LDST
Liverpool Diocesan Schools Trust

STAFF COMMUNICATION AND SOCIAL MEDIA POLICY

OUR TRUST'S PRAYER

Heavenly Father

Let peace, friendship and love grow in our schools

Send the Holy Spirit to give:

Excellence to our learning

Love to our actions and

Joy to our worship

Guide us to help others

So that we may all

Learn, Love and Achieve, Together with Jesus.

Amen

1. Introduction and Scope

1.1. LDST is committed to the promotion of effective communication between all stakeholders.

1.2. This document has been produced to address the effectiveness and efficiency of communication throughout our Trust. Through embedding the principles outlined in this policy, effective training and the commitment of all Trust colleagues' communication will be integral to the continuing success of LDST.

1.3. This document should be read in conjunction with the following documents:

- LDST Freedom of Information Policy
- Data Breach Notification Policy
- Subject Access Request Policy
- Data Protection Policy
- Call Recording Policy
- Data Protection Policy (Appropriate Policy Document)
- Acceptable Use policies
- Online Safety Policy

1.4. LDST recognises the numerous benefits and opportunities which a social media presence offers. The Trust respects privacy and understands that staff and may use social media platforms and direct messaging services in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

1.5. Professional communications are those made through official channels, posted on a school account, or using the Trust or school name. All professional communications are within the scope of this policy.

1.6. Personal communications are those made via a personal accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

1.7. Personal communications which do not refer to or impact upon schools, students or colleagues are outside the scope of this policy. Digital communications with students are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

1.8. Colleagues should be aware that all electronic communications, whilst they are held, are disclosable under Freedom of Information (FoI) and Data Protection legislation.

2. Objectives

2.1. The objectives of this policy are to:

- Ensure a clear and professional approach to communication is in place.
- Ensure all Trust communications are as accessible and inclusive as

possible, seeking to eradicate bias, stereotyping or any form of discrimination.
- Ensure that approaches to communication and the systems that are in place are fully aligned to the Trust vision and values.
- Recognise that monitoring and evaluation of communication practices is an ongoing consideration.

3. Staff Responsibilities

3.1. Staff are responsible for:
- Ensure that the principles and procedures of this policy are followed.
- Communicating proactively and professionally with all stakeholders, in a way that is in-keeping with LDST's vision and values.
- Reporting to a senior leader as soon as possible, if abuse or bullying of a colleague is witnessed via any electronic communication platforms.

4. Email Communication

4.1 Sending Emails

4.1.1 All colleagues have their own Liverpool Diocesan Schools Trust email addresses to be used for all professional communication. Personal email addresses or other legacy school email addresses must not be used.

4.1.2 Colleagues should know how to send, open, and forward emails, as well as how to administer basic housekeeping on their accounts. Training will be provided on request, and basic training can be accessed directly from the Microsoft website. Ongoing support will be available from the school admin teams.

4.1.3 Colleagues must ensure they use the Liverpool Diocesan Schools Trust email signature (see Appendix A).

4.1.4 Colleagues must be mindful of the tone and propriety of their email communications and ensure that their written correspondence is always appropriate and professional. Colleagues should also remember that emails are easily forwarded.

4.1.5 Colleagues must never send e-mails that are offensive, threatening, defamatory or illegal.

4.1.6 Inappropriate emails may be considered under the relevant policy such as the Data Protection Policy, Dignity at Work Policy, or Disciplinary Procedure.

4.1.7 Colleagues must be aware of copyright issues, for instance when sending scanned text, pictures or information downloaded from the internet.

4.1.8 Care should be taken when expressing personal views that these cannot be misinterpreted as belonging to the school, LDST, or other colleagues.

4.1.9 The Trust recognises that all staff work differently, and we encourage staff to have an appropriate work/life balance. Therefore, Staff are not expected to write and respond to emails or other forms of communication outside of their standard working hours, unless the matter is considered to be an emergency.

4.1.10 Emails should be responded to within 48 hours wherever possible. Some emails may need to be prioritised based on their content.

4.1.11 Colleagues are responsible for ensuring that email recipients are appropriate and email addresses are correctly typed.

4.1.12 To ensure effective management of emails, staff should be mindful of who is copied (cc) into emails. The cc function should only be used if the information in the email will be directly useful to the colleague.

