LDBS Academies Trust

Excellence and Equity for All Children in a Christian Context

Data Protection Policy – Email Security & Etiquette

INSPIRING BELIEF
in God and one another

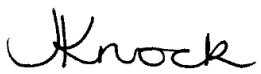
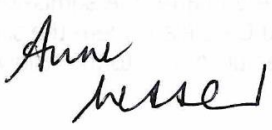
ST RICHARD'S SCHOOL

Our Vision:

To be a thriving and outstanding school where children and adults, working with the local community, have the opportunity to become the best they can be.

Inspiring belief…

- **in ourselves** – through progression and fulfilment
- **in each other** – through motivation and teamwork
- **in the children** – through showing them their potential
- **in the parents** – through building trust by results
- **in God to all** – through our whole lives

DATE APPROVED BY THE LAC	May 2019
REVIEW DATE	May 2021
Signed Headteacher	
Signed Chair of LAC	

LDBS Academies Trust

Contents

1. Aims

This policy applies to all email communication by the LDBS Academies Trust and the LDBS Academies Trust 2 (herein referred to collectively as the 'LAT') Directors, Local Academy Committee ('LAC') Governors, employees, volunteers, contractors and any other third part staff who is using emails to conduct business on behalf of the LAT, or who may have access to a LAT email account.

This policy aims to provide guidance to all users of a LAT email account, or those individuals conducting business on behalf of the LAT, on how to ensure that they maintain the highest standards in email security, confidentiality and professionalism while communicating using emails.

This policy complies with the higher standard of 'processing' introduced by the General Data Protection Regulation ('GDPR'). The GDPR has extended the definition of a 'processing' to include the use of emails to pass information and, therefore, this policy aims to ensure that all email communication is created, secured, transmitted and handled in accordance with the law.

2. Email security measures

All users of a LAT email account, or those individuals conducting business on behalf of the LAT, should abide by the following guidance on email security. Following the guidance will ensure that the technical information technology ('IT') security measures the LAT has in place remain robust and are less likely to be compromised.

1. All email and IT system logins and passwords should be changed regularly and must include at least one capital letter, number, and symbol (i.e. P@$5WoRd).

2. All users should endeavour to review their emails regularly and manage their accounts by filing, archiving, deleting old or unnecessary messages.

3. Sensitive or special data (such as information about an individual's race, ethnicity, religious beliefs, sexual orientation, political opinions, medical and health data, criminal records, financial circumstances, etc.) should not be sent using emails to any persons unless appropriate protection and / or encryption has been used to protect the data.

4. All users should carefully check the recipients of the emails they are sending, especially if the auto-complete function is operating and suggesting recipient email addresses.

5. All users should carefully check whether the carbon copy ('cc') and blind carbon copy ('bcc') fields to ensure that only the necessary recipients are listed to maintain confidentiality.

6. All users should ensure that all email contacts are up to date.

7. All users should ensure that the anti-virus software and the malware software is up to date on the machine being used to send emails.

8. Users should be wary of opening any attachments received in emails unless they arrive from a trustworthy source or the attachment has been scanned by the anti-virus software and the malware software.

9. Users should refrain from enabling any macroinstructions ('macros') unless they have checked with the IT Manager first.

10. Users should be wary when clicking on hyperlinks contained within emails and should adopt good safety practices when opening them (i.e. hovering the cursor above the hyperlink to review the website address, or entering the website address manually).

11. Users must report any unsolicited emails to a LAT school's office and / or the IT Manager by email office@strichards.hounslow.sch.uk. All users are advised to not click the 'unsubscribe' link in an unsolicited email as it may indicate to the sender that the email address is legitimate and result in more unsolicited emails being sent to the user and others within the organisation.

12. Email accounts are always monitored and the LAT may put into place measures to forward your emails to another account if you are on annual leave or upon the termination of your employment / contract.

13. Users should ensure that they do not leave themselves logged onto LAT machines / terminals when they leave. Users should ensure that they have a timed lock-out system in place or endeavour to always log out. All users must log out of their machines prior to leaving work for the day.

3. Email etiquette

The LAT expects all users to use the LAT's email and IT systems effectively and efficiently while adhering to the following guidelines.

1. **Understand the difference between the different address fields** – If you expect an individual to respond to an email or if the email is addressed to a specific individual(s), their email address should be written in the 'To' field.

   Users should use the 'cc' field sparingly and only when including recipients who must be kept aware about the issue being discussed in the email. Users should not include recipients from whom they expect to receive an answer in the 'cc' field.

   Users should use the 'bcc' field on in instances where they are sending out a chain message to numerous users and do not wish to disclose the email addresses of other users.

2. **Keep messages brief and to the point** – Make your most important point first, then provide detail if necessary. Make it clear at the beginning of the message why you are writing. Users are also recommended to ensure that they proof-read their messages to ensure that the punctuation and grammar is correct.

3. **Do not discuss multiple subjects in a single message** – If you need to discuss more than one subject, send multiple emails to allow recipients to scan subject lines quickly to find messages.

   If multiple subjects are discussed, users should ensure the subject line is appropriate and adequate headings are used to differentiate between each subject.

4. **Reply in a timely manner** – All users are encouraged to respond to emails in an appropriate timeline, but normally within one working day of receiving the email. Good etiquettes indicate that users should acknowledge an email in the event that it would take longer than one working day to respond.

5. **Be mindful of your tone** – Unlike face-to-face conversations or even telephone calls, emails do not have the benefit of a user's pitch, tone, inflection or other non-verbal cues. As a result, all users are encouraged to me careful about using sarcasm and idiom to avoid ambiguity and misinterpretation.

   Do not send messages where all letters are capitalised, and ensure that you do not respond in anger. Re-read your messages to ensure that all communication is constructive. Users are also recommended to not use emails to criticise others.

6. **Do not over-use the 'reply to all' feature** – Users are reminded that unnecessary use of the 'reply to all' feature clogs up email inboxes, which in turn can interfere with the efficient running of the LAT.

7. **Do not forward or send emails containing libellous, defamatory, offensive, racist or obscene remarks** – Users should be careful of the contents of the email they choose to send or forward. All users are reminded that offensive, or gross breach of this policy may result in disciplinary proceedings being commenced against them.

8. **Company emails are not private** – Users are reminded that all company emails or emails accounts being used to conduct business on behalf of the LAT are not private and can be retrieved if a successful subject access request has been lodged under the LAT's Data Protection Policy. Users are also reminded that all contents of a company email or email accounts being used to conduct business on behalf of the LAT can be retrieved and presented in a court of law during legal proceedings.

9. **Emails should not be printed unnecessarily** – Users are reminded that they should only print emails if absolutely necessary. Users are encouraged to use electronic filing systems.

10. **Do not send emails after 7pm** – The LAT encourages and promotes a positive work-life balance and advises all users to not use business email accounts after 7 pm.

4. Monitoring arrangements

The LAT's Data Protection Officer will monitor the guidance in this policy as part of his or her on-going compliance and auditing work. As previously stated, this policy will be reviewed biennially, except in the first instance where the review period has been shortened.

5. Links with other policies

This policy should be read in conjunction with the following LAT policies:

- Freedom of Information Publication Scheme
- Online & E-Safety Policy
- ICT User Agreement
- Data Protection Policy
- Information and Records Management Society's Information Management Toolkit for Schools
- Breach Management Policy
- Asset Management Recording Policy
- Business Continuity Plan
- Risk Register
- Safeguarding & Child Protection Policy