be managed via NetSuite.
Commercially Confidential Information	Commercially confidential information is any information pertaining to the business activities of LiveBetter and its subsidiaries that is not publicly available, or that a reasonable person would assume to be not publicly available, or any information that has a value that would be, or could

	reasonably expected to be, destroyed or diminished if disclosed. Examples of commercially confidential information include sales data, plans and strategies, finances, and product launch information.
Computer Surveillance	Surveillance by means of software or other equipment that monitors and/or records information input or output, or other use, of LiveBetter's information technology resources, including but not limited to the sending and receiving of emails and accessing of websites
Control	A control is a means of managing risk to information assets, and can be of administrative, technical, or management nature.
Data at Rest	Data at rest is a term used to describe inactive data stored physically in databases, data files, spreadsheets, archives, backup tapes etc.
Data Breach	A data breach is a compromise of information security that leads to the loss or unauthorised access, use, modification, disclosure, or other misuse of sensitive information.
Denial of Service Attack	A Denial of Service attack is an attempt to make a computer or network resource unavailable to its intended users.
Electronic Document	An electronic document contains information that requires an endpoint device to display it. Examples of electronic documents include Word documents, Excel Spreadsheets, PDFs.
Endpoint Device	Examples of endpoint devices include workstations, and portable devices such as laptops, smartphones, tablet computers, e-readers, removable hard drives, portable gaming devices, netbooks, USB flash disks, and any mobile device capable of storing LiveBetter's information and connecting to a network.
E-Learning	An E-Learning module is an online learning program used to ensure employees understand their responsibilities. LiveBetter staff access these online training modules through OLLIE (Online LiveBetter Learning & Interactive Engagement).
Email	Messages distributed by electronic means from one user to one or more recipients via either the internet or the LiveBetter internal network.
External Third Party	An external third party is a person, group or organisation that is not LiveBetter or a LiveBetter employee.
Inappropriate Material	Inappropriate material is a term used to refer to pornography, pornographic jokes or stories, videos or messages containing offensive comments about race, gender, age, sexual orientation, religious or political beliefs, or disability. It is not appropriate for this material to be present in a workplace.
Information Obfuscation	Information obfuscation is the concealment of sensitive information by making the information ambiguous, resulting in non-sensitive information.
Information Security	Information security is the preservation of confidentiality, integrity, and availability of information.
Information Security Event	An information security event is a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
Information Security Incident	An information security incident is an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security.
Information System	An information system is a system that stores, transfers, and processes information assets, such as operating systems, infrastructure, business applications, off-the-shelf applications, and user-developed applications.

Instant Messaging	A message sent via the internet that appears on the recipient's screen as soon as it is transmitted
iOS	iOS is a smart mobile phone and tablet operating system used by Apple smartphones and tablets.
Jailbreak	Modify a smartphone or other electronic device to remove restrictions imposed by the manufacturer or administrator, e.g. to allow the installation of unauthorized software.
JIRA	JIRA is the automated issue tracking system used by LiveBetter ICT.
Malicious Code	Malicious code, or 'malware', is a term used to describe any code in any software or script that is intended to cause undesired effects, information security breaches, or damage to information systems. Malicious code describes a broad category of system security terms that include viruses, worms, and Trojan horses
Managed IT Service Provider	An external organisation providing IT services including but not limited to support, infrastructure setup, and network maintenance. At present Diamond IT is contracted to provide this service for LiveBetter.
Network	LiveBetter's network includes all LiveBetter information technology resources which are used by users inside and outside working hours, in the workplace of LiveBetter or a related corporation, or at any other place whether or not performing work for LiveBetter. It includes but is not limited to personal computers, workstations, smartphones and tablets.
OneDrive	OneDrive is a file hosting service offered by Microsoft that allows users to sync files and later access them from a web browser or mobile device. LiveBetter includes access to a corporate OneDrive account as part of our Office 365 subscription.
Packet Sniffing	The recording of all network packets that travel past a given network interface, on a given computer, on a network. This allows an individual to extract sensitive information such as credentials from unencrypted transmissions.
Personal Information	Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable: a) Whether the information or opinion is true or not; and b) Whether the information or opinion is recorded in a material form or not. Examples of personal information include government issued identifiers such as driver's license and tax file number, non-permanent information like a customer's postal address or mobile number, and permanent information like a customer's full name or date of birth.
Phishing email	An unsolicited email designed to trick users into clicking on links, or to trick users into opening email attachments. The goal of this email is usually to steal personal information from the user, or to install malware on the user's computer.
Remote Access Services	Remote Access Services refers to the combination of hardware and software to enable remote access to information systems such as intranet and internet proxy access, Windows Remote Desktop access, Outlook Web Access, and Network File Share Access.
Removable Storage Media	Examples of removable storage media include USB flash drives, removable hard drives, CDs, DVDs, and printed media.
Rooted Operating System	An operating system that has been compromised through the use of scripts or exploitation of known vulnerabilities to gain root (unlimited

