General Data Protection Regulations (UK GDPR) Email Policy

DOCUMENT PROVENANCE			
Status	Draft	Current version no.	1.0
Organisation	NCC/NST	Version date	October 2025
Author	Jeremy Lyn-Cook/NST	Approved by (If applicable)	
Audience	Dunkirk staff, volunteers and visitors	Approval date	October 2025
Security classification	OFFICIAL	Next review date	Annually

DOCUMENT CHANGE HISTORY			
Revision date	Version no.	Author of changes	Summary of changes

Contents

Email Policy

1. Introduction

1.1 Email is an almost universal means of communication. It is often the primary communication and awareness raising tool within an organisation. Whilst email provides many benefits, the misuse of email poses security, privacy and legal risks. So it is important that users understand how to use it appropriately within the Dunkirk Primary School environment.

2. Purpose

2.1 The purpose of this policy is to ensure the proper use of the Dunkirk Primary School email system and make users aware of what Dunkirk Primary School considers to be acceptable and unacceptable use. This policy outlines the minimum requirements for use of email within the Dunkirk Primary School network.

3. Scope

This policy covers appropriate use of any email sent from an Dunkirk Primary School email address and applies to all employees, vendors and agents operating on behalf of Dunkirk Primary School.

4. Policy

- All use of email must be consistent with Dunkirk Primary School policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices. For details relating to encryption please visit; https://schuk.sharepoint.com/sites/schoolsit/gdpr

- Dunkirk Primary School email accounts should be used primarily for Dunkirk Primary School business-related purposes; personal communication is allowed on an occasional basis, but non- Dunkirk Primary School related commercial uses are prohibited.

- All Dunkirk Primary School data contained within an email message or an attachment must be secured in accordance with the provisions for protecting personal data in line with GDPR 2017 and the Data Protection Act 2018.

- Email should be retained if it qualifies as an Dunkirk Primary School business record, i.e. if there is a legitimate and ongoing business reason for maintaining the information contained in the email.

- The Dunkirk Primary School email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about age, gender, race, disability, sexual orientation, religious beliefs and/or practice, political beliefs or nationality. Employees who receive any emails containing this type of content from any Dunkirk Primary School employee should report the matter to the Head Teacher immediately.

- Users are prohibited from automatically forwarding Dunkirk Primary School email to a third party email system (noted below). Individual messages which are forwarded by the user must not contain Dunkirk Primary School confidential or the above information.

- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail, etc. to conduct Dunkirk Primary School business, to create or record any binding

transactions or to store or retain email on behalf of Dunkirk Primary School. Such communications and transactions should be conducted through proper channels using XXX approved documentation.

- Occasional use of Dunkirk Primary School resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke related emails from an Dunkirk Primary School email account is prohibited.

- Dunkirk Primary School employees shall expect only limited privacy in respect of anything they store, send or receive on the XXX email system.

- Whilst Dunkirk Primary School reserves the right to monitor messages without prior notice, it is not obliged to monitor email messages.

5. Policy compliance

On an ad hoc basis the Dunkirk Primary School Head Teachers may authorise verification of compliance to this policy through various methods, including but not limited to periodic walkthroughs around the buildings, business tool reports, internal and external audits, staff surveys, etc.

6. Exceptions

Any exception to the policy must be recorded and approved and recorded by the Head Teacher in advance.

7. Non-compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8. Related policies and processes

This Policy should be read in conjunction with the following:

Data Protection Policy
Data Incidents and Breaches Policy
Freedom of Information Policy
Acceptable Use Policy
Remote Access and Mobile Computing Policy
Subject Access Request Policy
Mobile Computing Policy
Safeguarding Policy and Guidance