

ACTIVITY CAMPS



E-Safety and Online Safety Policy

Company Name	Le Mourier Swim/Sea/Save
Company Address	Inverness Lodge, Le Mont au Meunier, St Lawrence, Jersey, JE3 1FQ
Author Name	Stuart Diack
Contact Telephone	01534 869050
Contact Email	stuart@lemourier.co.uk

Monitoring and Review

This policy will be reviewed annually to ensure they remain correct and are fit for purpose. However, the policy may be reviewed and updated at any time to reflect any changes made by Le Mourier or the regulatory authorities or government legislation

Version:	2/11.23
Policy Launch date	November 2023
Next review date	November 2024

ACTIVITY CAMPS

Policy

This policy sets out the obligations and expectations of all employees of Le Mourier, including contractors and temporary staff across all aspects of the company, who use the Company's IT facilities for any purposes. IT facilities are provided to assist with day-to-day running's of the company and it is important that they are used responsibly, are not abused, and that individuals understand the legal professional and ethical obligations that apply to them when using these facilities.

It is important to note that all staff members of Le Mourier play a vital part in keeping customer, employee, and company information safe from cyber-attacks or breaches. It is also each staff member's responsibility to report such attacks or breaches as soon as possible to prevent the severity of impacts to any staff member of customer within Le Mourier.

Within Le Mourier several IT Systems are in use throughout the company, these are, but not limited to:

- Microsoft Office 365
- Bookeyo
- Mailchimp
- Go Cardless
- Xero

Microsoft PowerApps

Power Apps, fundamentally, is a service for building and using custom built business apps that connect to your data and work across the web and mobile. Apps can be used to input, link, and edit information connected to the users account and allow a business to complete systems of work in a time efficient way.

Within power apps, Le Mourier has created the following applications which are used through the Microsoft PowerApps App which can be downloaded from the App Store or Google Play Store:

- Incident and Injury Form
- Le Mourier Staff Training Log
- Holiday Requests
- Le Mourier Pool Plant
- Pool Water Testing
- Vessel End of Day Reports
- Vehicle, Vessel, and Venue Defect Reporting
- Fuel Receipts
- Overtime Reporting
- Charter Safety Briefing

ACTIVITY CAMPS

Each app comes with its own link to a data store within SharePoint (“Le Mourier PowerApps Data Store”), direct access is limited to management of Le Mourier and Full IT Administrators, however contribution access to each data store is enabled when a user has permission to use the application.

Each app is distributed to users determined by Le Mourier’s Director. Permission is granted and email notification is sent, the application will then be seen on the “All Apps” section of the Microsoft PowerApps Mobile App. Permission can be granted from the Full IT Administration Team and revoked when required by the Managing Director.

For all the above-mentioned applications, connections have been made to a Le Mourier Sub Site on SharePoint using Power Automate. For many of the apps mentioned, using Power Automate, the user will receive a submission notification through Microsoft Teams with a prompt at the end of the entry for the user to ensure they have received this step. Other automations may include Approvals Through the Teams Approval service, Emails to certain users and triggers depending on the condition of the entry.

Safe Internet Usage

This section of Le Mourier’s IT Infrastructure Policy relates to how all Full-Time, Part-Time, Seasonal or Student staff members safely interact with the company’s Internet Connection Facilities.

Le Mourier provides Internet Access across 5 main areas and facilitates a further 2 areas as detailed below:

Main Networks

Inverness Lodge (Main Office)
Inverness Lodge (Pool & Chalet Area)
Les Roche (Pool & Training Suite)
No. 18 Albert Pier (Le Mourier Marine)
No. 24 Albert Pier (Le Mourier Marine)
Trinity Yard (Le Mourier Marine)

Facilitated Networks

Inverness Lodge (Main House)
Inverness Lodge (Cottage)

Facilitated networks will soon become their own network with different SSID and Passwords but still facilitated through Inverness Lodge (Office)

ACTIVITY CAMPS

Authorisation

Authorisation to Le Mourier's Internet Connection Facilities may be granted by a Management or Senior Member of Staff who will be provided with the Password by one of Le Mourier's IT Administrators.

Please see Le Mourier's "IT Systems of Work Policy" for further information on further authorisation to Le Mourier's IT facilities.

No person is allowed to use Le Mourier's IT facilities who has not previously been authorised to do so.

Unauthorised access to IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

Le Mourier reserves the right to revoke authorisation to any user at any point or to change the SSID or Password of any network.

Employees, Contractors, or any other user of Le Mourier's Network are prohibited to give out any password to the company's Internet Connection Facilities to any other party without prior approval from Le Mourier's Management or IT Administrators.