	access) or superuser rights. This is generally to bypass device controls or manipulate software on the device which would otherwise be prevented.
Secure Document Bin	A special ‘wheelie bin’ identified by its lockable red lid with an opening slit and specific labeling that identifies that it is for the disposal of sensitive documents.
Sensitive Information	Sensitive information is information that must be protected because it might cause perceivable damage to someone or something if revealed to persons not entitled to be in possession of this information. This includes personal information, commercially confidential information, and Payment Card Industry account data.
Skype for Business	Skype for Business is a communication and collaboration application. It allows instant messaging, video conferencing, and screen and application sharing.
Smartphone	A smartphone is a mobile phone offering advanced functionality such as applications for interacting with information systems and removable media storage.
Social Media	Websites and applications that enable users to create and share content or to participate in social networking
Spear Phishing email	A more specific version of a phishing email (see *Phishing email* definition) whereby the email is crafted using your personal details and appears to be from an individual or business that you know.
Tablet	A tablet computer is a slate or tablet shaped portable computer, equipped with a touchscreen or stylus. Examples of tablets include Surface Pros, or iPads.
Tunnelling	The use of a protocol that allows the secure and private transmission of data between two parties. Such transmission prevents monitoring of the data between the two points, and thus can be used to circumvent monitoring systems that attempt to determine the content of data being transmitted, particularly between internal and external party.
User Account	A user account defines the actions a user can perform in an information system, such as an operating system or business application.
Users	Users are people that interact with an information system or endpoint device, and can be employees, contractors, and third-party suppliers.
Virtual Private Network	A virtual private network (VPN) is a network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or travelling users access to a central organisational network. LiveBetter’s VPNs require remote users of the network to be authenticated and secure data with encryption technologies to prevent disclosure of confidential information to unauthorised parties.
Workstation	A workstation is a general-purpose computer with a higher performance level than a personal computer (PC). For the purposes of this document, the term workstation also refers to other portable devices such as laptops and tablet computers.
Work Area	A work area is a term used to describe the area surrounding a workstation. Generally, if a user leaves a work area they will no longer be able to see their workstation, and should first lock it.

5. Statement of Principles

IT resources are provided to staff to conduct activities on behalf of LiveBetter. Users must take responsibility for using such resources in an ethical, secure and legal manner; having regard for the objectives of LiveBetter and the privacy, rights and sensitivities of other people.

6. Roles and Responsibilities

This policy applies to all users of LiveBetter's information technology resources including staff, volunteers, and third-party contractors.

6.1. Departmental Managers

Departmental managers shall be responsible for ensuring secure document bins used by their departments remain locked at all times.

6.2. Chief Information Officer

The CIO is responsible for:

a) Ensuring employees are made aware of relevant new information security vulnerabilities
b) Assisting in the development and review of associated E-Learning modules
c) Investigating breaches to this policy
d) Approving exceptions to this policy

6.3. Human Resources Team

The Human Resources Team shall be responsible for ensuring that:

a) Contractors who are to access LiveBetter ICT systems are provided with a copy of this policy as part of their induction
b) New employees are provided with a hardcopy of this policy, or directed to access a softcopy, as part of their induction
c) New employees complete the E-Learning modules based on this policy within 3 months of commencement
d) All employees annually complete E-Learning modules based on this policy

6.4. Managed IT Service Provider

The Managed IT Service Provider shall be responsible for:

a) Managing the scanning of web traffic and inbound emails
b) Ensuring that backup media is strictly controlled when in the custody of technicians

6.5. LiveBetter ICT

LiveBetter ICT shall be responsible for:

a) Ensuring the destruction of all sensitive information contained within system components prior to disposal
b) Reviewing the encryption of portable endpoint devices
c) Ensuring that sensitive information is removed from endpoint devices including smartphones before their disposal or reissue
d) Managing the purchase, setup and ongoing maintenance of all information technology devices.

