liveBetter

Information Technology Acceptable Usage Policy

Policy Control		Document Reference	POL-ICT-0002
Owner	ICT	**Revision Number**	3.0
Date Reviewed	1/11/2019	**Review Period**	6 Month(s)
Next Review Date	1/05/2020	**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 and forms part of LiveBetter's Information Security Management Framework which outlines LiveBetter's approach to managing information security.

3. 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.

4. Roles and Responsibilities

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

4.1. LiveBetter Technology Services

LiveBetter Technology Services shall be responsible for:

a) Ensuring employees are made aware of relevant new information security vulnerabilities

b) Assisting in the development and review of associated training modules

c) Ensuring the destruction of all sensitive information contained within system components, computers, tablets and phones prior to their disposal or reissue

d) Reviewing the encryption of portable endpoint devices

e) Managing the purchase, setup and ongoing maintenance of all information technology devices.

f) Managing the scanning of web traffic and inbound emails

g) Ensuring that backup media is strictly controlled when in the custody of technicians

In addition, the Head of Technology Services and EGM Strategy shall be responsible for:

a) Investigating breaches to this policy

b) Approving exceptions to this policy

4.2. Human Resources Team

The Human Resources Team shall be responsible for ensuring that:

a) Contractors who are to access LiveBetter information technology resources 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 training modules based on this policy within 3 months of commencement
d) All employees annually complete training modules based on this policy

5. Employee Accountabilities

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.

5.1. Prohibited Usage

It is strictly prohibited to use LiveBetter systems and devices, including but not limited to internet, email, Skype for Business, Teams, laptops, tablets and mobile phones, for any purpose that is in violation of LiveBetter policies, state and federal laws and regulations, and contractual obligations. Examples of such usage may include:

a) Downloading or uploading of large files such as videos, streaming radio stations or other media, except as required as part of business functions
b) Download, upload, stream, share, send and/or display pornographic or other inappropriate material
c) Download, upload, send or forward copies of electronic works in violation of copyright or other general laws or contractual obligations
d) Send sensitive information to non-LiveBetter email accounts, including your personal account, with the exception of emails required to be sent as part of business functions
e) Send unsolicited mass distribution emails
f) Use LiveBetter systems for personal monetary gain or for commercial purposes not directly related to LiveBetter's business
g) Install or use software with the direct or indirect result of avoiding security controls and restrictions
h) Use LiveBetter systems to negatively impact the operations of another organisation

5.2. Personal Usage

Occasional and reasonable personal use of LiveBetter systems such as email, internet and instant messaging is allowed providing the usage:

a) Is not prohibited (see 5.1 Prohibited Usage)
b) Is not excessive
c) Does not adversely affect or cannot reasonably be expected to adversely affect the performance of the user's duties
d) Does not adversely affect or cannot reasonably be expected to impact the performance of LiveBetter's information systems

Access to personal email accounts such as Gmail or Hotmail, is strictly prohibited on LiveBetter's internal networks. LiveBetter reserves the right to restrict access to any external website or internet resource that it deems inappropriate for use by staff. LiveBetter may also place restrictions on access to sites based on the impact these sites may have on the performance of LiveBetter's information systems.

5.3. Password Management

Passwords form the primary defence and security for user accounts.

5.3.1. User Accounts

Individual user accounts exist to allow permissions to be allocated specific to the user. Your user account password is used to ensure that only you can access your user account and must be kept secret. For this reason, it is prohibited to:

a) Tell anyone your user account password
b) Write down a user account password
c) Record a user account password in an electronic document, with the exception of secured password vaults
d) Attempt to use another user's account to access information or information systems
e) Allow anyone to use your user account on a workstation that you are logged into
f) Leave a device unattended and unlocked that is logged in to your LiveBetter account

To assist in the protection of your account LiveBetter computers will automatically lock after five minutes, however staff should always lock their computer whenever they walk away from it.

5.3.2. 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 systems. This account may only be shared and used by approved staff at the residence and should never be provided to customers or the public. The same restrictions apply to Shared Accounts as User Accounts.

5.3.3. Account Password Selection

User account passwords must follow the rules listed below:

1. Contain 3 of the 4 following character types
   a) Lowercase letters
   b) Uppercase letters
   c) Special characters
   d) Numbers
2. Be at least 8 characters in length
3. 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 IT may increase the complexity requirement as required by the organisation's information security needs. For tips and tricks on setting your password, see the FAQs on the Intranet.

5.3.4. Forgotten Account Passwords

In the event that an employee has forgotten their user account password, they should contact the Technology Service Desk on 1800 002 500, option 4, and request a password reset. The Service Desk will verify the user based on shared unique identifiers for example, an employee ID, to prevent imposters from being able to gain access to LiveBetter systems. The Service Desk 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 the Technology Service Desk, 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 the Service Desk on their behalf.

5.3.5. 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.

5.4. Email Security

Emails sent to LiveBetter email accounts are automatically scanned for phishing *[an email designed to trick a user into providing their logon details],* 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 JIRA ticket with LiveBetter ICT to have the item reviewed.

While these systems are kept up-to-date, new versions of malware may not be recognised, and may not be blocked. Also, as phishing emails become more sophisticated, they may find ways to trick the filters. 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.

