



Email and Communications Protocol Policy (Ref 49 MPTEM)



Mosaic Partnership Trust

Email Protocol and Communications Protocol Policy (Ref 49 MPTEM)



Email and Communications Protocol Policy (Ref 49 MPTEM)

History of most recent changes

Version	Date	Page	Change	Origin of Change
V1.0	16/06/2024	Whole Document	Adoption by the Mosaic Partnership Trust and Implementation	New Academy Trust early agreement on protocols for email and social media groups
V1.1	16/07/2024	Page 5	Simplification of What's App section around Trust held data and information.	ARC Meeting feedback on protocol
V1.2	19/03/2025	Whole Document additions	Adding further clarification on email expectations, including school closure periods. Further detail on Trust expectations on the use of 'What's App'	Reflection on the first year of the protocol in action and what needed to be clarified or changed.
V1.3	15/06/2026	Page 5	Includes a reference to AI in the context of emails.	To align with the Trust AI Policy
V1.4	24/08/2026	Whole Document	Updated to become a policy document, with specific reference and links to acceptable use.	To move from a protocol to a policy.



Email and Communications Protocol Policy (Ref 49 MPTEM)

1.0 Overview

The policy sets out the email and communication protocols for staff across the Mosaic Partnership Trust (MPT).

Whilst emails are a valuable form of communication, **unnecessary emails add to staff workload and inappropriate use of emails can cause reputational damage to the organisation.**

This policy is designed to make emails manageable for staff by reducing the number of unnecessary emails and setting common parameters to improve their use. In an era where digital communication is ubiquitous, it's also imperative for schools to be vigilant about the platforms staff may use and the manner in which they're used, so the policy also covers 'WhatsApp' in some advisory notes at the end of the document.

We are expecting **ALL** staff to follow this policy across our Trust schools, with the aim of reducing inadvertent unnecessary workload, to ensure that we comply with data protection and to protect the organisation (MPT) from reputational damage.

All Trust email accounts, email addresses and associated IT systems are provided for authorised Trust business and remain under the control of the Trust. Information and communications created, sent, received or stored using Trust systems may constitute Trust records and may be subject to the Trust's information governance, records retention and data protection requirements.

2.0 Emails

Key questions before sending an email

1. Is this email necessary?
2. Is this a purely work-related email?
3. Is email the right way to communicate the message?
4. Is this email one of many for the recipient today, if it is – is there anyway this could be condensed into a single email?
5. Do I need a reply? If so, it can be helpful to add to the message **Response Required**. If it is for information, then add **For Information Only** and if it is urgent mark **Urgent** (this is only for matters that need immediate attention and should only be used in this context). If urgent it maybe that other forms of communication may also be required such as a telephone call or text message. The word Urgent should only be used for Urgent matters.
6. Have you checked the email is going to the email address of the intended recipient, and not another email address that Outlook has automatically filled in?
7. Have you considered who you are copying in and whether they need to be copied in?
8. Have you used the 'Blind copy - Bcc field' when emailing groups of parents and carers, so that personal email addresses are not shared?
9. If sending a group email, or replying to a group email, **do I need to send this to everyone in the group?** Is it clear in the text of the email that a reply to all is required, if not, this should be avoided.



Email and Communications Protocol Policy (Ref 49 MPTEM)

10. If you are forwarding a message, have you taken into account whether the email needs to be forwarded but also the email thread?
11. Have you checked your email content against the audience? Have you checked grammar, spelling and punctuation? Have you considered the tone?

Remember, email messages could be subject to a Freedom of Information and/or a Subject of Access request. Content from an email could also be used in the context of a Complaint, Grievance, Disciplinary or Whistleblowing investigation.

MPT Email Expectations

- People should feel able to send emails when their working patterns suit them but with the caveats below around the working week, working day and school holiday periods.
- Part-time staff are not expected to check, read or respond to emails on their non-working days.
- No-one should expect anyone to reply immediately, and the Trust approach is that responses should normally be provided within 3 working days of receipt.
- Staff may choose to work outside of their working hours but **any emails sent must be sent using the Delay Delivery function within Outlook (Options – Delay Delivery) so that emails are automatically sent during ‘operational hours’ (‘operational hours’ would be Monday to Friday between 8:00am to 6:00pm)** with the exception of any email that is **urgent**, which should also be marked urgent in the Header.
- Schools in the holiday period will need to provide a named contact in the context of matters of either importance or urgency – usually the Headteacher in the first instance but to protect their entitlement to a holiday, there should be another named person in their absence. The dates when either the Head or other contacts are available should be shared with the Trust Governance and Clerking Professional before each half-term or respective Christmas, Easter and Summer Holiday.
- The Trust central team in the holiday period will need to provide a named contact in the context of matters of either importance or urgency – usually the Chief Executive Officer (CEO) the first instance but to protect their entitlement to a holiday, there will also be another named person in their absence. The dates when either the CEO or other contacts are available will be shared with school leaders before each half-term or respective Christmas, Easter and Summer Holiday periods.
- Across the Trust, no one has to respond to emails or write an email at weekends or after 6.00pm.
- Individuals can check their emails when they choose. It is best practice to check them at least once every working day.
- Staff should respond to emails within 3 days during their working week where a request for a response has been made. Some staff may have mutual understandings between themselves of the best time to check and respond to emails- this is not prescriptive.
- Excessive emails from parents or other staff members should be brought to the attention of the line manager, Headteacher or CEO. Staff can use holding



Email and Communications Protocol Policy (Ref 49 MPTEM)

emails if needed when dealing with sensitive and / or emotive issues or where some investigation is needed.