7. Key Risk Management Process

Information security affects all employees of LiveBetter and is essential for the continued success of LiveBetter. This policy is intended as a statement of shared responsibilities for all management and employees and as such, all employees must be familiar with the contents and the application to their area of work.

7.1. Monitoring

LiveBetter reserves the right to monitor, record, inspect, audit and investigate any use of LiveBetter's information systems, software, files, devices, infrastructure and telecommunications by any individual. This includes, but is not limited to, smartphone, email, internet and instant messaging usage.

7.2. Incident Investigation

Emails and instant messages, may be inspected for sensitive information, inappropriate material, and malicious software, both during transmission and when stored in email accounts. An individual user's email account, instant messaging conversations, voicemails, and endpoint device geo-location may be accessed by LiveBetter ICT or authorised third parties after authorisation in writing by the CEO, General Manager People and Culture, or the relevant Executive Manager.

The CIO is empowered to initiate an investigation into suspected information security incidents and shall advise the General Manager People and Culture of any incident where an employee's conduct is reasonably suspected to be fraudulent, corrupt, or otherwise unlawful. Any investigation where disciplinary action is recommended, such action will be taken in accordance with the relevant human resources policies.

7.3. Education and Training

All users shall be provided with a copy of this policy and undertake the associated E-Learning module(s) to ensure that all employees are aware of their responsibilities in regards to information technology systems, security, threats, and concerns. This training will cover areas such as:

a) Acceptable usage of information technology
b) Reporting information security incidents and data breaches
c) Phishing, spear phishing, and social engineering attack awareness

7.3.1. Existing Employee Training

As part of the annual training refreshers, all users shall undertake E-Learning module(s) based on this policy.

7.3.2. E-Learning Completion Reporting

The HR Team shall generate E-Learning completion reports through OLLIE as per their training scheduling and follow-up process, to ensure Acceptable Usage training is undertaken.

7.3.3. Employee Awareness of New Information Security Vulnerabilities

The CIO shall ensure that employees are made aware of relevant new information security vulnerabilities.

8. Employee Responsibilities

Each user of LiveBetter information technology resources is responsible for upholding the principles of information security to preserve the integrity, confidentiality and availability of information, and must abide by the following rules.

8.1. Prohibited Information Systems Usage

It is strictly prohibited to:

a) Download, upload, and/or display pornographic or other inappropriate material on any LiveBetter endpoint device or network
b) Use LiveBetter's infrastructure to breach and/or disrupt external party network communications and operations, for example by Denial of Service attacks
c) Use LiveBetter's information systems or supporting infrastructure to collect data in an unauthorised manner, for example by packet sniffing
d) Install or use tunnelling or circumventing software with the direct or indirect result of avoiding security controls and restrictions

8.2. Phishing Email Awareness

'Phishing emails' are designed to trick users into clicking on links, or to trick users into opening email attachments. The goal of these emails is usually to steal personal information from the user, or to install malware on the user's computer, which can then be used as a beachhead to conduct further attacks on the organisation.

While LiveBetter employs up-to-date antimalware software and email filters, new versions of malware may not be recognised, and may not be blocked.

For this reason, it is extremely important that employees remain aware of the dangers of phishing emails, and exercise consideration before clicking on links in emails, or opening email attachments if the email is unsolicited and from an unknown sender.

Employees should forward phishing emails to Support@diamondgroup.net.au with a comment of "*please investigate suspicious email*".

8.3. Password Management

User account passwords are the primary defence and security for user accounts.

8.3.1. User Accounts

Individual user accounts exist to ensure non-repudiation – simply put, the ability to identify who undertook an action.

For this reason, it is prohibited to:

a) Tell anyone your user account password
b) Attempt to use another user's account to access information or information systems
c) Allow anyone to use your user account on a workstation that you are logged into
d) Leave your work area without first locking your workstation

8.3.2. Shared (House) Accounts

In some residences and departments, shared (house) accounts have been created to allow for a single user profile that can be used to access shared email. This user is an extremely low privileged account, with no access to any sensitive information system. This account may only be shared and used by approved staff at the residence, and should never be provided to customers or the public.

For this reason, it is prohibited to:

a) Tell anyone your account username/password who is not authorised to use this login
b) Allow anyone not authorised to use this account to use the workstation while it is logged into this account
c) Leave your work area without first locking your workstation

8.3.3. Account Passwords

Your user account passwords are used to ensure that only you can access your user account, and must be kept secret.

