TLM LASER

YOUR PRODUCTIVITY OUR PRIORITY

IT Policy and Procedure Manual

Version 1.1
January 1, 2020

2 Navigation Court, Harris Business Park, Stoke Prior, Bromsgrove, Worcestershire, B60 4FD

TEL. +44 (0) 1527 959099 FAX. +44 (0) 1527 959091 EMAIL. info@tlm-laser.com

Table of Contents

1 INTRODUCTION

TLM Laser Limited IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the agency which must be followed by all staff. It also provides guidelines that will be used to administer these policies, with the correct procedure to follow.

TLM Laser Limited will keep all IT Policies and Procedures current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

These policies apply to all employees.

2 TECHNOLOGY HARDWARE PURCHASING

This policy provides guidelines for the purchase of hardware for the Agency to ensure that all hardware technology for the Agency is appropriate and where applicable integrates with existing technology. The objective is to ensure there is minimum diversity of hardware within the Agency.

2.1 Purchasing desktop computer systems

The desktop computer systems purchased must run Windows Pro 7, Windows 8, Windows 8.1 or Windows 10 and integrate with existing network.

The desktop computer systems must be purchased as standard desktop system bundle.

The desktop computer system bundle must include:

- Desktop tower
- Desktop screen of 20" minimum
- Keyboard and mouse
- Windows Pro 7, Windows 8, Windows 8.1 or Windows 10
- Speakers

The minimum capacity of the desktop must be:

- Intel I5 Minimum
- 8 GB Ram Minimum

Any change from the above requirements must be authorized by the Network System Administrator.

All purchases of desktops must be supported include three (3) year NDB onsite service and be compatible with the existing network.

2.2 Purchasing portable computer systems

The purchase of portable computer systems includes notebooks and laptops.

Portable computer systems purchased must run Windows Pro 7, Windows 8, Windows 8.1 or Windows 10 and integrate with existing network.

The portable computer systems purchased must be Dell.

The minimum capacity of the portable computer system must be:

- Intel I5 Minimum
- 8 GB Ram minimum

Any change from the above requirements must be authorized by the Network System Administrator.

All purchases of all portable computer systems must include three (3) year NBD onsite service and be compatible with the existing network.

2.3 Purchasing server systems

Server systems can only be purchased by the Network System Administrator.

Server systems purchased must be compatible with all other computer hardware on the network.

All purchases of server systems must include 3 Year NBD onsite service and be compatible with the existing network.

Any change from the above requirements must be authorized by Network System Administrator.

2.4 Purchasing computer peripherals

Computer system peripherals include add-on devices such as printers, scanners, external hard drives etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software on the network.

The purchase of computer peripherals can only be authorized the Network System Administrator.

Any change from the above requirements must be authorized by the Network System Administrator.

2.5 Purchasing cell phones and mobile hot spots

Purchasing of cell phones and mobile hot spots requires the approval from the requesting programs division director.

.

3 Software

The goal of the IT Department is to provide stable technology solutions that both perform well and appropriately address business needs. A lack of standards regarding what software titles can be installed on company end-user devices, including desktop and laptop machines, can hinder provision of excellent service to all end users and departments.

The purpose of this Software Policy is to address all relevant issues pertaining to appropriate software installation and deployment on TLM Laser Limited end-user computing devices.

3.1 Supported Software

The following is a list of fully supported, standard software that may be installed on company-owned end-user devices:

- Microsoft Windows 7
- Microsoft Windows 8
- Windows 10
- Microsoft Office 2010,2013,2016 (Outlook, Word, Excel, PowerPoint)
- Adobe
- Markus
- Fobadraw
- Saleforce
- Sage
- Microsoft Teams

- Teamviewer
- Microsoft Edge

Other supported software titles, available upon request and approved by manager.

The IT Department does not provide support for any software titles not listed above. The IT Department expressly forbids installation of the following software:

- Privately owned software.
- Internet downloads.
- Pirated copies of any software titles.
- Any title not listed in this policy.
- Any software not installed according to the procedures set out in this policy.

