Making holidays accessible

Email Acceptable Use Policy

Introduction

The Lyneal Trust encourages use of email where it supports the aims and objectives of the Trust. It is essential that when emailing as a trustee, officer, contractor or volunteer the content complies with current legislation and relevant Trust's policies and procedures and does not create unnecessary business risk for the Trust.

Risk Management

Email is a business communication tool and users are obliged to use email in a responsible, effective and lawful manner. Although, by its nature email seems to be less formal than other written communication, the same laws apply.

The Trust therefore recognises that there are risks associated with the use of email and the extensive damage that can be caused by:

- Sending or forwarding emails, including an attachment, with any libellous, defamatory, offensive, racist or obscene remarks.
- Unlawfully forwarding confidential information.
- Unlawfully forwarding or copying messages without permission.
- Sending or forwarding an attachment that contains a virus.

This policy aims to ensure appropriate use of email and to help mitigate the following risks:

- Harm to individuals.
- Damage to the Trust's reputation.
- Potential legal action and/or fines against the Trust or individual(s).

If any user disregards the rules set out in this policy the user will be fully liable and the Trust will disassociate itself from the user as far as legally possible.

Scope

This Policy applies to all trustees, officers, contractors, and volunteers of the Trust.

Email Content

Email messages may be disclosed under the General Data Protection Regulation, or in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered; email messages should be treated as potentially retrievable, either from the main server or using specialist software. Users should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Users should assume that email messages may be read by others and not include anything that would offend or embarrass any reader, or themselves, if it found its way into the public domain.

Legal Requirements

The following rules are required by law and are to be strictly adhered to:

- It is strictly prohibited to send or forward emails containing libellous, defamatory, offensive, racist or obscene remarks. If an email of this nature is received, promptly notify the Secretary.

- Do not forward a message or attachment without acquiring permission from the sender first (This applies to mail received from a third party being forwarded to another third party.)
- Do not send unsolicited email messages whereby you would be invading someone's privacy.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's email account.
- Do not send a copy of a message or attachment belonging to another user without permission of the originator
- Do not disguise or attempt to disguise your identity when sending email.

Data Protection Issues

Personal data is subject to the Data Protection Act 1998 and from 25 May 2018 the General Data Protection Regulations. Under the terms of the Act and Regulations, personal data includes any information about a living identifiable individual, including their name, address, phone number, email address and any other information about the individual. If such information is included in an email or an attachment to an email, a user is deemed to be "processing" personal data and must abide by the law. In particular, a user must not collect such information without the individual knowing what the user's proposes to do with such information. Such information may not be disclosed or amended except in accordance with the purpose for which the information was collected. The user must ensure the information is accurate and up to date. In addition, the individual has the right to inspect what is held about him or her on the email system, or held in separate archives of emails. The individual can demand correction of inaccurate information, can request blocking or erasure of damaging information, and can sue for damage caused by inaccurate information.

The law also imposes rules on storing of personal data. Such data should be kept only for as long as it is needed for the purpose for which it was collected. If a user maintains their own stores of emails, they should ensure that such stores are not maintained for longer than is necessary for the purpose for which they were collected. Emails should be held in such a way that they can be easily identified, reviewed and when necessary, destroyed.

Best Practices

The Trust considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Therefore, the Trust wishes trustees, officer, contractors and volunteers to adhere to the following guidelines when emailing on behalf of the trust:

Distribution:

- Using 'bcc' should be considered if recipients have not authorised their email addresses to be shared.
- Use 'to' as standard as it can be helpful to know who else has received the email.

Writing emails:

- Write well-structured emails and use short, descriptive subjects.
- The Trust's email style is informal. This means that sentences can be short and to the point.
- For external emails signatures must include your name, role, Trust name and phone number. Signatures are not necessary for internal e-mails.
- Use the spell checker before you send out an email.
- Do not send unnecessary attachments.
- If you forward emails, state clearly what action you expect the recipient to take.
- Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password.
- Only mark emails as important if they really are important.

Replying to emails:

- Emails should be answered within the same time scale afforded to other forms of communication .
- Consider whether 'reply to sender' is more appropriate than 'reply to all'.