Legislation

All users must comply with the relevant legislation. This includes the following:

Data Protection (Jersey) Law 2018

The Data Protection (Jersey) Law 2018 sets out the rights of individuals in respect of their personal data as well as the obligations and conditions organisations must follow to process it.

GDPR - General Data Protection Regulation 2018

This is the legislation covering data privacy in Europe. It protects personal data which can be described as:

"Any Information from which a person can be identified or potentially identified from."

Le Mourier has an obligation to ensure we are compliant with this regulation which follows 7 steps:

- Lawfulness, Fairness and Transparency - Only processing data as required by Law.
- Purpose Limitation - Only collecting data for legitimate means.
- Data Minimisation - Collecting no more data than is necessary.
- Accuracy - Making sure personal data is kept up to date.
- Storage Limitation - Only keeping personal data for as long as necessary.
- Integrity and Confidentiality - Protecting against data corruption, loss, and unauthorised access with use of appropriate preventative measures.
- Accountability - Following process and procedures to demonstrate compliance.

Data Protection Act 1998/Freedom of Information Act 2000

Any information which Le Mourier holds is potentially disclosable to a requester under one of these pieces of legislation. This includes emails.

ACTIVITY CAMPS

Users need to be sure that they are not breaching any data protection when they write and send emails. This could include but is not limited to:

- Passing on personal information about an individual or third party without their consent.
- Keeping personal information longer than necessary.
- Sending personal information to a country outside the EEA.

Email should, where possible, be avoided when transmitting personal data about a third party. Any email containing personal information about an individual may be liable to be disclosed to that individual under the Data Protection Act 1998. This includes comments and opinions, as well as information. Therefore, this should be borne in mind when writing emails, and when keeping them.

Computer Misuse Act 1990

This Act makes it an offence to try and access any computer system for which authorisation has not been given.

Appropriate Use of the Internet

Use of the Internet by employees is encouraged where such use is consistent with their work and with the goals and objectives of Le Mourier in mind. Reasonable personal use is permissible subject to the following:

- Users must not participate in any online activities that are likely to bring Le Mourier into disrepute, create or transmit material that might be defamatory or incur liability on the part of Le Mourier, or adversely impact on the image of Le Mourier.
- Users must not visit, view, or download any material from an internet site which contains illegal or inappropriate material. This includes but is not limited to pornography (including child pornography), obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling, and illegal drugs.
- Personal use of the internet must not cause an increase in significant resource demand, e.g., storage, capacity, speed or degrade system performance.
- Users must not “hack into” unauthorised areas.
- Users must not download commercial software or any copyrighted materials belonging to third parties unless such downloads are covered or permitted under a commercial agreement or other such license.
- Users must not use the internet for personal financial gain.
- Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- Users must not use the internet to send offensive or harassing material to other users.
- Use of the internet for personal reasons (e.g., online banking, shopping, information surfing) must be limited, reasonable and done only during non-work time such as lunchtime.
- Use of gambling sites and online auction sites is not permitted.

ACTIVITY CAMPS

- Personal Social networking sites such as, but not limited to, Facebook, LinkedIn, YouTube, Twitter, Snapchat, Flickr, Myspace etc. must be kept to a minimum and be kept in line with this policy.
- The use of Facebook by Admin Staff for the purpose of accessing the Companies Facebook Page & Accompanying Messaging Service is permitted.
- Staff may face disciplinary action or other sanctions (see below) if they breach this policy and/or bring embarrassment on Le Mourier or bring it into disrepute.

Remote Users

Users may sometimes need to use personal equipment and access the Company network while working remotely, whether from home or while travelling. The safe usage standards set out in this document apply to whether Company equipment and resources are being used.

Remote Networks

When working remotely users should refrain from using any Public Wi-Fi network, and if using one of these should not log in to any Le Mourier IT Facility (Such as Bookey or Microsoft 365). Public Networks are inherently riskier from attacks like Man in the Middle attacks, Cyber threats, or theft of personal information. Users should ensure that they are logging onto a credible WIFI network and wherever possible should use the Hotspot Function on a mobile 3G/4G device for any device not network enabled. Should users require access while abroad or outside of mobile network service a public / known Wi-Fi network may be required. In this case users should install a VPN (Such as ExpressVPN or NordVPN) and access Wi-Fi through this. Users should still bear in mind that sensitive information should only be accessed while using a Le Mourier Internet Facility.

Monitoring

All resources of Le Mourier, including computers, email, and voicemail are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of the normal business activity of the Company then, at any time and without prior notice, Le Mourier maintains the right to examine any systems and inspect and review all data recorded in those systems. This will be undertaken by authorised staff only. Any information stored on a computer, whether the information is contained on a hard drive, USB pen or in any other manner may be subject to scrutiny by Le Mourier. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists in the management of information systems.

