The Active Learning Trust

EMAIL ACCEPTABLE USE POLICY

This policy is reviewed on an annual basis

History of Document

Issue No	Author/Owner	Date Written	Approved by Trust Board	Comments
1	Director of Finance & Operations / DPO	May 2018	12 July 2018	1st formal issue

1. INTRODUCTION

1.1 Email has now become an integral part of the Active Learning Trust's ("Trust") organisational culture and is relied upon for both internal and external communication.

2. PURPOSE OF THE POLICY

2.1 The purpose of the Trust's Email Acceptable Use Policy ("Policy") is to outline the framework of acceptable email usage and controls in order to safeguard ICT equipment and information assets from unauthorised access, accidental or intentional damage, interruptions to availability of systems and prohibited illegal purposes.

3. SCOPE

3.1 This Policy is intended for anyone who sends or receives emails whether on school owned or personal ICT equipment held internally and outside a school.

3.2 For this Policy:

- Information covers any method of information creation or collection, including electronic capture and storage, video and audio recordings and any images.
- ICT or ICT system means computing and communications facilities that support teaching, learning and a range of activities in education.
- ICT is the knowledge, skills and understandings needed to employ information and communication technology appropriately.
- Where the term Headteacher is used this incorporates Executive Headteacher roles where these exist and the Chief Executive Officer of the Active Learning Trust when the statement refers to the central operations of the Trust.

4. RESPONSIBILITIES

4.1 The Trust Board has ultimate responsibility for setting this Policy.

4.2 A Headteacher is responsible for ensuring that the requirements relating to this Policy are adopted and adhered to and is responsible for the day to day management of email security arrangements, including delegating roles and monitoring effectiveness and has overall responsibility for the implementation of email communication arrangements in their school, must ensure it is implemented consistently and effectively, and is free from discrimination and subject to regular review.

4.3 Everyone who has access to a school's ICT systems and data must comply with this Policy, the Trust's ICT Security Policy and its Internet, Social Media and E-Safety Acceptable Use Policy. Anyone outlined in 3.1 above are required to read, accept and agree to abide with all these policies.

4.4 The Trust has produced IT Standards which cover how emails should be used in order to protect personal data as outlined by the General Data Protection Regulation.

4.5 A school's ICT service is responsible for implementing and monitoring security measures applied to a school's email system.

4.6 An Information Management & Cyber Security Governance Group reports to the Trust's Senior Leadership Team and considers Trust wide cyber security and information management matters.

4.7 The Trust's Data Protection Officer and the Trust's Director of Finance and Operations are responsible for monitoring a school's compliance with the Policy; submitting a report on the effectiveness of the Policy (GDPR matters – the Data Protection Officer) and ICT matters (the Director of Finance and Operations) to the Trust Board as a minimum on an annual basis. The Trust's Data Protection Officer is responsible for submitting any reportable security breaches to the Information Commissioner's Office.

5. MANAGING EMAILS

5.1 A school email account should be the only email account that is used for Trust/School business.

5.2 All email is filtered and logged, and email histories can be traced. Employees should remember that when a Subject Access Request or Freedom of Information Request is submitted, relevant email communications will be included in the material to be provided.

5.3 The following rules apply:

- Email users must treat others with respect and in a way in which they would expect to be treated (e.g. unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague should not be sent);
- Password/s must be kept securely;
- If any issues/complaints are involved then staff sending emails to parents, external organisations or students are advised to cc their line manager/s and other relevant individuals;
- Emoticons or 'smileys' should not be within emails as they are too informal for work-related communication;
- All emails should be written and checked carefully before sending;
- If a person has lengthy or detailed information to convey, an email may not be the best option. Other communications methods, or attachment options should be considered;
- Attachments should not be sent/forwarded unnecessarily. Where possible the location of the path to the shared drive where the document is held should be included in the body of the email.

5.4 Emails of short term value should be deleted so that mailbox capacity limit is not exceeded, and it just contains items requiring action. Users should try to decide what to do with each email as it is read (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical); Emails should not be printed unless necessary; and emails should be responded to in a timely fashion within 24 hours, where possible.

