



General Data Protection Regulations (UK GDPR)

Nottingham Schools Trust Email Policy

October 2025

Email Policy

Contents

1. Introduction
2. Purpose
3. Scope
4. Policy
5. Policy compliance
6. Exceptions
7. Non-compliance
8. Related policies and processes
9. Review

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 Nottingham Schools Trust environment.

2. Purpose

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

3. Scope

This policy covers appropriate use of any email sent on behalf of MELLERS either from an MELLERS email address or from a personal address which has been accepted for use for MELLERS business, and applies to all “employees” (staff, consultants, vendors and agents working or operating on behalf of MELLERS).

4. Policy

- All use of email must be consistent with MELLERS policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- MELLERS email accounts should be used primarily for MELLERS business-related purposes; personal communication is allowed on an occasional basis, but non-MELLERS related commercial uses are prohibited.
- All MELLERS 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 MELLERS business record, i.e. if there is a legitimate and ongoing business reason for retaining the information contained in the email.
- Email identified as an MELLERS business record will be retained in accordance with MELLERS’s Retention Schedule.
- The MELLERS 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 MELLERS employee should report the matter to the CEO immediately.

- Users are prohibited from automatically forwarding MELLERS email to a third party email system (noted below). Individual messages which are forwarded by the user must not contain MELLERS confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail, etc. to conduct MELLERS business, to create or record any binding transactions or to store or retain email on behalf of the MELLERS. Such communications and transactions should be conducted through proper channels using MELLERS approved documentation.
- Occasional use of MELLERS 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 MELLERS email account is prohibited.
- MELLERS employees shall expect only limited privacy in respect of anything they store, send or receive on the MELLERS's email system.
- Whilst the MELLERS 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 MELLERS's CEO 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 by the MELLERS's CEO in advance.

7. Non-compliance

Any 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

- Data Protection Policy
- Freedom of Information Policy
- IT Acceptable Use Policy

9. Review

This policy will be reviewed in October 2026 and then annually thereafter

