LIONHEART
EDUCATIONAL
TRUST

ELECTRONIC COMMUNICATIONS POLICY

This policy applies to all schools in The Lionheart Educational Trust

Approved by Trust Board:

September 2024 - September 2026

Contents

1.0 Introduction

1.1 Lionheart Educational Trust ("the Trust") provides email facilities to authorised users as a communications channel for Trust business purposes only.

1.2 The Trust recognises that there are numerous risks associated with the use of email as a communications platform, which could lead to personal data breaches or cyber-attacks if used inappropriately; the consequences of which could be severe and long lasting to the Trust, to staff and to data subjects.

1.3 All authorised users of the Trust email platform must be aware that:

- emails generated and processed through the Trust email platform are the property of the Trust;
- the content of an email is potentially disclosable in response to an information request or subject access request;
- the email platform is not to be used storage location for 'business records' which represent records of the Trust's actions and decisions.

2.0 Purpose

2.1 The purpose of this policy is to ensure that all authorised users of the Trust email platform understand the potential risks and their responsibilities for how to use this platform securely and appropriately.

2.2 It is a condition of access that authorised users abide with this policy when using the email facilities.

3.0 Scope

3.1 This Electronic Communications Policy applies to all staff and other authorised users, including students and contractors, who are provided with access to a Trust email account.

3.2 The Trust may consider action, in accordance with the Trust's Disciplinary Procedure, where users knowingly and deliberately contravene this policy. Additionally, if an individual's conduct or actions are illegal the individual may become personally liable.

4.0 Roles and Responsibilities

4.1 Authorised users are responsible for using the email facilities provided in accordance with this policy and for reporting any incidents or data breaches without delay.

4.2 Managers are responsible for ensuring staff within their area of management are informed of and adhering to this policy.

4.3 The IT Department are responsible for providing and maintaining central email systems, and for ensuring the ongoing security of the email platform.

5.0 Conditions of Use

5.1 Email facilities are provided to support the business activities of the Trust, including the delivery of teaching and learning and the general management of school and Trust business.

5.2 All emails are subject to Freedom of Information and Data Protection legislation, and may be subject to public disclosure or as part of a subject access request. This also applies to all instant messaging platforms used for work purposes.

5.3 Statements must not be made that could expose the Trust to legal liability or damage its reputation.

5.4 In order to present a consistent and professional image all staff are expected to adhere to corporate guidelines when creating their email signature.

5.5 In cases of planned absence, staff must set up an out-of-office email message giving alternative contact details to ensure that enquiries can be answered promptly.

5.6 Where approved by the Head of School or a member of the senior leadership team, delegated access to an email account may be granted, so that messages can be checked in cases of staff absence/illness.

5.7 Emails are records of the Trust's actions and decisions, and must be managed as efficiently as paper and other electronic records. It is the responsibility of all staff to ensure that messages with continuing value are saved into the appropriate corporate system.

5.8 Users must regularly review their emails to ensure that those that have served their purpose are deleted from the system.

5.9 Reasonable personal use of Trust individual email accounts is allowed as long as it does not impact on your work. These messages should be labelled 'Personal' in the subject line.

5.10 Staff are not permitted to use Trust email accounts to sign up for personal accounts on websites.

6.0 Security

6.1 Whilst emails are routinely scanned for virus content and spam, account holders must remain vigilant and to challenge any emails that appear suspicious. These include:

- not opening attachments received from unknown or untrusted sources;
- not opening links received from unknown or untrusted sources;
- not transmitting attachments known to be infected with a virus;
- ensuring that antivirus/anti-spyware software is installed and maintained on any personal device used to gain access to the Trust's IT facilities.

6.2 Staff must lock their workstations (windows key+L on a Windows PC) when away from their desk, even for short periods. Computers which cannot be locked must not be left unattended whilst logged-on.

6.4 The automatic forwarding of emails is prohibited except in exceptional circumstances.

6.4 It is the responsibility of the email sender to:

- Always re-check the recipients of an email message before sending, particularly when the email contains confidential or personal information

- Send links to documents where these contain personal data, for example: links to documents contained on the network drive or OneDrive. This will prevent the document being accessible to unauthorised individuals should the email be sent to the wrong recipient

- Where it is necessary to email an attachment containing personal data, ensure that the attachment is password protected

- Do not include personal data in the subject line of an email
- Encrypt all email sent to external recipients that contain personal data, and consider the use of 'Do not forward' where this is appropriate
- Ensure that emails are sent 'BCC' where it is necessary to protect the identity of other recipients in the same email. BCC should always be used when emailing parents
- Do not use email distribution lists to share personal data.

6.5 It is the responsibility of the email recipient to:

- delete emails containing personal data once these have been saved to the appropriate storage location, and/or are no longer needed
- To notify the sender of an email if personal data has been shared inappropriately, for example, you are not the intended recipient, or the personal data has been shared in a way that contravenes this policy
- Report any data breach immediately to the Data Protection Team.

7.0 Retention

7.1 Mailboxes for staff who leave the Trust will be deleted one year after they leave the organisation unless otherwise authorised.

7.2 Emails contained in archive are maintained for the purposes of disaster recovery only and will not be subject to disclosure in the event of an information request.

7.3 Emails that are deleted will be permanently deleted from the deleted folder after 30 days and will no longer be accessible.

8.0 Emails to Parents and Carers

8.1 All mass electronic communications to parents should only be sent via Trust approved communication systems. These are:

- Beehive
- MailOut
- Truancy Call / Keep Kids Safe (RS Connected)

8.2 Only Staff trained to use the application should configure the system for a communication.

8.3 Where group emails must be sent, they must be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

9.0 Personal Data Breaches and Security Incidents

9.1 The IT Service Desk should be informed immediately, if a suspected virus is received or a user becomes aware that someone has gained unauthorised access to their account, or potentially obtained their personal details (e.g. disclosed via a phishing attack).

9.2 The Data Protection Team must be informed immediately, and without delay, in the event that a data breach, or suspected data breach has occurred.

10.0 Incident Handling and Data Protection

10.1 The Trust reserves the right to monitor emails sent and received relating to Trust business in accordance with the Regulation of Investigatory Powers Act 2000, the Data Protection Act 2018 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

10.2 The IT Team will carry out proactive monitoring to scan for phishing emails.

10.2 The Trust will investigate all complaints received from both internal and external sources, about any unacceptable use of email that involves Trust facilities. Where there is evidence of an offence it will be investigated in accordance with the Trust's disciplinary procedures applicable to all members of staff.

11.0 Related policies

11.1 Users should read this policy in conjunction with other Trust policies including:

- Data Protection Policy
- Social Media Policy
- IT Security Policy
- Acceptable Use Policy [Staff]

12.0 Review

12.1 This policy will be reviewed periodically as it is deemed necessary to ensure that it remains appropriate and up to date. These reviews will be no less frequently than every two years. The policy review will be undertaken by the Head of IT.