4.1.13 Blind copying (bcc) should only be used were appropriate. It should not be used for internal communication with colleagues but should be used to avoid the unauthorised disclosure of email addresses of intended recipients. For example, when emailing a group of parents.

4.1.14 Where possible, colleagues should provide a link to a website or SharePoint, rather than send an attachment.

4.1.15 It is likely to be inappropriate to discuss issues of a sensitive nature by email and staff must always be mindful of our duty of confidentiality. Although not exhaustive, sensitive issues may include addressing staff performance or student performance and behaviour. Issues of this nature should be discussed in a face-to-face manner or via a private telephone conversation.

4.1.16 Sensitive information should be sent by post or via an encryption system.

4.1.17 Personal information (such as a pupil's name) should not be included in the subject line of an e-mail.

4.1.18 Child Protection details should not be reported via e-mail other than where necessary, and CPOMs should be used wherever possible.

4.2 Receiving Emails

4.2.1 Emails should be read by the intended recipient only. If a colleague receives an email that was not intended for them, they should delete the email immediately and inform the sender of what they received.

4.2.2 Email accounts should be accessed on a regular basis, at least once each working day.

4.2.3 In the case of absence, an automatic reply (Out of Office) should be set up saying how long the colleague will be absent and providing an alternative contact.

4.2.4 Important emails that need to be stored should be saved as a PDF in an appropriate SharePoint folder.

4.2.5 Colleagues should be mindful of IT security and should not click on a link in an email, open an attachment, or provide any personal data or passwords in an email, without verifying the source of the email first.

4.3 Retaining Emails

4.3.1 Colleagues should be aware that they may need to provide copies of emails to individuals as part of Subject Access Requests.

4.3.2 Inboxes should not be used for file storage. Emails and attachments should be stored in appropriate folders.

4.3.3 The period of time that an email should be retained is based on the type of information within the email as per the LDST Retention Policy.

4.4 Directors and Governors

4.4.1 The same expectations apply for use of email as those for staff.

4.4.2 Governors and Directors may also communicate with the Trust and their schools via Governor Hub.

5. Using other electronic platforms for meetings and communication

5.1. Microsoft Teams is available for all staff to undertake meetings at cross-site level or to host training events. This includes Trust-wide meetings such as collective worship and conference events.

5.2. Colleagues are also permitted to use the direct messaging and chat functions of Microsoft Teams in both the desktop and mobile apps, provided that they abide by the principles in this policy.

5.3. Other methods of direct electronic communication such as text messaging, WhatsApp (including voice notes) or Facebook messenger must not be used to exchange any confidential information regarding the Trust or schools, or any information regarding staff or students. (This is particularly pertinent if a colleague is not a member of the What's App/Messenger group in which they are referenced).

5.4. Colleagues should also remember that messages are easily forwarded.

5.5. Colleagues must never send messages that are bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring their school, the Trust or teaching profession into disrepute. This applies both to public pages and to private posts e.g. in WhatsApp groups.

5.6. Inappropriate messages may be considered under the appropriate policy such as the Data Protection Policy, Dignity at Work Policy, or Disciplinary Procedure.

5.7. Care should be taken when expressing personal views on direct messaging platforms, that these cannot be misinterpreted as belonging to the school, LDST or other colleagues.

5.8. Colleagues should be aware that they may need to provide copies of messages to individuals as part of Subject Address Requests.

6. Security Considerations

Colleagues should ensure they read and understand the ICT Regulations and associated policies and protocols relating to IT system usage. However, the following are some specific considerations in relation to electronic communications.

6.1. Colleagues are responsible for the security of all IT and communication equipment provided to them by LDST, and for protecting any information or data used and/or stored on it.

6.2. Colleagues should not leave a mailbox open and unattended.

6.3. Colleagues must keep their IT account passwords confidential to prevent other users from accessing their accounts.

6.4. Emails will only be monitored by the Executive Headteacher/ Headteacher/ Head of School in exceptional circumstances.

6.5. Absent colleagues should be made aware that their e-mail account may be accessed by proxy by another member of staff.

6.6. LDST reserves the right to access all Trust IT accounts via the Trust Senior Information Risk Officer, for a justified reason such as safeguarding concerns or the need to access information in a colleague's absence.