3.2 Software Requests

It is imperative that all software installations and de-installations be thoroughly documented so that appropriate licensing fees can be paid or amended.

If you would like to have software installed on your device, approval must be obtained from your manager (or designate) as well as the IT Department. This includes all software titles listed above, currently unlisted titles, and privately owned and licensed titles. The IT Department reserves the right to reject any software installation request for any reason.

Please submit a ticket for any software needs. The ticket submitted is subjected for validation by requestor's direct report to authorize.

3.3 Software Installation

Software titles are to be installed on company-owned end-user devices by the IT Department, or under their direct supervision.

All software installed on TLM Laser Limited (including all commercial and shareware products) must be used in compliance with all applicable licenses, notices, contracts, and agreements.

The IT Department reserves the right to uninstall any unapproved software from a company-owned machine.

3.4 Periodic Audits

The IT Department reserves the right to monitor software installation and usage on TLM Laser Limited end-user computing devices. The IT Department will conduct periodic audits to ensure compliance with this Software Installation Policy. Unannounced, random spot audits may be conducted as well. During such audits, scanning and elimination of computer viruses may also be performed. Other unsanctioned software may also be uninstalled at this time.

3.5 Non-Compliance Penalties

Penalties for violation of this policy will vary depending on the nature and severity of the violation. Penalties include: Disciplinary action, including, but not limited to, reprimand, suspension and/or termination of employment.

4 Personal Devices

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and other technology devices deemed appropriate for business purposes. All staff who use or access TLM Laser Limited technology equipment and/or services are bound by the conditions of this Policy.

4.1 Current mobile devices approved for business use

The following personally owned mobile devices are approved to be used for business purposes:

- Smart phones
- Tablets
- Laptops and desktops for remote connectivity (Requires prior management and IT approval)

Each employee who utilizes personal mobile devices agrees:

- Not to download or transfer business or personal sensitive information to the device.
- Not to use the registered mobile device as the sole repository for TLM Laser Limited. All business information stored on mobile devices should be backed up
- To make every reasonable effort to ensure that TLM Laser Limited information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorized persons and all registered devices should be password protected
- Not to share the device with other individuals to protect the business data access through the device
- To abide by TLM Laser Limited Acceptable Use policy for appropriate use and access of internet sites etc.
- To notify TLM Laser Limited immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to TLM Laser Limited equipment.

4.2 Exemptions

This policy is mandatory unless a member of AMT grants an exemption. Any requests for exemptions from any of these directives, should be referred to the AMT.

4.3 Breach of this policy

Any breach of this policy will be referred to HR who will review the breach and determine adequate consequences.

4.4 Indemnity

TLM Laser Limited bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify TLM Laser Limited against any and all damages, costs and expenses suffered by TLM Laser Limited arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by TLM Laser Limited.

5 Security

This policy provides guidelines for the protection and use of information technology assets and resources within the agency to ensure integrity, confidentiality and availability of data and assets.

5.1 Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through a door with a cipher lock.

It will be the responsibility of the Network System Administrator to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify the Network System Administrator immediately.

All security and safety of all portable technology, such as laptops, tablets, projectors etc. will be the responsibility of the employee who has signed an Equipment Receipt Acknowledgement form. Each employee is required to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, the AMT will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All computers, laptops, notebooks, tablets etc. when kept at the office desk is to be secured by a password provided by the HR department during orientation.

Computers located in residential homes should never be left logged in and unattended to prevent unauthorized access by our consumers, vendors and any other visitors.

5.2 Information Security

All data is to be backed-up using existing backup process in place.

It is the responsibility of the IT Department to ensure that data back-ups are conducted.

All technology that has internet access must have anti-virus software installed. It is the responsibility of the IT Department to install all anti-virus software and ensure that this software remains up to date on all technology used by the agency.

All information used within the Agency is to adhere to the privacy laws and the Agency's confidentiality requirements.

5.3 Technology Access

Every employee will be issued with a unique identification code to access the business technology.