6. EMAIL FORMAT

6.1 The following rules apply:

- All external emails should be composed with formal language in the same way as a letter on school headed paper (i.e. Dear Mr/Mrs/Ms);
- Emails should be concise, easy to read in plain English and text broken up using short paragraphs, headings and lists, highlighting / underlining important aspects. Numbered and bulleted lists may change format when read in other mail systems, so this should be considered when formatting an email;
- All capital letters should not be used in both the subject box and the main body of text as it is considered to be 'SHOUTING' in email terms;
- Where possible emails should be marked 'for information' or 'for action' as this will allow the recipient to prioritise reading those mails which require action and leave those to be read for information for later attention;
- Email signatures should be short and include name, title, phone number(s) and website address as shown by the example below:

  Gary Peile
  Chief Executive
  The Active Learning Trust
  Office: 01223 728394

  www.activelearningtrust.org

- A standard disclaimer must be attached to **all** email correspondence - refer Appendix I. This disclaimer should be automatically added to emails sent externally. Such disclaimer is a statement of legal character that identifies that the email is only for the recipient and contains a disclaimer for opinions and errors.

7. SENDING EMAILS

7.1 The following rules apply:

- The number and relevance of email recipients, particularly those being copied, should be kept to the minimum necessary and appropriate;

- The workload of the recipient should be considered by either grouping several matters into one message or if it would be better to send separate messages on each matter;

- Use the 'red flag' urgent message signal only when absolutely necessary;

- When an out of office reply is received to an email this means the recipient is currently unavailable. Reduce the amount of email (especially items cc'd for information) to such persons during the times they are not available so as to avoid a build-up of messages for them on their return;

- It is also important to recognise the emails sent late at night, late on a Friday, or at the weekend should not require or assume a reply outside of working hours.

- Automatic forwarding or redirection of email to other mail domains is possible. The Trust absolves all responsibility for email forwarded off the school network. It is the individual's responsibility to set forwarding up and make sure the forwarding address is correct and the email service being used is reputable and reliable.

- Read receipts are not be used on all emails and only used where specific read / delivery receipts are required.

7.2 Users **MUST NOT**

- Use language which might cause offence or be seen as abusive, discriminatory, bullying in nature or harassment as defined in the Trust's approach to equality and diversity (including race, gender, disability, age, religion/belief or sexual orientation);

- Send personal and confidential information to home or external email accounts;

- Contact students, parents or conduct any school business using any personal email addresses;

- Include personal information in the message line or body of an email;

- Send emails from another User's email account unless authorised to do so e.g. send on behalf of …..;

- Send emails with jokes, chain letters, unsolicited commercial or advertising material, junk-mail or other offensive or inappropriate content;

- Send/forward attachments unnecessarily. Where possible send the location path to the shared drive;

- Send an email with a scanned version of a handwritten signature to sign an email;

- Send an email to a large group of people without bcc'ing the email;

- Send an email where it is unclear as to whether the user is publishing or transmitting information externally on behalf of a School/Trust and in fact the opinions were personal;

- Send whole School/Trust emails unless essential for school business purposes;

- Send material such that it infringes the copyright of another person, including intellectual property rights;

- Unreasonably or excessively send emails for personal use, engage in 'recreational' chatting during working time, on email or through instant messaging, that results in lost productivity or distracts other employees from their work; and

- Create or transmit anonymous emails or deliberately forge messages or email header information, (i.e. without clear identification of the sender).

8. SENDING PERSONAL AND CONFIDENTIAL INFORMATION BY EMAIL

8.1 Emailing personal data or confidential information outside a school's network, unless it is sent through a secure service, without the use of encryption is prohibited.

8.2 Users must apply the following checks before releasing an email:

- Verify (preferably by phoning) the details of the requestor and email address if unknown, before responding to email requests for information;

- Do not copy or forward the email to any more recipients than is absolutely necessary;

- Provide the de-encryption key or password via a separate medium as the encrypted data;

- Do not identify the personal information in the subject line of any email or body of the email – put "Confidential" in the subject line and as a header in the email and any attachments to the email; and

- Request confirmation of safe receipt of the email.

9. RECEIVING EMAILS

9.1 Emails must be checked regularly.

9.2 If appropriate, out of office notification must be activated when away from a school/Trust for extended periods.

9.3 Email systems must not be used to store attachments. School related attachments should be detached and saved to the appropriate shared drive/folder.

9.4 Users are to allow a reasonable time for a response before issuing a follow up email. Users should not "chase" a reply with reminder email before necessary as this may be considered harassment by the recipient.