7. Social Media

7.1. Guidance on Social Media use for staff can be found at Appendix B.

7.2. Colleagues are advised to contact the Professionals Online Safety Helpline if they have any concerns about social media or other elements of online safety.

7.3. **Process for Requesting New Official Accounts**

7.2.1 Each school has or can request official social media accounts.

7.2.2 LDST does not support official social media accounts tied to individual teachers.

7.2.3 Anyone wishing to create a new account must present a business case to the Headteacher which covers the following points:
The aim of the account.

- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)

- Will the account be open or private/closed

7.2.4 Following consideration by the Headteacher an application will be approved or rejected.

7.2.5 In all cases, the headteacher must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

7.4. **Managing Official Social Media Accounts**

7.3.1 Administrators should check with the Headteacher before publishing content that may have controversial implications for the school or Trust.

7.3.2 Official accounts must not be used to be express personal views.

7.3.3 It should be clear who is posting content.

7.3.4 Administrators must ensure they have permission to 'share' other peoples' materials and acknowledge the author.

7.3.5 Content should be written in a balanced and measured manner.

7.3.6 Careful consideration should be given before responding to comments and, when in doubt, a second opinion should be sought.

7.3.7 Any concerns should be reported to the Headteacher.

7.3.8 Image tagging should be turned off wherever possible.

7.3.9 No content should be posted that would bring the school or Trust into disrepute.

7.3.10 No confidential or commercially sensitive material should be posted.

7.3.11 No content should be posted that would breach copyright, data protection or other relevant legislation.

7.3.12 Administrators must take care not to link to, embed or add potentially inappropriate content.

7.3.13 Accounts must not be used to air internal grievances.

7.5. **Monitoring of Official Social Media Accounts**

7.4.1 School accounts must be monitored regularly and frequently (daily during term time).

7.4.2 Any comments, queries or complaints made through those accounts must be responded to on the next working day, even if the response is only to acknowledge receipt.

7.4.3 Regular monitoring and intervention are essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

7.6. **Staff Conduct on Social Media Accounts**

7.5.1 The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.

7.5.2 Digital communications by staff must be professional and respectful at all times, and in accordance with this policy. Colleagues should not post content that is bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring their school, the Trust or teaching profession into disrepute.

7.5.3 Staff will not use social media to infringe on the rights and privacy of others or make personal comments or judgments about colleagues, students, parents and carers or other stakeholders.

7.5.4 Official social media accounts must not be used for personal gain.

7.5.5 Staff must ensure that confidentiality is maintained on official social media accounts, even after they leave the employment of the Trust.

7.5.6 If media contact (e.g. from a journalist or reporter) is made about posts via social media accounts, staff must report this to the Headteacher or Trust CEO and must not respond unless they have authorisation to do so.

7.5.7 Unacceptable conduct (e.g., defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) on social media will be considered extremely seriously by the Trust and should be reported as soon as possible to a relevant senior member of staff and escalated where appropriate.

7.5.8 In line with the Prevent Duty, colleagues must not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit their school, nor browse, download or send material that is considered offensive or of an extremist nature.

7.5.9 The use of official social media channels by staff will be monitored, in line with Trust policies.

7.5.10 Personal social media accounts should not be accessed via Trust ICT equipment, without express permission from the Headteacher (or relevant director in the Trust Central Team).

7.5.11 The school will take appropriate action in the event of breaches of this policy under the relevant HR policy.

7.5.12 Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may act according to the disciplinary procedure.

7.5.13 Colleagues are advised not to name their employer on personal social media accounts, if possible. However, if staff wish to have accounts on professional networks such as LinkedIn, they are advised to list LDST as their employer, rather than an individual school.

7.5.14 Trust or school logos or branding must not be used on personal social media accounts.

7.5.15 Colleagues must not be connected to pupils/students on social media under any circumstances. Colleagues must report any attempt by a pupil/student to connect with them or another member of staff on social media to their headteacher as soon as possible as this is a significant safeguarding concern. The same applies to any attempt by a staff member to connect with a pupil/student.

7.5.16 Staff are advised to not have colleagues as friends/connections on social media to maintain their privacy, apart from accounts that are used for professional purposes (e.g. LinkedIn) and ideally, should apply the same to parents/carers/relatives of children who attend the school where they work.

