



LIONHEART
EDUCATIONAL
TRUST

ELECTRONIC COMMUNICATIONS POLICY

**This policy applies to all schools in
The Lionheart Educational Trust**

Approved by Trust Board:

September 2026 - September 2028



Contents

1.0	Introduction	3
2.0	Purpose	3
3.0	Scope.....	3
4.0	Roles and Responsibilities.....	3
5.0	Conditions of Use	4
6.0	Security	5
7.0	Retention	6
8.0	Emails to Parents and Carers	6
9.0	Personal Data Breaches and Security Incidents.....	6
10.0	Incident Handling and Data Protection.....	7
11.0	Related policies	7
12.0	Review.....	7



1.0 Introduction

- 1.1 Lionheart Educational Trust ("the Trust") provides electronic communication systems and facilities to authorised users for the purpose of conducting Trust business. Use of these systems is permitted only in accordance with this policy and for authorised educational, operational, and administrative activities undertaken on behalf of the Trust.
- 1.2 For the purposes of this policy the term 'electronic communication systems' refers to any electronic system that can be used to communicate with any other person including but not limited to Email, Microsoft Teams, Mailout and Text (SMS) messages.
- 1.3 The Trust recognises that there are numerous risks associated with the use of electronic communication platforms, 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.
- 1.4 All authorised users of communication platforms provided by the Trust must be aware that:
 - Electronic communication messages and other content generated or processed through Trust communication platforms are the property of the Trust;
 - The content of electronic communication messages may be disclosable in response to an information request, subject access request, investigation or legal process;
 - Electronic communication systems must not be used as the sole storage location for business records representing the Trust's actions and decisions.

2.0 Purpose

- 2.1 The purpose of this policy is to ensure that all authorised users of Trust electronic communication platforms understand the potential risks and their responsibilities for how to use these platforms securely and appropriately.
- 2.2 It is a condition of access that authorised users abide by this policy when using any Trust electronic communication system.

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 communication platform account.
- 3.2 The Trust may consider action, in accordance with the Trust's Disciplinary Procedure, where users knowingly and deliberately contravene this policy. In addition, where an individual's actions are unlawful, they may be held personally liable and may be subject to criminal or civil proceedings.

4.0 Roles and Responsibilities

- 4.1 Authorised users are responsible for using the electronic communication 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 adhere to this policy.



- 4.3 The IT Department are responsible for providing and maintaining electronic communication systems, and for ensuring the ongoing security of all platforms.

5.0 Conditions of Use

- 5.1 Electronic communication 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 Electronic communications may be subject to disclosure under data protection, freedom of information, regulatory, legal or audit requirements. This applies to emails, Teams messages and other communications created or stored on Trust systems.
- 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 and safeguarding risks mitigated.
- 5.6 In exceptional circumstances, such as staff absence or illness, delegated access to an employee's email account may be granted where there is a clear business need. Any such access must be authorised by both the Executive Head Teacher and the Chief Operating Officer and will be limited to the extent necessary to meet that need.
- 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 Limited personal use of Trust email accounts is permitted where it is reasonable, infrequent, and does not adversely affect work performance, network resources, or the reputation of the Trust.
- 5.10 Staff must not use Trust email accounts to create, maintain, or receive communications relating to personal online accounts, memberships, subscriptions, or services that are not connected with Trust business.
- 5.11 Trust electronic communication systems must only be accessed using Trust-provided accounts. Users must not conduct Trust business using personal email or personal communication accounts unless expressly authorised by the Trust.
- 5.12 Teams, channels, private channels and shared channels must have a clear business purpose, an appropriate owner and membership limited to those who require access.
- 5.13 Staff who create or own a Microsoft Team are responsible for managing its membership and permissions. Owners must ensure that access remains appropriate, remove members who no longer require access and review guest or external access regularly.



- 5.14 External or guest participants must only be added where there is a legitimate business requirement and the user has confirmed that the chat, meeting, team or channel is suitable for external access.
- 5.15 Before posting or sharing information in Teams, users must check the audience, channel membership, meeting participants and file permissions. Confidential, safeguarding, special category or other sensitive personal data must only be shared using an approved method and with access restricted to authorised recipients.
- 5.16 Significant decisions, approvals and actions discussed within Teams must be recorded or retained within the appropriate corporate, educational, safeguarding, HR, finance or records management system where required.
- 5.17 Meeting organisers must consider whether recording or transcription is necessary and appropriate. Participants must be informed when recording or transcription is enabled, and access to resulting recordings, transcripts and meeting artefacts must be restricted appropriately.

6.0 Security

- 6.1 Whilst emails are routinely scanned for virus content and spam, account holders must remain vigilant and challenge any emails that appear suspicious. These include:
- not opening attachments received from unknown or untrusted sources;
 - not launching links received from unknown or untrusted sources;
 - not transmitting files known or suspected to contain malware;
 - ensuring that antivirus/anti-spyware software/latest security updates are installed and maintained on any personal device used to gain access to the Trust's electronic communication systems.
- 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.
- 6.3 The automatic forwarding of emails is prohibited except in exceptional circumstances and may only be configured by the IT Department following approval from the Head of IT.
- 6.4 It is the responsibility of the sender electronic communications to:
- Always re-check recipients, chat participants and channel membership before sending or posting, particularly where the communication contains confidential or personal information
 - Send links to documents instead of attachments where these documents contain personal data.
 - Password protect any email attachment containing personal data
 - Not include personal data in an email subject line, Teams post title, meeting title or channel name
 - Encrypt all email sent to external recipients that contain personal data, and consider the use of 'Do not forward' where this is appropriate
 - Use BCC where an email is sent to multiple parents or carers who do not need visibility of each other's contact details.
 - Not use email distribution lists to share personal data.



- Not install or authorise Teams applications, bots, connectors or integrations unless approved by the IT Department.
- Not create externally shared teams, channels or meetings for sensitive information unless the external collaboration has been authorised and access controls have been verified.
- Report suspicious Teams messages, unexpected meeting invitations, unauthorised participants or unexpected changes to team or channel membership to the IT Service Desk.

6.5 It is the responsibility of recipients of electronic communications to:

- delete communications containing personal data once they have been saved to the appropriate storage location and are no longer needed, subject to retention requirements and any applicable hold
- notify the sender if personal data has been shared inappropriately, for example where the recipient was not intended or the information was 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 backup and archive systems are maintained primarily for business continuity and disaster recovery purposes and are not intended to serve as active record repositories.
- 7.3 Emails that are deleted will be permanently deleted from the deleted folder after 30 days and will no longer be accessible.
- 7.4 Teams chats, channel messages, meeting chats, recordings, transcripts and files are subject to the Trust's approved retention arrangements. Users must not assume that deleting content from Teams removes all copies or records.

8.0 Emails to Parents and Carers

- 8.1 All mass electronic communications to parents should only be sent via Beehive which is the Trust's approved parental communication system.
- 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.
- 8.4 All electronic communications to parents and carers must follow Trust guidelines for tone and content at all times.

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 (as amended by the Data (Use and Access) Act 2025), and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Monitoring will only be undertaken where lawful, proportionate and necessary for legitimate business, security, safeguarding, regulatory or investigative purposes.
- 10.2 The IT Team will carry out proactive monitoring to scan for phishing emails and threats.
- 10.3 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]
 - Recording Policy

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 and approved by the Chief Operating Officer.