- Where a request has not been made for a response, there is no need to reply. Senders will assume that the contents have been read.
- “All Staff” emails should only be used sparingly, and staff should avoid a ‘Reply All’ response
- Out of Office can be used by staff on a non-working day or when they are out of school or the office. There should not be the necessity to put out of hours on at the weekend, as these are non-working days for the Trust.
- Out of Office can also be used during school holiday period.
- The Trust Central Team and schools should consider the use of a bulletin or similar tool rather than separate emails as the main form of communication for non-sensitive information that needs wide distribution.
- Large files shouldn’t be attached to emails as this slows the system. Consideration of the types and numbers of attachments should be made
- Avoid sending short emails with single links if this can be covered in a longer email.
- Avoid sending emails with a link or using FYI unless absolutely necessary. Any emails that share a link should have the link content summarised before being shared and consideration needs to be given on both the importance and relevance.
- Always check the email thread before forwarding in case it contains confidential information.
- Employees should consider removing email alerts from their mobile phones and smart watches unless this helps with their work life balance.
- AI Co-Pilot only in the context of support the generating of an email. Any use of AI must be in line with the Trust AI Policy.
- **Staff must not use emails for non-work-related matters**
- **Staff must not use Trust email addresses for non-work-related subscriptions**
- **Nothing should be sent to employees personal email addresses**

Staff should report any emails that are sent to the wrong recipient(s) as soon as possible to the Data Protection Officer (Judicium) who will advise on further action.

Remember, email messages could be subject to a Freedom of Information and/or a Subject of Access request. Content from an email could also be used in the context of a Complaint, Grievance, Disciplinary or Whistleblowing investigation.

3.0 WhatsApp Groups

Personal ‘WhatsApp’ or ‘other platform’ accounts are not to be used for sharing Mosaic Partnership Trust organisational data under any circumstances. This encompasses student data, staff information, or any other confidential school or Trust related details.



Email and Communications Protocol Policy (Ref 49 MPTEM)

As a Trust we advise against using 'What's App' as a tool for any formal Trust or School communication and discussion between staff, we advise using MS Teams for this.

Remember, WhatsApp messages could be subject to a Freedom of Information and/or a Subject of Access request. Content from 'What's App' could also be used in the context of a Complaint, Grievance, Disciplinary or Whistleblowing investigation.

4.0 Critical Incident or Urgent Response Email

There may be times when a school is subject to a critical incident or a matter that needs an urgent response such as:

- Any Critical Incident
- Cyber/IT Security Breach
- Closure due to snow, fire, flooding
- A safeguarding incident
- A health and safety incident
- A health-related incident
- Bereavement

In these circumstances where an urgent communication is needed the most appropriate forms of communication are telephone and email in the first instance and an alert (only) via text. Text messages if used should be brief and not contain any personal information. Please also refer to the Trust Business Continuity Plan which also covers how to manage Critical Incidents.

All Heads need to provide their emergency contact details to the Governance Clerking Professional and that of a second competent person if they are not available. The central teams contact details are published termly including email and mobile telephone number.

5.0 Trust processes to ensure acceptable use

The trust reserves the right to monitor the use of its email systems and other IT facilities where this is necessary, proportionate and lawful in line with the Trust IT Acceptable Use Policy. Monitoring may include email traffic, metadata, usage information and, where justified, and in accordance with applicable law and Trust policies, the content of communications.

Monitoring may be undertaken for purposes including, but not limited to, safeguarding, maintaining system and information security, protecting confidential information, preventing or detecting unauthorised or unlawful activity, ensuring compliance with Trust policies and/or legal/regulatory obligations, investigating suspected misconduct, and supporting the effective operation of Trust systems.

Users should therefore have no expectation of complete privacy when using Trust email accounts or IT systems. However, the Trust will only access or monitor information where such monitoring is necessary and proportionate.



Email and Communications Protocol Policy (Ref 49 MPTEM)

To ensure acceptable use, the Trust may access an employee's Trust email account where it is deemed reasonably necessary, including during periods of absence, following departure from the Trust, or as part of an authorised investigation. Access will be restricted to those with a legitimate need to access the information and will be undertaken in accordance with the Trust's data protection and information governance requirements.

Updated August 2026