

INFORMATION, SECURITY & DATA PROTECTION POLICY

POLICY STATEMENT

Long O Donnell Associates Ltd recognises the importance of correct and lawful treatment of personal data. We are committed to the promotion of confidence in our information security and data handling procedures in compliance with the Data Protection Act 1998.

Internet Usage

Internet access is provided for users who require access to business related information. Users should be aware that Internet site visits may be logged and therefore traceable. Internet access must not be used for accessing, receiving, transmitting or downloading any material, the content of which could be deemed illegal, pornographic, indecent, offensive or unacceptable under UK law, the laws of any destination country or any country that the information may take route to reach its destination or the Long O Donnell Associates policy.

Users are also prohibited from subscribing to Newsgroups or from posting any information not associated with the interests of the Long O Donnell Associates. This includes a specific prohibition on the use of private chat rooms and forums. Materials available on the Internet should not be construed as 'free issue'. Copyright and other laws still apply to the Internet. You must have full authorisation from owners of materials, also having authorisation to download such materials. Users must not download, distribute or copy information or software that violates the company's policy, and are also advised that downloading materials from the Internet introduces the risk of allowing virus or malicious code into the company's computer network systems. When using any computer attached to the Long O Donnell network, users must not access the Internet except through a Long O Donnell approved Internet firewall/router. Users must not access the Internet directly, whether through a modem or through another service provider, unless the accessing computer is disconnected from all Long O Donnell networks.

Privacy Of Electronic Communications

Users of Long O Donnell's electronic communications should be aware that e-mails and other communications electronically are not private. On occasion, it may be necessary for e-mails that have failed to reach their destination, to be read by Technical Operations staff. The purpose of this is to determine the intended addressee and redirect the message to the correct address, not to read or discuss the content of the message.

Monitoring

Long O Donnell may engage in electronic monitoring of email and Internet access. All users are made aware of such monitoring and as a condition of access to electronic communications and computers will be required to consent to the company policies. All emails in and out of the company may be scanned for policy breaches, virus and malicious code. All Internet access may be electronically monitored and all site visits are traceable.


Disciplinary Action

Any infringement of the company policy will be regarded as misconduct. Any user misconduct of the company policy may result in disciplinary action, including summary dismissal. Any unauthorised use of email or the Internet is likely to result in disciplinary action including summary dismissal.

User Names & Passwords

Users are given individual passwords and must never give out their username or password, even to a superior, doing so the user will take any responsibility that person does using the user's credentials and may result in disciplinary action. If a user suspects that their password has become known they should contact the IT Supervisor or IMS Manager immediately.

Complaints

 LONG O DONNELL ASSOCIATES LTD	INTEGRATED MANAGEMENT SYSTEM	Reference LOD/IMS/IUS/001	
		Date Jan.17	Rev 03
		Page	2 of 3

Users who feel that they have cause for complaint as result of electronic communications should raise the matter initially with their immediate manager and/or the HR Co-ordinator. If necessary, the complaint can then be raised through the Grievance Procedure.

E-mail Content Checking

All email entering and leaving the Long O Donnell network may be subject to both content and virus checking. This is designed to mitigate against issues such as viruses, .exe files, partial messages, encrypted files and those containing possible threats such as java scripts. Corrupt, dangerous or otherwise undeliverable mail will be held on the server and will not be transmitted to the end user.

URL Filtering

All web access from Long O Donnell sites and equipment may be subject to URL filtering. This allows Long O Donnell to block access to sites deemed inappropriate. When accessing the Internet from a remote location, users are reminded that these access controls still apply and that users are not permitted to access the following site areas or download files associated with them.

Access Control

Long O Donnell allow the following material to be access via the internet:

- Business & Economy
- Education
- Entertainment
- Government
- Health
- Information Technology
- Job Search
- News & Media
- Religion
- Social Organisations
- Society, Lifestyle & Shopping
- Special Events
- Sports
- Travel
- Vehicles
- Images

Long O Donnell do not allow the following material to be access via the internet:

- Adult Material
- Drugs
- Gambling
- Games
- Illegal / Questionable
- Militancy / Extremist
- Malicious Web Sites
- Racism / Hate
- Tasteless
- Violence/Weapons
- Executable Downloads
- Sound Downloads
- Video Downloads

Should there be a requirement to access specific sites banned due to category then, upon approval; access can be provided to those web sites. There are no different restrictions for "out-of-hours" periods, including lunchtimes. There is no limit to the size of downloads given that inappropriate file types are restricted. Virus protection is present at all times when using the Long O Donnell system.

Data Protection

It should be noted that Long O Donnell conforms to the Data Protection Act of 1998 and as such, any personal information held by the company electronically or otherwise will address the following points:

- Personal data shall be obtained fairly and lawfully.
- Personal data shall be kept accurate and up to date and shall not be kept for longer than is necessary.
- Appropriate security measures shall be taken against unlawful or unauthorised processing of personal data and against accidental loss of, or damage to personal data.
- Personal data shall not be transferred to a country outside the European Economic Area unless specific exemptions apply. NB This includes the publication of personal data on the internet.



Thomas J. O'Donnell
Managing Director
Long O Donnell Associates Limited

January 2017