For this reason, it is prohibited to:

a) Write down a user account password
b) Record a user account password in an electronic document

8.3.4. Account Password Selection

User account passwords must contain three of the following four elements:

a) Lowercase letters
b) Uppercase letters
c) Special characters
d) Numbers

Passwords must be at least 8 characters in length

Passwords should not contain parts of your username or commonly used words.

When you update your password a verification check will run to ensure your password complies with the complexity requirements.

LiveBetter ICT may increase the complexity requirement as required by the organisation's information security needs.

Password Generation Example

The following table demonstrates how a strong password can be created and remembered

Step	Instruction	Example
1	Start with a sentence – think of something meaningful to you.	Fridays are my favourite day (This is my starting sentence)
2	Turn your sentence into a row of letters, by using the first letter of each word.	famfd (Fridays are my favourite day)
3	Add complexity by making one of the letters uppercase.	Famfd (I have made 'F' uppercase)
4	Add length with numbers, by adding a number that is meaningful to you.	Famfd10 (10 is my lucky number)
5	Add length with punctuation, such as adding a special character.	Famfd10! (and this is my 8 character password)

8.3.5. Forgotten Account Passwords

It is important to verify the identity of employees who are requesting a user account password reset. This verification is used to stop imposters attempting to reset passwords of user accounts to gain access to LiveBetter systems, by pretending they have forgotten their password.

For this reason, in the event that an employee has forgotten their user account password, they should contact Diamond IT on (02) 4944 2444 and request a password reset. The Diamond IT helpdesk will verify the user based on shared unique identifiers, for example an employee ID. The Diamond IT helpdesk will then set a temporary password which the user can change when they next log on.

If an employee is unable to verify themselves to Diamond IT, they will need to contact their line manager or the HR Team who can verify them based on additional information and make the request to Diamond IT on their behalf.

8.3.6. Information System Passwords

Where possible, information systems will be configured to use the same user account password as email and computer logons, however in some cases additional passwords may be required. These passwords should never be written down, as they may provide access to highly sensitive information. If an employee wishes to record these passwords somewhere so they are not forgotten, they may do so in a secure Password Management application, which can be obtained by contacting LiveBetter ICT.

8.4. Email Usage

The following rules govern acceptable usage at LiveBetter

8.4.1. Personal Email Usage

The sending and receiving of personal emails from LiveBetter’s email accounts is acceptable, providing the use is not prohibited (see prohibited email usage) and that the use is not excessive in that it does not adversely affect, or could reasonably be expected to adversely affect the performance of the user’s duties.

Access to personal email accounts, such as Gmail or Hotmail, is strictly prohibited on LiveBetter’s internal networks.

8.4.2. Prohibited Email Usage

It is prohibited to:

a) Send or forward emails which contain pornography or other inappropriate material
b) Send emails containing sensitive information to non-LiveBetter email accounts outside of those emails required to be sent as part of business functions
c) Send emails containing sensitive information to your personal non-LiveBetter email account
d) Configure automatic forwarding of LiveBetter emails to non-LiveBetter email accounts
e) Forward chain letter emails
f) Send or forward emails for personal monetary gain or for commercial purposes not directly related to LiveBetter’s business

g) Send or forward copies of electronic works in violation of copyright or other general laws or contractual obligations
h) Send unsolicited mass distribution emails
i) Disseminate personal contact information of LiveBetter employees without their prior consent
j) Any purpose that is restricted by LiveBetter's policies, and/or any applicable State and/or Federal regulations or laws

8.4.3. Email Broadcasts

Emails sent to multiple departments or branches must:

a) Be relevant to the majority of the recipients and provide information about LiveBetter's issues, policies, procedures, or decisions; AND
b) Have a degree of urgency, to the extent that the message should be drawn to the attention of relevant employees prior to a specified time.

If the information contained in the email is based on policy, procedure or is an important announcement, employees must ensure that the information is also added to the intranet by contacting your team's supervisor or administration assistant.

Broadcasting information that does not satisfy the above conditions should be done via the intranet by contacting your team's supervisor or administration assistant.

8.4.4. Quarantined Emails

Emails sent to LiveBetter email accounts are automatically scanned for phishing, spam and viruses, and if detected they are blocked and placed in quarantine.

The recipient shall receive an email containing basic details of the quarantined item, and depending on the case for the quarantine they may have the option to release it. Emails containing viruses cannot be released.