Penalties for Improper Use

Users in breach of these regulations may have penalties imposed on them including, but not limited to, some of the following:

Restricted Access to Le Mourier IT Facilities

ACTIVITY CAMPS

Complete Withdrawal of Access to Le Mourier IT Facilities

Internal Disciplinary Action

Severe or Multiple Breaches of these regulations may be dealt with under Le Mourier's Disciplinary Procedures. It may lead to termination of employment from Le Mourier
Breaches of the Law, where appropriate these will be reported to the police.

Safe Email Usage

This section of Le Mourier's IT Infrastructure Policy relates to how all Full-Time, Part-Time, Seasonal or Student staff members safely interact with the company's Email Facilities. Le Mourier runs all Email communications through the platform Microsoft 365 (Outlook) and a few selected address' through 1and1 webmail (Mainly for use with Printers). Le Mourier hosts 3 main types of mailboxes which are distributed as required by the IT Administrator under the authority of the Director of Le Mourier, these mailboxes are:

User Mailbox's - These are directly linked with each user's account on the Microsoft 365 platform.

Shared Mailbox's - These are created by the IT Admin in process' where multiple staff members need to be involved with the distribution of work coming to one central Le Mourier Generic email address, such as info@lemourier.co.uk or charter@lemourier.co.uk

Calendar Mailbox's - These are created by the IT Admin for the sole purpose of providing a separate mailbox to utilise as a Shared Calendar. Permissions are given out based on Authorisation as mentioned below.

Authorisation

Permissions to any Le Mourier Mailbox, whether User, Shared or Calendar, are granted by the IT Administrator following authorisation from the Managing Director.

Should a user feel they require further authorisation they should speak with their Line Manager in the first instance. Should the Line Manager feel this is a suitable request this will then be put forward to the Managing Director and IT Administrator.

No person is allowed to use any Le Mourier Email Facility without being authorised to do so by the Managing Director or Line Manager. It is also important to note that Le Mourier's IT Administrators cannot apply any changes to permissions without first having the authorisation from the company's Managing Director.

Unauthorised access to email facilities is prohibited and may result in either restriction of access, disciplinary action or criminal prosecution.

Use of Email

Emails sent or received on the email system form part of the official records of Le Mourier; they are not private property. Le Mourier does not recognise any right of employees to impose restrictions on disclosure of emails within the Company. Emails may be disclosed under the Freedom of

ACTIVITY CAMPS

Information Act, as part of legal proceedings (e.g. tribunals), and as part of disciplinary proceedings. Users are responsible for all actions relating to their email account/pc username and should therefore make every effort to ensure no other person has access to their account.

When using Company email, users must:

- ensure they do not disrupt Le Mourier's wider IT systems or cause an increase for significant resource demand in storage, capacity, speed, or system performance e.g., by sending large attachment to many internal recipients.
- ensure they do not harm Le Mourier's reputation, bring it into disrepute, incur liability on the part of the Company, or adversely impact on its image.
- not seek to gain access to restricted areas of the network or other "hacking activities" is strictly forbidden.
- must not use email for the creation, retention, or distribution of disruptive or offensive messages, images, materials, or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs, or social background. Employees who receive emails with this content from other employees of Le Mourier should report the matter to their line manager or supervisor.
- not send email messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libelous or contain illegal or offensive material, or foul language.
- not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- not engage in any activity that is likely to
 - Corrupt or destroy other users' data or disrupt the work of other users.
 - Waste staff effort or Company resources or engage in activities that serve to deny service to other users.
 - Be outside of the scope of normal work-related duties – for example, unauthorised selling/advertising of goods and services.
 - Affect or have the potential to affect the performance of damage or overload the Company system, network, and/or external communications in any way.
 - Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights.

Staff who receive improper email from individuals inside or outside the Company should discuss the matter in the first instance with their line manager or supervisor.

Good Practice

Le Mourier has good practice guidelines for dealing with email when staff are out of the office for longer than three days. When activating the "out of office" facility messages should name an

ACTIVITY CAMPS

alternative member of staff for correspondents to contact if necessary. This will ensure that any important messages are picked up and dealt with within the required timescales.

During periods of absence when highly important emails are anticipated, the employee (or manager) should plan for notification and access by another appropriate member of staff.

Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender's knowledge. They may be read by people other than those they are intended for.