9.5 Users **MUST NOT** open emails from an address or person not recognised, untrusted source or suspicious messages received from unknown sources. Such should be reported to the ICT service who will investigate and advise how to proceed.

10. STUDENTS AND EMAIL

10.1 If students are issued with a school email account when joining a school, staff should make students aware of the following when using email:

- Appropriate formal language must be used in messages;
- Personal details about themselves or others must not be revealed in emails;
- Arranging to meet anyone unknown on email is not allowed;
- Email attachments are automatically checked for viruses before opening;
- They must immediately inform a teacher if they receive an offensive email;
- Staff will inform other relevant staff if they become aware of any misuse of emails.

11. SENDING AND RECEIVING OFFENSIVE ITEMS

11.1 Creating, accessing, transmitting, downloading, uploading or storing any of the following material (unless it is part of an authorised investigation) is likely to amount to gross misconduct and result (where the adult is employed) in summary dismissal (this list is not exhaustive):

- pseudo-images of children (child abuse images), pornographic or sexually suggestive material or images of children or adults which may be construed as such in the circumstances (that is, writing, texting, pictures, films and video clips of a sexually explicit or arousing nature),

- any other type of offensive, obscene or discriminatory material, criminal material or material which is liable to cause distress or embarrassment to a School/Academy or others.

11.2 If indecent images of children are discovered at the premises or on a school's/ Trust's equipment/devices, an immediate referral should be made to the School/Trust Designated Safeguarding Lead and Head Teacher (unless he or she is implicated) and the external Designated Officer and, if relevant, the police contacted. The images/equipment should be secured, should not be used by others and should be isolated from the network. There should be no attempt to view, tamper with or delete the images as this could jeopardise any necessary criminal investigation. If the images are of children which are known to the School/Academy, a referral should also be made to children's social care in accordance with local arrangements.

12. MONITORING

12.1 The Headteacher will keep all monitoring at work within the provisions of the Data Protection Act 2018 and the European Convention of Human Rights. Users should have no expectation of privacy in any emails transmitted to, received, or stored or recorded on the Trust's electronic information and communications systems.

12.2 The Trust reserves the right to monitor, intercept and review, without prior notification or authorisation from adults, its email systems to monitor whether the use of the e-mail system is legitimate and in accordance with this Policy. This includes messages sent or received by system users within and outside the system as well as deleted messages to assist in the investigation of alleged wrongful acts and to comply with any legal obligation.

12.3 The following details are recorded by a school system in respect of every email message:

- Name of the person sending the email
- Email addresses of all recipients and copy recipients
- Size and name of any file attachments
- Date and time sent
- Copy of the email
- Copy of file attachments

12.4 Suspected or actual security breaches of this Policy are to be reported to a Headteacher who in turn will notify a school's ICT service and Trust's Data Protection Officer in accordance with the Trust's Data Protection Policy.

13. DISCIPLINARY ACTION

13.1 Disciplinary action may be taken against any User suspected of being in breach of this Policy, including an immediate ban from using a school's ICT facilities.

13.2 Breaches of this Policy may constitute gross misconduct and as such may lead to staff dismissal. For individuals not directly employed by the Trust, breaches of the Policy may result in withdrawal of facilities and referral made to their employer. For all other adults, breach of this Policy may be a breach of the Code of Conduct and may lead to sanctions being applied up to and including their removal from the Governing Bodies.

13.3 The Police will be informed where there is a possibility that a criminal offence has been committed.

13.4 If an employee is aggrieved or wishes to register or report a complaint they must follow the Whistleblowing Policy and/or Staff Grievance Procedures.

14. REPORTING

14.1 The Trust's Director of Finance and Operations is responsible for submitting a report on the effectiveness of this Policy to the Trust Board as a minimum on an annual basis.

15. REVIEW

15.1 This policy will be reviewed on an annual basis by the Trust Board.

APPENDIX I – EMAIL DISCLAIMER TEXT

The registered office of The Active Learning Trust Limited is c/o Isle of Ely Primary School, School Road, Ely, Cambs CB6 2FG. Registered in England & Wales No.7903002. The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential or privileged material. Any review, transmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer. Internet communications are not secure and The Active Learning Trust Limited accepts no legal responsibility for the contents of this message. The Active Learning Trust Limited makes no representation and accepts no responsibility or liability as to the completeness and accuracy of the information contained in this message. Opinions may change without notice.