If a user believes an email has been incorrectly quarantined, they can log a support ticket with Diamond IT to have the item reviewed.

8.5. Internet Acceptable Usage

Occasional and reasonable personal internet usage is acceptable, providing use is not excessive and it does not adversely affect, or could reasonably be expected to adversely affect, the performance of the user's own duties, or the duties of others, or the performance of LiveBetter's information systems. Reasonable usage is considered as browsing websites and similar activities that do not require large and/or continuous data transmission sessions.

Downloading or uploading large files such as videos, streaming radio stations or other media, or playing online games is not considered reasonable internet usage. Where there is a business purpose for access such content, a request can be made to the CIO for such access to be provided to specific staff. This may involve consideration of alternative means of access to the content and/or restricted access times, so as to minimise impact on other staff and LiveBetter's information systems.

LiveBetter reserves the right to restrict access to any external website or internet resource that it deems inappropriate for use by staff. LiveBetter may use time-of-day- based restrictions on access to sites based on the inherent impact accessing these sites within working hours may have on the performance of LiveBetter's information systems.

Where websites and internet usage involving large files such as videos and interactive content are used for delivery of corporate content and training, such as E-Learning websites, these will not have any access restrictions imposed on staff. Such sites will be approved by the appropriate executive manager.

Social Media usage is governed by the Social Media Policy. In the event that material is posted by staff on social media sites, LiveBetter reserves the right to request the removal of posted content where the content is deemed inappropriate.

8.5.1. Prohibited Internet Usage

It is prohibited to:

a) Download or upload pornography or other inappropriate material
b) Upload sensitive information to websites outside of those required to be sent as part of business functions
c) Download or upload copies of electronic works in violation of copyright or other general laws or contractual obligations
d) Any purpose that is restricted by LiveBetter's policies, and/or any applicable State and/or Federal regulations or laws

8.6. Profile Picture

A profile picture is great for matching names to faces and to help new employees familiarise themselves with other employees. It is encouraged that employees add a profile picture to their profile in Office 365 and JIRA. Profile pictures must be of the employee themselves, and be of a professional nature. Employees must not use inappropriate photos.

It is prohibited to use another user's personal photo for any non-business purpose without their expressed consent.

For details on how to set up your profile picture, please see the ICT Q&A on the LiveBetter Intranet.

8.7. Instant Messaging Acceptable Usage

Microsoft Skype for Business is an instant messaging application that allows employees to have instant communication. When using Skype for Business or any other application for instant messaging, employees are prohibited from:

a) Sharing files which contain pornography or other inappropriate material
b) Sharing copies of electronic works in violation of copyright or other general laws or contractual obligations
c) Streaming video containing inappropriate material

Where staff require the sharing of sensitive documents and information, this should be undertaken via either the Intranet or Microsoft OneDrive, with a link sent via instant messaging. This provide the ability to maintain a central copy of the information, and allows for the revocation of access once the document is no longer required by the other party.

8.8. Enterprise Social Networking Acceptable Usage

Yammer is an enterprise social networking service used by LiveBetter to allow staff to collaborate and engage other staff across the organisation. Staff must remember that anything shared on Yammer is potentially shared with the LiveBetter community, and as such should consider the following:

- Be polite: Remember you are having a conversation with other staff within LiveBetter
- Be aware: Confidential information must only be shared with those who are appropriate to know that information, preferably NOT within a collaborative network such as Yammer. If Yammer is used, we recommend using a private group whose members need to know that information for business purposes.
- Be smart: It is VERY easy to accidentally post information to the entire organisation, rather than a specified group!

Usage of Yammer is governed by the same standards as usage of Email and Instant Messaging within LiveBetter.

8.9. Endpoint Devices

Only LiveBetter ICT issued endpoint devices, including workstations, tablets and phones, may be connected to LiveBetter's internal network, with the exception of remote access and web based portals. Users accessing remote access or web based portals on a personal device should ensure that the device is running up-to-date antivirus software.

8.9.1. File Storage

If a workstation has a hardware failure, all information on the device could be lost. For this reason, employees should avoid saving important files to local hard drives on workstations. Instead, employees should save these files to LiveBetter's network drives or LiveBetter OneDrive (as per 8.11).

8.9.2. Power Saving

LiveBetter workstations must be powered on of a Monday night in order to receive important security updates for the operating system and applications, as well as up-to-date antimalware definitions. Workstations will automatically go into a power-saving mode overnight, thus there is no need for staff to explicitly power off workstations that are plugged into mains power.