7.5.17 Colleagues should regularly review their current connections on social media to ensure they are safeguarding their privacy. Wherever possible, colleagues should avoid sending request to connect to parents/carers/relatives of children at the school and are advised to politely decline and notify their headteacher if requests are received for parents/carers/relatives.

7.5.18 Staff are advised not to use the name that they use professionally on personal social media as best practice in order to safeguard their privacy and make it less likely that pupils, former pupils, parents and carers to find them on personal social media. Common practice is to have profiles under one's first name and middle name or perhaps a maiden name.

7.7. Dealing with Inappropriate Comments or Behaviour on Official Social Media Accounts

7.6.1 When acting on behalf of the school, manage offensive comments swiftly and with sensitivity.

7.6.2 Account administrators should delete any offensive or unacceptable comments and block and report the individual responsible as soon as possible.

7.8. Tone of Voice on Official Social Media Accounts

7.7.1 The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Messages/posts should be engaging and informative.

7.7.2 All messages/posts should be in-keeping with the core values of LDST:

- We value Difference

- We value Local
- We value Collaboration
- We value Inclusion

8. Use of Images in Electronic Communication

8.1. School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to:

- When a student joins a Trust school, their parent/carer will complete a consent form in relation to the use of images and videos of that student. We will not use images or videos of student for any purpose where we do not have consent (see Trust Data Protection Policy information).
- If anyone, for any reason, asks not to be filmed or photographed, or for their child not to be filmed or photographed, then their wishes must be respected.
- Under no circumstances should staff share or upload student/pupil pictures online, other than via school owned social media accounts.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts.
- Students/pupils should be appropriately dressed, not be subject to ridicule or distress and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes or posts a compromising or inappropriate which could be misconstrued or misused, they must delete it immediately.

9. Personal Communication with Students or Former Students

9.1. Any personal communication with a student or a former student under the age of eighteen (or over the age of eighteen but classed as a vulnerable adult) must be appropriately reported as per the LDST Safer Working Practices Code.

10. Communication with the Media

10.1. Any contact with the media (both local and national) concerning the Trust or a Trust school must always be made via the Chief Executive Officer (CEO) and Chair of the Trust Board. No one else (including Headteachers and members of Staff) are authorised to speak to the press without first having agreed this with the Chief Executive Officer and Chair of the Trust Board.

Review Schedule

Policy Author	Trust HR Lead
Policy Approver	LDST Directors
Current Policy Version	1.0
Policy Effective From	January 2024
Policy Review Date	January 2026

Revision Schedule

Version	**Revisions**	**By whom**
1.0	Original Document Produced	THRL

Appendix A: Email Signatures

The Trust email signature

Liverpool Diocesan Schools Trust

Learn, Love and Achieve, Together with Jesus

St James' House | St James Road | Liverpool | L1 7BY

www.ldst.org.uk | contact@ldst.org.uk | @LDSTEducation

Liverpool Diocesan Schools Trust is a company limited by guarantee.

Company Number 09235635

[Full name]
[Job role]
[School name]

Email: [email.address@ldst.org.uk]
Mobile: [work mobile number]
Office: [school office number]

My working week is [working pattern].

My working hours may not be the same as yours. Please feel free to respond to this email when it is convenient and meets with your work commitments.

A school email signature example is shown below.

St Michael's Church of England High School

[School strap line]

[road address] | [town address] | [city] | [postcode]
[school website] | [school]@ldst.org.uk | [@socialmedia]

[School name] is part of the Liverpool Diocesan Schools Trust
St James' House | St James Road | Liverpool | L1 7BY
www.ldst.org.uk | contact@ldst.org.uk | @LDSTEducation

Liverpool Diocesan Schools Trust is a company limited by guarantee.

Company Number 09235635

[Full name]
[Job role]
[School name]

Email: [email.address@ldst.org.uk]
Mobile: [work mobile number]
Office: [school office number]

My working week is [working pattern].

My working hours may not be the same as yours. Please feel free to respond to this email when it is convenient and meets with your work commitments.

Appendix B – Managing Your Personal Use of Social Media

- Nothing on social media is truly private.
- Social media can blur the lines between your professional and private life.
- Check your settings regularly and evaluate your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those to whom you want to be connected.
- When posting online consider the scale, audience and permanency of what you post.
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Useful Sources of Information

Professional reputation | Childnet

Professional reputation - UK Safer Internet Centre