

# SCALBY LEARNING TRUST

## E-MAIL PROTOCOL AND GUIDANCE

### HISTORY OF DOCUMENT

Issue No.	Author	Date Written	Approved by Governors	Comments
1	A Wappat/J Marshall	March 2010	21 April 2010	
2			21.3.12	No amendment
3			29.1.13	Appendix A added
4	N Penn/P Skelton		10.6.15	New appendix A
5		Updated 23.9.16	19.10.16	Approved

### EMAIL POLICY AND GUIDANCE

#### What does this document refer to?

It refers to the e-communications infrastructure, which is owned and controlled by Scalby Learning Trust. Through this infrastructure, users are able to send and receive internal and external email from an individual account.

#### Who does this policy apply to?

It applies to all users of Scalby School's email system, through any other hardware device.

It covers includes students and staff and applies equally whether working from School, at home or from any other location. These groups of people will thereafter in this document be collectively referred to as **users**.

#### Introduction

Email is a fast and efficient communications tool, but we have to be careful that we are using it legally, efficiently, appropriately and securely.

With ever increasing volumes of email, users of Scalby School's email system are finding it more and more difficult to remain in control of their inbox. Email senders should be aware of this before dispatching emails to large numbers of people or copying users into messages unnecessarily. There also needs to be an understanding that staff have different work patterns, so while some may be able to respond immediately, other staff may often be out of the office or spend large parts of their day in meetings.

Equally, email recipients need to manage their inbox effectively, prioritising responses according to their importance, rather than feeling under pressure to reply to all messages immediately.

The purpose of this document is to provide a framework within which email can be used to its full potential

within certain parameters. It is divided into two sections; policy (things that you must do when using Scalby School's email system) and guidance (best practice that users ~~you~~ should seek to follow wherever practical).

*This document should be read in conjunction with the IT security standards, which are available via the website. Usage of email is also covered within the Disciplinary Procedure available. For Members, compliance with this policy will support the standards of behaviour required by the Code of Conduct for Members and the ICT Conditions of Use.*

### **Seeing it from the customer's point of view**

What opinion would you form of an organisation if you contacted them and:

- They responded promptly?
- The reply was clear and fully answered your question?
- The reply was well written in plain English and contained no errors?
- The tone was approachable, non-bureaucratic and polite?

### **When communicating with the public we will aim to ...**

- Ensure people are treated with respect, courtesy and understanding
- Be as helpful and open as possible
- Point people in the right direction if we can't help
- Let people know what will happen next

## **Email policy**

Users **must** follow the points below. If there is evidence to suggest that users have failed to abide by these policy requirements, Scalby School has the right to conduct an investigation. This may result in the removal of your email facility and/or disciplinary action.

Scalby School retains the right to view all emails sent or received using our email system at any time. Your emails can be intercepted and monitored using powers under the Regulation of Investigatory Powers Act 2000 (RIPA).

1. Ensure your email account is kept secure by changing your email password regularly and not giving it to anyone.
2. Users must only use email for educational purposes in work time.
3. Personal use of e-mails in your own time is acceptable but, in line with the internet filtering policy, use in school time is not permitted, unless in exceptional circumstances where you have prior agreement.
4. Any agreed personal use must not make significant demands on IT resources. Therefore, transferring or storing large attachments such as images, audio and video clips is not permitted.
5. Any personal or business use for illegal, threatening, offensive, obscene, pornographic or libellous purposes is strictly prohibited.
6. Never use your school email address when posting comments on public bulletin boards or chat rooms unless directly related to school.