Staff do not need to be logged into the device for this to occur, and should ensure that they are either logged out or the device is locked when not in use.

8.9.3. Purchasing and Procurement

All Information Technology equipment must be requested via LiveBetter ICT's standard request process. Any equipment purchased outside of this process will not be correctly configured for LiveBetter's network and will not be supported.

If peripheral devices such as keyboards and mice are required urgently, these devices may be purchased directly by employees with prior approval from LiveBetter ICT.

Equipment allocation will be as per the standard for each staff member's role and department. Any requests for IT equipment over and above the standard allocation must be made by the staff members' executive manager, with justification for the non-standard request.

8.9.4. Software

Software must not be installed on or removed from any LiveBetter workstation, including laptops, without authorisation from LiveBetter ICT. This also applies to windows and android tablets, due to the increased inherent risk with these devices being compromised by malware. Staff using devices with an iOS operating system are permitted to install apps from the Apple App Store.

8.10. Mobile Devices

Mobile devices, such as laptops, tablets and smartphones require additional security controls when compared to access from traditional stationary workstations, outlined below.

8.10.1. LiveBetter Smartphones/Tablets

LiveBetter issued smartphones shall be able to access email, calendar appointments, voicemail and instant messaging.

Employees with LiveBetter issued smartphones and tablets must regularly update the operating system to protect against security vulnerabilities. It is recommended that regular device backups should be completed by employees to ensure that, in the event the device is lost or stolen, content on the device is not lost. Staff are required to action all requests to update their device by LiveBetter ICT.

In order to protect sensitive information, all LiveBetter smartphones and tablets must lock after a period of inactivity and require a complex pattern, pin code, password, or biometrics to unlock. Devices must be configured to automatically wipe all data in the event that a passcode is incorrectly entered 10 times in a row.

LiveBetter issued smartphones and tablets must not operate jailbroken operating systems, not should have the operating system rooted. Apps installed on these devices must be obtained from legitimate sources, such as the Google and Apple App Stores.

Where LiveBetter has installed mobile-device-management software onto the device, staff must not remove this software under any circumstance.

8.10.2. Non-LiveBetter Smartphones/Tablets

Non-LiveBetter smartphones and tablets will have the ability to access corporate resources, such as email, calendars and OneDrive, and as such may pose a high level of risk for data loss to the organisation. As such, any staff member who accesses corporate resources from personal smartphones and tablets must ensure that the device is configured to lock after a period of inactivity and require a complex pattern, pin code, password, or biometrics to unlock. The devices must also be configured to automatically wipe all data in the event that a passcode is incorrectly entered 10 times in a row.

To maintain access to corporate resources from non-LiveBetter smartphones and tablets, staff must regularly update the operating system to protect against security vulnerabilities. Staff are also required to action all requests to update their non-LiveBetter device by LiveBetter ICT.

In order to sync LiveBetter email, calendars and OneDrive, LiveBetter may require staff to install mobile-device-management software onto the device. Such software will allow LiveBetter to remotely wipe LiveBetter data from the device should the device be lost. Where a staff member does not want to have such software installed, they will still have access to LiveBetter email, calendars and OneDrive via the Office 365 portal.

8.10.3. Smart Watches / Wearables

While LiveBetter does not currently issue smart watches and wearables to staff, it is acknowledged that staff may wish to pair these devices with LiveBetter and non-LiveBetter smartphones and tablets that have access to access corporate resources, such as email, calendars and OneDrive.

As a minimum, smartwatches and wearables must be configured with a PIN or passcode to protect any information stored on the watch. This PIN/passcode must be enforced to be entered when at least one of the following events occurs:

a) The smart watch / wearable is out of range of the paired mobile device (proximity-based lock)
b) The smart watch/wearable has not been used for 5 minutes (time-based lock)
c) The smart watch/wearable has been removed from the person (e.g. the apple watch has the ability to automatically lock after being removed from a person's wrist)

Where the device does not support a PIN or passcode, it **must not** be used to access corporate resources, such as email, calendars and OneDrive.

