

Use of the internet by employees of LI Europe is permitted and encouraged where such use supports the goals and objectives of the business. However, LI Europe has a policy for the use of the internet whereby employees must ensure that they:

- Comply with current legislation.
- Use the internet in an acceptable way.
- Do not create unnecessary business risk to the company by their misuse of the internet.

In particular the following is deemed unacceptable use or behaviour by employees:

- Visiting internet sites that contain obscene, hateful, pornographic, or otherwise illegal material.
- Using the computer to perpetrate any form of fraud, or software, film, or music piracy.
- Using the internet to send offensive or harassing material to other users.
- Downloading commercial software or any copyrighted materials belonging to third parties unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Publishing defamatory and/or knowingly false material about LI Europe, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Revealing confidential information about LI Europe in a personal online posting, upload, or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of malicious software into the corporate network.
- Company-owned information held on third-party websites.
- If you produce, collect and/or process business-related information in the course of your work, the information remains the property of LI Europe. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

1.0 Monitoring

LI Europe accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the company's internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

1.1 Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary action.

All company employees, contractors or temporary staff who have been granted the right to use the company's internet access are required to sign this agreement confirming their understanding and acceptance of this policy.

2.0 Internet

LI Europe expects every employee to have a fast broadband connection into their homes for use on the weekly video conference.

LI Europe provides a laptop and mobile phone and there are dongles that can be shared throughout the team. Each mobile provided comes with tethering and has a data bundle. Mobile internet on laptops should be accessed via a wifi dongle, mobile phone tethering or a wifi hotspot. Most client sites now offer a guest wifi facility and hotel access to free wifi. You should use these facilities wherever possible.

Employees should ensure that this usage does not bring the company into disrepute by using it for any illegal activity or malicious activity.

3.0 Email

Email sent out from employees' LI Europe account should be written in a professional manner and not bring the company into disrepute.

4.0 Mobile Phones

LI Europe will provide employees with a fully paid mobile phone. This is to be used for work related calls as well as any personal calls when travelling for work. This phone should not be used for any illegal activity or anything that will bring the company into disrepute.

When travelling abroad, due to the large costs associated with data usage, please ensure data usage is turned off unless required for a specific purpose.

Where possible use Skype/Zoom/Microsoft teams (or other video call service) for international calls.

5.0 Security Software

All LI Europe computers and laptops should have an up-to-date version of anti-virus software installed.

6.0 Related Policies

LIEURAPP22001 – Apprenticeship Continuity Plan
LIEURAPP22002 – Equality and Diversity Policy
LIEURAPP22003 – Safeguarding Adults Policy
LIEURAPP22004 – Prevent Duty Policy
LIEURAPP22005 – Health & Safety Policy
LIEURAPP22006 – Concerns, Complaints and Compliments Policy
LIEURAPP22007 – Recognition of Prior Learning Policy
LIEURAPP22008 – Quality and High Standards in Apprenticeship Training Policy
LIEURAPP22009 – Employee Professional Development Policy
LIEURAPP22011 – GDPR Policy
LIEURAPP20014 – Safer Recruiter Policy
LIEURAPP22017 – Functional Skills Subcontracting Policy
LIEURAPP22018 – Intervention Policy
LIEURAPP22019 – Plagiarism and Malpractice Policy
LIEURAPP22020 – External Speaker Policy
LIEURAPP22021 – Bullying and Harassment Policy
LIEURAPP22022 – Additional Learning Support Policy
LIEURAPP22023 – Whistleblowing Policy
LIEURAPP22024 – Malpractice in Certification and Assessment Policy
LIEURAPP22025 – Recruitment of Ex-Offenders Policy
LIEURAPP22026 – Academic Appeals Policy
LIEURAPP22027 – Apprenticeship Code of Conduct
LIEURAPP22028 – Conflict of Interest Policy

Policies are reviewed in January on an annual basis.

Company Director _____ Date _____