Each password is not to be shared with anyone.

HR is responsible for the issuing of the initial password for all employees.

Where an employee forgets the password or is 'locked out', then the IT Department is authorized to reset the employees initial password.

he following table provides the authorization of admin access:

Technology – Hardware/ Software	Persons authorized for access
ADP	HR/Fiscal
Email	IT
Intranet	IT
eAcademy	HR
Network Shares	IT
Networks Servers	IT
Wired and Wireless Connectivity	IT
Firewalls and security devices	IT
VPN Access	IT

Technology – Hardware/ Software	Persons authorized for access
Shared Printers / Copiers	IT
Desktop Faxing	IT
Facility access controls	IT, Maintenance
Facility Alarms	Maintenance (removed IT)
Phone Systems	IT, Fiscal
Internet Access	IT, Fiscal
Building / Lot Access	IT
PI Issued Cell Phones	IT/ Fiscal

6 Social Networking

Social media are powerful communication tools that have a significant impact on organizational and professional reputations. The following policy is to help clarify how best to enhance and protect our organization, personal and professional reputations when participating in social media.

Social media are defined as media designed to be disseminated through social interaction, created using highly accessible publishing techniques. Examples include Facebook, Blogs, MySpace, RSS, YouTube, Second Life, Twitter, LinkedIn, Delicious, Flickr, etc.

Employees need to follow the same behavioral standards online as they would in real life. The same laws, professional expectations, and guidelines for interacting with consumers, fellow employees and others apply online as in the real world. Employees are liable for anything they post to social media sites.

1. **Make clear disclosures:** Personal blogs and other online posts should have clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of TLM Laser Limited. Be clear and write in first person. Make your writing clear that you are speaking for yourself and not on behalf of the company.
2. **Protect confidential and proprietary information:** Do not post confidential or proprietary information about TLM Laser Limited, employees, or consumers. Employees must still follow the applicable federal requirements such as FERPA and HIPPA. Adhere to all applicable agency privacy and confidentiality policies. Employees who share confidential information do so at the risk of disciplinary action or termination.
3. **Respect copyright and fair use:** When posting, be mindful of the copyright and intellectual property rights of others and of the agency.
4. **Avoid hazardous materials:** Do not post or link to any materials that are defamatory, harassing, discriminatory, or obscene.
5. **Do not qualify your work:** Do not post statements regarding the quality of your work nor the agency's.
6. Do not return fire: If a negative post or comment is found online about the agency, or yourself, or coworker do not counter with another negative post. Instead, please notify the Human Resources Department so it may take appropriate action.
7. **Terms of service:** Obey the Terms of Service of any social media platform employed

6.1 Guidelines

Remember that the Internet is not anonymous, nor does it forget. Everything written on the Web can be traced back to its author one way or another and very easily. Information is backed up often and posts in one forum are usually replicated in others through trackbacks and reposts or references.

The President and/or CEO is the only authorized person to speak on behalf of TLM Laser Limited with outside entities.

Any Social Media Communication should be consistent with TLM Laser Limited's Employment Manual, code of ethics, values, policies and applicable laws.

There is no clear line between your work life and your personal life. Always be honest and respectful in both capacities.

For further questions about this policy, please contact your supervisor or the Human Resources Department.

7 Acceptable/Unacceptable Use

TLM Laser Limited makes every effort to provide the best available technology to its employees. We communicate to employees through e-mail. This is a great way to keep the lines of communication open in a productive and efficient manner. We also have our Intranet as a key internal communication tool for important notices and updates as your first resource for policies and forms, and as the portal where you can connect directly to our e-mail website.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing e-mail, WWW browsing, and FTP, are the property of TLM Laser Limited. These systems are to be used for business purposes in serving the interests of the company in the course of normal operations.

Effective security is a team effort involving the participation and support of every TLM Laser Limited employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

7.1 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at TLM Laser Limited These rules are in place to protect the employee and TLM Laser Limited Inappropriate use exposes TLM Laser Limited to risks including virus attacks, compromise of network systems and services, and legal issues.