Due to the wide variety of models of smart watch / wearables on the market, the following best practices should be adhered to, to ensure the information is safe on the device:

a) Do not enable USB debugging on the device. This can be used to access the device's data when connected to a computer without the need for the PIN/passcode being entered.
b) Keep the device up to date by either enabling automatic updates (where possible) or regularly checking for updates to the device. This ensures known security weaknesses are patched.
c) Where remote wipe features are available, if the device is lost, remote wipe the device to ensure that the information is not compromised.
d) Avoid using cheap knock-off smart watches/wearables, as these devices have very poor data protection, risking both your personal information as well as LiveBetter sensitive information.

8.10.4. Reporting Loss or Theft of Mobile Device

If a mobile device is stolen while the user is logged in, the thief could use the device to access sensitive information or undertake actions as the authenticated user. If a smartphone or tablet is stolen while unlocked, the thief could use the phone to view internal emails containing sensitive information. They could also send emails as the smartphone user.

For this reason, the loss or theft of a mobile device must be reported to your line manager and LiveBetter ICT as soon as possible, and an incident logged in the CareWest

Incident Management System (CIMS). ICT will then undertake a remote wipe of the device to ensure any sensitive information is removed.

8.11. Cloud-based File Storage Applications

OneDrive for Business is a cloud-based file storage application that is provided to each user in Office 365 using your LiveBetter credentials. This instance of OneDrive is managed by LiveBetter, and thus is secure and backed up. Other cloud-based applications like Dropbox and Evernote are popular for storing information, but unless LiveBetter has conducted an information security risk assessment, we cannot rely on the information to be secure. Therefore, applications other than the LiveBetter OneDrive for Business should not be used to store sensitive information.

8.12. Removable Storage Media

Sensitive information on CD/DVDs and USB flash disks could be stolen or lost leading to data breaches. Therefore, sensitive information should only be copied where there is a business requirement to do so, and must only be transferred to secure encrypted storage media. Secure encrypted USB flashdrives can be obtained from LiveBetter ICT on an as needed basis.

8.12.1. Reporting Loss or Theft of Removable Storage Media

The loss or theft or removable storage media, such as CD/DVDs, USB flash disks, or backup tapes must be reported to your line manager and the CIO as soon as possible, and an incident logged in CIMS.

8.13. Clear Desk & Clear Screen

Hardcopy printouts containing personally identifiable information (PII) left unattended on desks could be viewed or taken by individuals who are not authorised to have this information, potentially creating a data breach.

For this reason, all hardcopy printouts containing personally identifiable information must be appropriately stored, and workstations locked, before employees leave their work area.

Printouts containing sensitive information should be collected from the printer promptly. When disposing of printouts containing sensitive information, the printouts must be placed in a document security bin.

8.14. Physical Access to Workstations

Unauthorised individuals accessing workstations could undertake activities as the authenticated user. These activities could include accessing sensitive information, and using information systems to perform unauthorised actions.

For this reason, only authorised individuals shall be allowed access to LiveBetter's workstations. Customers and unauthorised visitors must not be provided with access to LiveBetter workstations which are intended for use by employees.

8.14.1. Reporting Unauthorised Access

If an employee observes a customer or unauthorised visitor accessing a LiveBetter workstation they should immediately inform their line manager and log an incident in CIMS.

8.15. Sensitive Information Handling

Sensitive information is information that must be protected because it might cause perceivable damage to someone or something if revealed to persons not entitled to be in possession of this information. This includes personal information, commercially confidential information, and health information.

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a) Whether the information or opinion is true or not; and
b) Whether the information or opinion is recorded in a material form or not.

Examples of personal information include government issued identifiers such as driver’s license and tax file number, non-permanent information like a customer’s postal address or mobile number, and permanent information like a customer’s full name or date of birth.

Commercially confidential information is any information pertaining to the business activities of LiveBetter and its subsidiaries that is not publicly available, or that a reasonable person would assume to be not publicly available, or any information that has a value that would be, or could reasonably expected to be, destroyed or diminished if disclosed. Examples of commercially confidential information include sales data, plans and strategies, finances, and product launch information.

Health Information is any information pertaining to an individuals past, present, or future physical or mental health or condition or to the provision of health care to an individual. Due to the increased sensitivity of health information, and the additional requirements under the NSW Health Records and Information Privacy Act 2002, such information when linked with personally identifiable information, such that the individual could be uniquely identified, poses an increased risk to customers of LiveBetter. As such, a data breach involving health information should be taken extremely seriously.

