Information Security Policy

Key Details

Policy prepared by	David Riddell
Approved by board / management on:	30th March 2018
Policy became operational on:	31st March 2018
Reviewed on:	31st March 2021
Next review date:	31st March 2022

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be read and understood by all company employees. This document will be reviewed and updated by Management on an annual basis, or when relevant to include newly developed security standards into the policy.

2. Information Security Policy

The Company handles personal and confidential information daily. Such information must have adequate safeguards in place to protect the data, to protect privacy, to ensure compliance with various regulations and to guard the future of the organisation.

The Company commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end we are committed to maintaining a secure environment in which to process information so that we can meet these promises.

Employees handling personal or confidential data should ensure they:

- Handle information in a manner that fits with its sensitivity.
- Do not disclose personnel information unless authorised.
- Protect sensitive information.
- Keep passwords secure and do not share accounts.
- Take all necessary steps to prevent unauthorised access to confidential data.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- Take extra care when working on portable computers as these are especially vulnerable.
- Use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- When connecting a laptop or mobile device to a network outside the company's office, thought should be given to the security of that network, for instance connections should not be made to open wireless networks as they have no

encryption of data transmitted over the air.
- Do not install new software or hardware, including wireless access devices unless they have management approval.
- Always leave desks clear of sensitive data, locking any sensitive documents in a secure cabinet.
- Lock computer screens when unattended.

Information security incidents must be reported, without delay, to the office manager. We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from the office manager

3. Acceptable Use Policy

The management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Company's established culture of openness, trust and integrity. The management team is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless posting is in the course of business duties.
- Employees should limit personal use of the Company information and telecommunication systems and ensure it doesn't interfere with their job performance.
- The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.
- Employees should not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

5. Protect Stored Data

All data stored and handled by the Company and its employees must be securely protected against unauthorised use at all times. Any sensitive data that is no longer

required by the Company for business reasons must be discarded in a secure and irrecoverable manner. Timescales for deletion of inactive data is detailed in the company's GDPR statement.

6. Physical Security

- Access to sensitive information in both paper and electronic format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.
- Employees should take all necessary steps to prevent unauthorised access to confidential data, this includes locking the office door when leaving the office unattended.
- Documents containing sensitive information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive information, this would include access to the company's servers or routers.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors. For instance, employees will be wearing staff uniforms.
- Visitors should not be granted access to the companies Wi-Fi network.
- Strict control is maintained over the external or internal distribution of any documents containing data and has to be approved by management.
- Strict control is maintained over the storage and accessibility of all forms of sensitive documentation.
- All computers that store sensitive data must have a password protected screensaver enabled to prevent unauthorised use.

7. Protect Data in Transit

- All sensitive data must be protected securely if it is to be transported physically or electronically.
- Sensitive data must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send data via email or via the internet or any other modes then it should be done after authorisation and by using a strong encryption.
- The transportation of physical documentation containing sensitive data to another location must be authorised by management. Only secure courier services or company vehicles may be used for the transportation of such media.

8. Disposal of Stored Data

- All data must be securely disposed of when no longer required by the company, regardless of the format (paper or electronic) on which it is stored.
- Hardcopy materials must be crosscut shredded so they cannot be reconstructed.
- The Company procedures for the destruction of electronic media are as follows. All data on electronic media must be rendered unrecoverable by the physical

destruction of the media.
- All electronic, or hardcopy, material awaiting destruction must be held in lockable storage clearly marked “To Be Destroyed” - access to this area must be restricted.
- Data files should be deleted and immediately removed from any recycle bin.

9. Network security

- Firewalls must be implemented at each internet connection and the internal company network.
- Firewall and router configurations must restrict connections between untrusted networks and any company systems.
- All inbound and outbound traffic must be restricted to that which is required for the operation of the business.
- All inbound network traffic is blocked by default, unless explicitly allowed.
- Disclosure of private IP addresses to external entities must be authorised.
- No direct connections from Internet to the business network will be permitted. All traffic has to traverse through a firewall.

10. System and Password Policy

All users, including contractors and suppliers with access to the Company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- All users must have a unique ID.
- All users must use a password to access the company network or any other electronic resources.
- All user ID’s for terminated users must be deactivated or removed immediately.
- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.
- All user level passwords must be changed on a six-monthly basis.
- A minimum password history of four must be implemented.
- A unique password must be setup for new users.
- All non-console administrative access will use appropriate technologies like ssh, vpn, ssl etc or strong encryption is invoked before the administrator password is requested.
- System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands.
- The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:
    - **a)** Be as long as possible (never shorter than 8 characters).
    - **b)** Include mixed-case letters.
    - **c)** Include digits and punctuation marks.
    - **d)** Not be based on any personal information.

11. Anti-virus policy

All machines must be configured to run the latest anti-virus software as approved by the Company. The preferred application to use is AVG Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.

- The antivirus software in use should be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits).
- All removable media (for example USB devices and others) should be scanned for viruses before being used.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain a virus.

12. Patch Management Policy

All Workstations, servers, software, system components etc. owned by the company must have up-to-date system security patches installed to protect the asset from known vulnerabilities.

Where ever possible all systems and software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from the respective vendor and have to follow the process in accordance with change control process. **Employees must not reject updates when offered.**

13. Remote Access policy

It is the responsibility of employees, contractors, suppliers and agents with remote access privileges to Later Life Training's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the company.

Secure remote access must be strictly controlled. Control will be enforced by strong password authentication or public/private keys with strong pass-phrases.

Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity.

All hosts that are connected to the Company internal networks via remote access technologies will be monitored on a regular basis.

All remote access accounts will be reconciled at regular intervals and the accounts will be revoked if there is no further business justification.

14. Wireless Policy

Installation or use of any wireless device or wireless network intended to be used to connect to any of the company networks or environments requires authorisation by the office manager.

The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.

Any other security related wireless defaults should be changed if applicable.

Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of data.