7.2 Scope

This policy applies to employees, contractors, consultants, temporary/seasonal, and other workers at TLM Laser Limited, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by TLM Laser Limited.

7.3 General Use and Ownership

TLM Laser Limited, at its option, may change, delete, suspend or discontinue parts of the manual in its entirety, unilaterally, at any time without prior notice. In the event of a policy change, employees will be notified. Any such action shall apply to existing as well as to future employees.

Agency property including computers, electronic mail, and voice mail should only be used for conducting Agency business. The use of the electronic mail system may not be used to solicit for commercial ventures, religious or political causes, or other non-job-related solicitations. Furthermore, the electronic mail system is not to be used to create any offensive or disruptive messages (i.e., messages which contain sexual implications, racial slurs, or any other comments that offensively address someone's age, sexual orientation, religious or political beliefs, national origin, or disability). In addition, the electronic mail system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials. Employees should understand that these systems are intended for business use, and that all computer information and electronic mail messages are considered Agency records. TLM Laser Limited must, and does, maintain the right and the ability to enter into any of these systems and to inspect and review any and all data recorded in those systems, so employees should not assume that such messages are private and confidential or that TLM Laser Limited will not have a need to access and review this information. Individuals using TLM Laser Limited's business equipment should also have no expectation that any information stored on their computer - whether the information is contained on a computer hard drive, computer disks, or in any other manner - will be private. TLM Laser Limited has the right to, but does not regularly, monitor electronic mail messages. The Agency will, however, inspect the contents of computers, or electronic mail in the course of an investigation triggered by indications of unacceptable behavior or as necessary to locate needed information that is not more readily available.

Given the Agency's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient.

Employees should not have any expectation of privacy and access. Employees are expected to access the Internet at least weekly to gain access to our Intranet and e-mail system.

7.4 Security and Proprietary Information

1. The information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: corporate strategies, competitor sensitive, trade secrets, specifications, consumer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed twice per year.
3. All PCs, laptops and workstations should be logged-off when the employee will be away for an extended period of time.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Postings by employees from a TLM Laser Limited email address to any Internet websites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of TLM Laser Limited, unless posting is in the course of business duties.
6. All PCs, laptops and workstations used by the employee that are connected to the TLM Laser Limited Internet/Intranet/Extranet, whether owned by the employee or TLM Laser Limited, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

7.5 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of TLM Laser Limited authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing TLM Laser Limited owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

7.6 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by TLM Laser Limited
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which TLM Laser Limited or the end user does not have an active license is strictly prohibited.
3. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Using a TLM Laser Limited computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6. Making fraudulent offers of products, items, or services originating from any TLM Laser Limited account.

7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
8. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
9. Circumventing user authentication or security of any host, network or account.
10. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
11. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet.
12. Providing information about, or lists of, TLM Laser Limited employees to parties outside TLM Laser Limited

7.7 Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within TLM Laser Limited 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by TLM Laser Limited or connected via TLM Laser Limited’s network.

8 Technical Support

Technical support will be provided by the IT department during normal business hours for all Agency approved devices and software. After hours support is available under special circumstances and will be reviewed on a case by case basis.

All technical support requires an IT request which can be created via the Intranet. No support will be provided without a request.

8.1 Equipment Requests

Permanent Assignment

All requests for new equipment such as laptops, desktops, printers, projectors etc. must be approved by division directors.

All requests require an IT request to be created.

The request should include:

- Equipment being requested
- Staff the equipment is being assigned to
- Date the equipment is required
- Approval

Temporary Assignment

In most case, equipment can be assigned for temporary use.

The IT department has a limited number of devices available temporary use and it is assigned on a first come first serve basis. Staff should create a request for the equipment at least five business days for it is required.

All requests require an IT request to be created.

The request should include:

- Equipment being requested
- Staff the equipment is being assigned to
- Date the equipment is required
- Date the equipment will be returned