8.15.1. Sending Sensitive Information to Third Parties

When considering sending sensitive information to external third parties via any electronic means, including email, uploads, and file sharing, firstly determine whether the information can be obfuscated or anonymised. If the information cannot be obfuscated or anonymised, it should be sent in line with the sensitive information transfer rules below.

8.15.1.1. Obfuscating Sensitive Information

Obfuscation of sensitive information – that is, modifying it in such a way that the information is ambiguous, results in non-sensitive information. LiveBetter ICT can assist with determining the best way to obfuscate information.

Obfuscation Example

An external third party supports an information system and has asked for a copy of the system’s files in order to troubleshoot an issue. The files contain sensitive information – Medicare IDs. By replacing the Medicare IDs with random numbers, the information is obfuscated, and can now be safely sent to the external third party.

8.15.1.2. Anonymising Sensitive Information

Anonymising sensitive information – that is, modifying it in such a way that the information is anonymous, results in non-sensitive information. LiveBetter ICT can assist with determining the best way to anonymise information.

Anonymising Example

An external third party supports an information system and has asked for a copy of the system's files in order to troubleshoot an issue. The files contain sensitive information – customers' names. By replacing all the customer names with 'John Doe', the information is anonymised, and can now be safely sent to the external third party.

8.15.1.3. Information Transfer Rules

If it is not practical to obfuscate and/or anonymise sensitive information, the following rules must be followed when sending sensitive information to third party businesses:

a) Only send information if it is really necessary, and limit the information to only that which is required.
b) Password protect the information before sending it, and provide the password in a different manner to the information. For assistance with this, please contact LiveBetter ICT.
c) Ensure the third party's information security has been assessed by LiveBetter. An information security risk assessment can be requested by contacting LiveBetter ICT.

Information Transfer Rules Example

LiveBetter needs to provide a spreadsheet containing customer names and postal addresses to a third party, 'Massive Mailouts', so they can send letters for LiveBetter to its customers. This is a business process; therefore, this information is needed to be sent.

The spreadsheet contains the customers' names and postal addresses but also contains customers' date-of-birth. As the date-of-birth is not required by Massive Mailouts, that information is removed from the spreadsheet (rule 1).

The spreadsheet is then encrypted and password protected, ready to be sent via email. The sender can call 'Massive Mailouts' to let them know the password (rule 2).

An information security risk assessment of 'Massive Mailouts' has previously been completed by LiveBetter. 'Massive Mailouts' have good information security in place, so our customers' information will be safe when we share it with them (rule 3).

8.16. Reporting Information Security Incidents and Data Breaches

An information security incident is either a breach of this policy or failure of information security safeguards that has a significant probability of compromising business operations and threatening information security.

If an employee becomes aware of an information security incident or a data breach, they must log an incident in CIMS.

Examples of Information Security Incidents:

- Sending emails containing pornography
- Writing down user account passwords
- Allowing someone other than an authorised user to use a workstation.

A data breach is a compromise of information security that leads to the loss or unauthorised access, use, modification, disclosure, or other misuse of sensitive information

Examples of Data Breaches:

- Lost or stolen laptops, or lost or stolen USB flash drives
- Sending of sensitive information to the wrong external third party email address
- A third party vendor being hacked or accidentally allowing other customers to access LiveBetter information

9. Breach of Policy

Breaches of this policy shall be reported as information security incidents in accordance with LiveBetter's IT Incident and Data Breach Management Policy.

Breaches or non-compliance with this policy can lead to disciplinary action which may result in termination of employment. Where disciplinary action is recommended, such action must be taken in accordance with the relevant HR processes.

10. Functions and Delegations

Function	Delegation Authority (e.g. Board, CEO, etc.)
Policy Approval	Executive
Policy Implementation	CIO
Policy Review	CIO

11. Revision History

Revision No	Date Revised	Brief description of nature of amendments	Modified By
1	31/01/2017	Initial Version	Craig Tye - CIO
2	23/03/2017	Minor changes due to feedback from Document Review Committee	Craig Tye - CIO

12. Related Policies, Procedures, Standards, Instructions and Other Documents

Policies

- POL-ICT-0001 Information Security Policy
- POL-ICT-0004 IT Incident and Data Breach Management Policy
- LiveBetter Privacy and Confidentiality Policy
- LiveBetter Social Media Policy

Procedures

- None

Instructions and Forms

- None

Other Documents

- None

13. Acknowledgements

The Office of the Australian Information Commissioner’s Guide to securing personal information – ‘Reasonable Steps’ to protect personal information (2015)