If you are unsure of an email you can forward it to ICT@livebetter.org.au with a comment to "*please advise if this email is safe"*

5.5. Internal Collaboration Platforms

LiveBetter has a number of systems intended to be used by staff to interact and collaborate. These systems include Skype for Business, Yammer and Teams, but may be extended to include other systems as determined by LiveBetter Technology Services. These platforms offer instant messaging, phone and video calling, screen sharing, file sharing and social-media-esque functionality.

When staff are using these platforms they 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 authorised to know that information.
- Be careful: It is VERY easy to accidentally post information to the entire organisation, rather than a specified group!

Where staff require the sharing of sensitive documents and information, this should be undertaken via either the Intranet or Microsoft OneDrive. This provides 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.

5.6. Computers, Tablets, Phones and Equipment

Only LiveBetter IT issued computers, tablets and phones may be connected to LiveBetter's corporate 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.

5.6.1. 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.

5.6.2. Updates

Operating system updates are regularly released to improve the security of your computer. These updates will be downloaded and installed on your computer in the background. Periodically your computer will need to restart to apply these updates. When this occurs, you will receive an alert on your screen allowing you to postpone the restart. It is important that you manually restart your computer within 24 hours of this alert, or it will automatically restart on its own, which may result in it restarting at an inopportune time.

5.6.3. Purchasing and Procurement

All Information Technology equipment and software must be requested via an IT Equipment Request in JIRA to ensure that it is purchased and configured in line with our standards. It is a breach of this policy for staff outside of IT to purchase IT assets without prior approval from IT. This ensures that any equipment and software purchased will be standardised, compatible, supported and correctly configured for LiveBetter's network. 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' senior manager, with justification for the non-standard request.

5.6.4. Mobile Devices

Staff issued mobile devices must be regularly updated, must lock after a period of inactivity and must require pin code, password or biometrics to unlock. 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. Where LiveBetter has installed mobile-device-management software onto the device, staff must not remove this software under any circumstance.

5.6.5. Non-LiveBetter Smartphones/Tablets

Non-LiveBetter smartphones and tablets will have the ability to access corporate resources for example email, calendars and OneDrive, and as such may pose a high level of risk for data loss to the organisation. Therefore, any staff member who accesses corporate resources from personal smartphones and tablets must ensure that the device is used in accordance with the [BYOD Policy]

5.6.6. Removable Storage Media

Sensitive information on CD/DVDs and USB flash drives 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 IT on an as needed basis.

5.6.7. Reporting Loss, Theft or Damage of Equipment

If a laptop, phone, tablet or removeable storage media is lost, the thief could use the device to access sensitive information or undertake actions as the authenticated user. For this reason, the loss or theft of any IT equipment must be reported to your line manager and LiveBetter Technology Services as soon as possible, and an incident logged in the Company Incident Management System (CIMS). IT will then undertake a remote wipe of the device to ensure any sensitive information is removed.

Damaged equipment must be reported to LiveBetter Technology Services as soon as reasonably possible, where it may be repaired or replaced. It is important that any damaged device is returned to LiveBetter Technology Services as even a non-functioning device can pose a risk of a data breach.

5.7. 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. Any other cloud-based applications (e.g. Dropbox and Evernote) are not subject to a LiveBetter information security risk assessment, and therefore are not be used to store any LiveBetter information.

5.8. Physical Access to Workstations

Unauthorised individuals accessing workstations could undertake activities as the authenticated user including accessing sensitive information. 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. 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.

5.9. Reporting Information Security Incidents and Data Breaches

An information security incident is a 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, data breach or a breach of this policy, they must log an incident in CIMS in line with LiveBetter's IT Incident and Data Breach Management Policy.

Examples of Reportable Incidents:

- Sending emails containing pornography or accessing pornography on any device
- Writing down user account passwords
- A LiveBetter email account being used to send phishing emails
- Allowing someone other than an authorised user to use a workstation
- Unauthorised access to your LiveBetter account by another individual
- Lost, stolen or incorrectly disposed of equipment that stores data including laptops, USB flash drives, mobile phones and printers

- 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

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.

5.10. Monitoring

All monitoring of LiveBetter's information systems shall be in line with LiveBetter's *Workplace Surveillance Policy*.

5.11. 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 IT or authorised third parties after authorisation in writing by the CEO, Executive General Manager People and Culture, or the relevant Executive Manager.

The Executive General Manager (EGM) Strategy is empowered to initiate an investigation into suspected information security incidents and shall advise the EGM 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.

6. Functions and Delegations

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

7. 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
3.0	26/08/2019	Substantial revision to reduce length and improve readability. Updated with new executive structure. Removed details around monitoring and added reference to Workplace Surveillance Policy. Clarified 8.9.3. Purchasing and Procurement regarding requirement and method to request equipment	Chris Rawlins - EGM, Strategy

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

<u>Policies</u>

- POL-ICT-0001 Information Security Policy

- POL-ICT-0004 IT Incident and Data Breach Management Policy
- POL-ICT-0009 Workplace Surveillance Policy
- LiveBetter Privacy and Confidentiality Policy
- LiveBetter Social Media Policy

Procedures

- None

Instructions and Forms

- None

Other Documents

- None