# Email, Internet and Communications Policy

1. The Michael Lonsdale Group inclusive of (Michael Lonsdale Ltd, Michael J Lonsdale Ltd, Michael J Lonsdale (Electrical) Ltd and E7 Building Services Ltd, believe that it is important that all staff must read, accept and adhere to the information set out within this policy. This policy is essential in ensuring that as an organisation the security around our information, transactions and correspondence is maintained.

2. Our internet and email facilities are primarily provided to support Michael Lonsdale Group business activities. However, we do permit the limited personal use of these systems. Whether using these tools for business or personal purposes, you must adhere to the requirements described in this document.

3. When referring to our systems, the following are covered;
   - Email
   - Internet
   - Social networking
   - Michael Lonsdale Group social networking accounts
   - Unacceptable use of the Michael Lonsdale Group Systems
   - Monitoring
   - Security
   - Breaches of policy

Email

4. Email is a way in which we communicate with each other and our customers. When using email, it is essential to ensure whether business or personal, they are appropriate and would bear scrutiny.

5. Emails must not be used as a substitute for face-to-face communication. 'Flame emails' (emails that are abusive) can be a source of stress and damage work relationships. Hasty messages, sent without proper consideration, can also cause unnecessary misunderstandings. It is your responsibility to ensure that all emails sent by you, including forwarded or attached content will not cause offence to the recipients.

6. It is also important to consider the following things when using emails:

   - They should not be defamatory, discriminatory, contain inappropriate material.
   - Be in breach of confidentiality or any relevant contract, including the terms of your employment.
   - You must ensure that emails are sent only to the intended and relevant recipients, consider to whom you are sending emails.

- When sending an email, you have a responsibility to check email addresses and attachments before a message is sent to ensure that you are sending the correct information to the intended recipient.
- Inappropriate disclosure of information, for example sending sensitive personal data to the wrong recipient may result in disciplinary action and could lead to termination of contract.
- Your personal email account should not be used for Michael Lonsdale Group business purposes. Where company information is not in the public domain it should not be uploaded to, sent or forwarded from your personal email account.
- You must use your out of office assistant to indicate who will deal with your emails in your absence and specify your date of return.

7. It is also important to note that contracts can be set up by email and electronic messages can be legally binding. All emails have the possibility of release under the Freedom of Information or Data Protection Act.

8. In most cases the Michael Lonsdale Group, as well as the individual, would be held responsible for the content of electronic messages created and sent from its network.

9. If you receive an unsolicited message from an unknown source, you should immediately create a new email, add the message as an attachment and send it to the DHTS Help desk.

10. Inappropriate or excessive use of email for non-Group business activities will normally result in disciplinary action and could lead to termination of contract.

Internet

11. This section applies to internet browsing using company equipment whilst connected to the network or whilst offline (e.g., on your home broadband or a public wi-fi hotspot.) Personal use of the internet should not interfere or take priority over the performance of your normal working duties. Use should be infrequent, of short duration and be carried out as far as possible outside working hours (e.g., during lunch breaks).

12. Use of the internet at work should be lawful and users should take care that any websites visited would bear scrutiny. You should also not download any software that may be required for some websites. All requests for downloaded software must be made through the DHTS Help desk. Any use must be compatible with our dignity at work policy and our policies on diversity.

13. Inappropriate or excessive personal use of the internet will result in disciplinary action and could lead to termination of contract.

Social networking

14. If you use any sort of social networking site, you must not use your company e-mail as your contact e-mail or for logging on. (Unless you are using a social networking site to conduct Michael Lonsdale Group business, and this has been approved by your director.)

15. Don't say anything on these sites that you wouldn't be comfortable saying to your colleagues and line manager at work.

16. You must ensure that you do not breach confidentiality in anything you publish and ensure that the Michael Lonsdale Group is not associated with any images or comments that are inappropriate. Anything you do post must never include material that you have obtained during your work.

Michael Lonsdale social networking accounts

17. Do remember that, as a member of staff, if you comment on Group-related matters you may be perceived as a public representative of the Michael Lonsdale Group and your views can carry significant weight. They may well be interpreted as the company's official position, so please consider anything you post carefully.

18. Don't respond to provocation. Again, this may well be interpreted as our position. Not all comments on these sites will be kind but, like negative stories in the press, please don't give them too much weight. Anything you see of concern please do raise it with your manager.

19. Do remember that when you become a 'fan' on Facebook, other 'fans' may be able to view your profile (this could include colleagues at work and us as your employer), depending on your privacy settings.

Unacceptable use of Michael Lonsdale Group systems

20. The following activities would be unacceptable use of the Michael Lonsdale Group systems and would normally result in disciplinary action and could lead to termination of your contract:

    - Harassment, including, but not limited to; threats; statements of intimidation; derogatory comments, statements or messages relating to a person's religion, race, colour, ethnic origin, national origin, gender, age, sexual orientation, marital status, or disability.
    - Deliberate misuse of personal data or a serious breach of the Data Protection Act.
    - Intentionally impersonating or masquerading as another person without having consent from the person you are impersonating. For example, if you have access to a colleague's mailbox and calendars. You must only send out communications in their name where you have their permission to do so.
    - Attempting to gain unauthorised access to resources, mailboxes, files, services, etc.