Users must exercise due care when writing emails to avoid being rude or unnecessarily terse. Emails sent from Le Mourier may be interpreted by others as Company statements. Users are responsible for ensuring that their content and tone is appropriate. Emails often need to be as formal and businesslike as other forms of written correspondence.

Email Concerns - Phishing or other Risk Associated Email

Le Mourier's Email system, hosted by Microsoft Office 365, has a robust and compliant Email filtering system which will automatically scan through incoming emails for any Spam, Phishing, or other Risk Factors. If found, these will be automatically sent to the facilities Junk Email Folder.

Users must only click on these emails if they are from a reputable source. Where there is any doubt surrounding the sender's address these should be immediately deleted.

However, caution should always be used when opening any attachments or emails from unknown senders that have arrived in the main Inbox folder. Users must best endeavor to ensure that any file downloaded from any email is done so from a reliable source. It is a disciplinary offence to disable any background system put in place to protect Le Mourier's IT Facilities, whether physical or remote.

Any concerns about external emails, including files containing attachments, should be discussed with the IT Administrator before opening or downloading any material.

Sending Emails - CC / BCC

There may be circumstances where users are required to send an email to multiple sources at once, such as emailing a class or group of customers. Users must be sure that when sending to multiple external customers that the email addresses are placed in the BCC (Blind Carbon Copy) option to ensure anonymity and protection of personal data is always kept. Where an internal email is sent then CC (Carbon Copy) is sufficient. Great care must be taken to use the correct option to ensure data is hidden from multiple external sources. Where a user has accidentally used the incorrect method (EG, sending as CC rather than BCC) this will constitute as a data breach and must be reported using the process in the "Data Breach" Section of this document.

Monitoring

All email resources of Le Mourier remain company property. At any point Le Mourier can delegate authorisation to any mailbox in the company, whether to investigate misuse, assist with workload or any other reason deemed necessary by the company's Managing Director. Where appropriate Le

ACTIVITY CAMPS

Mourier will inform users of this change in advance, however, reserves the right to take over a mailbox without prior notice.

Penalties for Improper Use

Users in breach of these regulations may have penalties imposed on them including, but not limited to, some of the following:

Restricted Access to Le Mourier IT Facilities

Complete Withdrawal of Access to Le Mourier IT Facilities

Internal Disciplinary Action

Severe or Multiple Breaches of these regulations may be dealt with under Le Mourier's Disciplinary Procedures. It may lead to termination of employment from Le Mourier Breaches of the Law, where appropriate, will be reported to the police.

Safe Usage of Portable Devices - Portable Devices (iPads / iPhones or other Tablets)

Each device will be set up by Le Mourier's IT Administrator and will be password protected with a unique password for that device. Users are not permitted to attempt to change any settings while in possession of the device. The password to such devices will only be provided to specific staff members, it is not permutable for any user to pass on password details without prior authorisation by the IT Administrator or Managing Director.

Once again while the device is in use it is the responsibility of the user to ensure the device is looked after.

- Ensuring the device is protected from damage while in transit.
- Ensuring the device is protected from any water damage (Such as keeping away from poolside as well as any kitchen or bathroom area)
- Ensuring the device and any additional components are kept clean (E.G charger) - Screen / Keyboard suitable wipes can be provided by the IT Administrator on request.
- Users must ensure the device is looked after while off site, any loss of device will incur breach procedures and potential internal investigations.
- Users are responsible for any costs associated with damage through misuse of the device.

Processor / Security Updates

Le Mourier will ensure regular updates will be rolled out across all devices as soon as practical following release from "Apple" or other regulatory body. To ensure this is completed, Le Mourier reserves the right to request any Device be brought in to the IT Administrator at any point. Le Mourier will make every effort to provide as much notice of this as possible, however in certain such cases this may not be possible and will require immediate response from the IT Administrator and User of the device, such event may include, but not limited to, an update because of a data or security breach which requires immediate action.

ACTIVITY CAMPS

Users themselves are not permitted to undertake such updates and require the assistance / authorisation from a Le Mourier IT Administrator. In cases where an IT Administrator deems it necessary, users may be requested to perform the update themselves. During this point the IT Administrator will talk the user through the process and must only happen with expressed authorisation from the Managing Director or IT administrator

Unexplained Events

Should a user suspect something unexplained is happening / has happened to a Le Mourier device, or indeed a personal device, they must contact an IT Administrator as soon as possible. Failure to do so may lead to a potential security or data breach which if not caught soon may lead to further damage to Le Mourier's or personal IT Facilities. It is important to note, in cases where an accidental breach has occurred, users will not be sanctioned should they come forward as soon as it is noticed. Failure to notify Le Mourier of a potential breach may lead to disciplinary action.