- Any activity that takes a disproportionate amount of time away from normal work responsibilities.
- Any activity that could reflect unfavourably upon Michael Lonsdale Group's reputation, including the pursuit of illegal activities.
- Sending material in support of any business other than the Michael Lonsdale Group. This includes, but is not limited to, forms of solicitation or advertising.
- Sending material benefiting or promoting charitable, athletic, political, religious, or any organisation other than Michael Lonsdale Group.
- Expressing personal views inappropriate to a productive workplace or about subjects unrelated to the Michael Lonsdale Group.
- Using third party web-based applications or file sharing systems for the storage, sharing or processing of company material. Examples include Dropbox and iCloud. The DHTS Help desk can advise on appropriate methods of information exchange.
- Storing company information on a non-Michael Lonsdale Group device such as your own computer, laptop, tablet, USB memory stick or mobile phone. The DHTS Help desk can advise on appropriate methods of information storage.
- Browsing, downloading, sending, posting or forwarding any of the following:
  - Chain letters of any type.
  - Hoax emails.
  - Emails that are known to contain a virus.
  - Materials such as software or text, which may be subject to copyright, unless you are certain that the owner of the copyright has given permission.
  - Materials such as software, music, graphics, photographs, as attachments to e-mails. You must check with the DHTS Help desk if you are in doubt.
  - Large numbers of emails of non-business messages to groups or individuals.
  - Discriminatory, offensive, or pornographic material. Discrimination is defined in the Equality Act 2010. If you require any clarification about discrimination, please contact your manager.

Monitoring

21. Various monitoring, recording, filtering and other similar applications have been, or will be, used to maintain the integrity of the Michael Lonsdale Group systems and network. They will also be used to ensure compliance, where appropriate, with our corporate policies and the law (including, but not limited to, the Computer Misuse Act 1990, Data Protection Act 2018 and Equality Act 2010 as may be otherwise mentioned in this policy). Here are some examples of how monitoring will be used:

    - To identify or prevent inappropriate use of the Michael Lonsdale Group's email, internet and other information systems.
    - To prevent the introduction of viruses and other external threats.
    - To ensure that system performance is not affected by personal use.
    - To establish the details of transactions or other matters relevant to the business of the Michael Lonsdale Group.
    - To respond to a court order or a discovery request in relation to legal action.
    - To prevent or detect crime or serious breaches of the company's corporate policies.

- To ensure compliance with regulatory or self-regulatory practices and procedures relevant to the business of the Michael Lonsdale Group.
- To provide information relevant to legal proceedings, subject access or freedom of information requests.

22. We may monitor telephone, email and internet traffic data (i.e., sender, receiver, subject, non-business attachments to email, numbers called and duration of calls, domain names of websites visited, duration of visits and non-business files downloaded from the internet) at a network level (but covering both personal and business communications) for the purposes specified above.

23. The monitoring also includes monitoring chat and newsgroups, file downloads and reviewing server and workstation file contents. For the purposes of your maintenance of your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you. E.g., if you regularly visit websites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By carrying out such activities using the Michael Lonsdale Group's facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

24. In exceptional circumstances and where there is a business-critical issue, we may access your business communications during your absence, be it sickness, annual leave, or if necessary whilst you are visiting clients.

Security

Protecting the Michael Lonsdale Group and its customers/clients

25. There are three essential elements to effective security:

- Integrity: information should be complete, accurate and consistent.
- Confidentiality: information may be disclosed to authorised persons only.
- Availability: information should be available when required.

Your responsibility for security

26. Within the Michael Lonsdale Group IT systems there are several security controls. For example, network access is restricted by password to authorised users. To make these security controls work requires a full and personal commitment from all users. You must be:

- Informed: ensure that you understand and follow the security requirements defined in this policy.
- Responsible: do not attempt functions for which you have not been granted permission and do not introduce any unauthorised software.
- Vigilant: be alert to any security breach, or suspicious activity, and report it to your line manager and the DHTS Help desk immediately.

MICHAEL LONSDALE GROUP

Security guidelines

27. All users have a responsibility to ensure the security of the Michael Lonsdale Group information and systems. The following points are particularly important:

- Make sure you are aware of your individual responsibilities under the Data Protection Act as described in the Data Protection Policy. Your line manager can advise on the relevant policies and procedures relating to your specific role.
- If you receive computer files from an external correspondent on disk, CD or other external storage medium, you must contact the DHTS Helpdesk to arrange for it to be checked before it can be transferred to our network.
- Subject to the above, users should not request or accept personal data provided on portable media. Please speak to DHTS Help desk colleagues who will advise on a safe means of transferring or accessing the information.
- Clear your desktop of any sensitive information when you no longer need it.
- Do not leave sensitive information in printer trays, on photocopiers, fax machines or on desktops.
- Never save your password to any IT system.
- Never share passwords or disclose them to a third party including your colleagues. Access to systems is granted to individuals. This is important both to limit who can do what, and to know who did what. There are alternatives to sharing passwords which you can discuss with DHTS Help desk colleagues.
- Lock your screen each time you step away from your desk.
- At the end of each day, log off or shut down your computer as appropriate. This is important to ensure software security patches are deployed to your computer.
- Be prepared to act if you notice anything suspicious or actions likely to place systems or information at risk.
- As part of their day-to-day duties' managers should ensure that these guidelines are being followed by colleague's they have management responsibility for.

Breaches of policy

28. This is a statement of the Michael Lonsdale Group's current policy. It is under constant review and when changes are made, they will be communicated to all employees. You have a duty to keep up to date. Failure to comply with the requirements of this policy may result in disciplinary action up to and including dismissal, civil or criminal proceedings or a combination of both.

MICHAEL LONSDALE GROUP

Name: Gary Herbert

Signature:

For and on behalf of the
Michael J Lonsdale Group Board of Directors
(Michael J Lonsdale Limited/ Michael J Lonsdale (Electrical) Limited
E7 Building Services Limited

Position Managing Director

Date: 31st July 2022