7. If you receive an email that is obviously spam or of an adult nature, do not open it, rather delete it immediately.
8. Never participate in chain emails where you are asked to forward an email to a number of others.
9. In legal terms, under the Telecommunications Regulations 2000, sending an email is as binding as sending a signed letter. Therefore, do not express personal views or information by email, because Scalby School could be held vicariously liable for the opinions and views expressed.
10. This also applies to comments posted on public discussion boards if you use a Scalby School email address or state the opinions in a work or school capacity.
11. Users can be held criminally liable if they knowingly or recklessly disclose personal information outside the Trusts procedures.
12. As email is an insecure means of communication any personal or confidential information that must be transmitted by email **must** be sent within a password-protected or encrypted document, with any password/key being sent separately.
13. Many distribution lists are maintained to help optimise the delivery of email. Ensure you use the correct distribution group for your email (e.g. use 'Teaching' instead of 'Staff'). The distribution groups are available in the online address book, or a list is available on request from IT Support.

## Email guidelines

The following points support best practice in the use of Scalby School's email system. Whilst failure to follow this guidance will not result in disciplinary procedures, users are strongly encouraged to adopt these points wherever possible.

### Respond promptly ...

- If a full answer is not possible within this timescale, send an acknowledgement email with details of when a full response will be sent. The full response must be within ten working days
- You should set up your out of school reply if you are unable to access your email account for more than a day and include an alternative contact in the message
- Staff should also aim to respond to internal emails within the same timeframes as above

### Write clearly and concisely ...

- Your message should be easy to read and understood, using plain English rather than jargon – see [www.plainenglish.co.uk](http://www.plainenglish.co.uk) for more information
- Adapt the tone according to the situation. For example, a response to a formal external email should be replied to formally, but an internal email to a colleague can be more informal
- Don't go into more detail than is required. A concise email is quicker to deal with by the recipient than a rambling one
- Only attach documents when necessary and refer to them in the email. Name attachments properly so the recipient knows what is being attached
- Make it clear what action, if any, is expected in response to your email
- Read all messages through, check the recipients and spell check them before you press 'send'. For example, staff should check e-mails are not going to students by accident.

### **Manage email effectively ...**

- Email attachments should be detached and stored on local shared network drives etc or deleted within twelve months of receipt, rather than stored within your email account
- If storing emails for a short period, make use of the ability to file emails within folders, rather than keeping all emails in your inbox
- Email attachments like Word documents and PDFs take up large amounts of storage space. They should be removed from emails you wish to store and saved on local network drives if required
- Your emails should consume no more than 400MB (staff) / 40MB (students) storage space at any given time. If you go above this, an automatic warning will be sent to you
- Try to keep to a maximum of 50 messages in your inbox and 300 in total throughout your email folders. Weed out your 'sent items' folder regularly. This should help you manage your email and prioritise your work effectively. Be aware of Freedom of Information (FOI) and data protection legislation ...
- Archive old emails to a password protected personal storage folder
- All emails, regardless of length, are public records. There is no distinction between information contained in an email and any other document. You need therefore to be aware that what you write in an email could become disclosable and therefore available to the public
- Keep personal information about individuals to a minimum and dispose of that information as soon as the need to use that information has passed
- Scalby School may where required use data protection legislation to check users email accounts in their absence.
- Where access to another member of staff's email is required for retrieval of cover work or other important information, IT Support require express permission from either the owner of the mailbox or the Senior Leadership Team.
- Under FOI, the public have a right to request information held by the Trust, unless it is exempt. It is therefore important that you compose emails with this in mind and that any important emails are stored on shared servers so they can easily be accessed by colleagues if required
- Check with the IT Support if unsure about any of the above points

### **Be aware that emails are not secure ...**

- Whilst internal emails sent within the school network are secure, external emails are not a secure means of transferring sensitive or confidential information. This is because they are relatively easy to intercept.

### **When not to send email ...**

- Think carefully about whom you send messages to. Do they really need to be sent or copied into the message?
- When the information is or should be available on the public drive
- If using the telephone or meeting face-to-face would be more effective
- To numerous people, even if you are just copying them in – reading unnecessary emails wastes time and overflowing inboxes can cause stress. Only include people if they really need to see the message
- Do not attach large documents or use formats that recipients may not have. A 2MB document, for example, will take around five minutes to download for a user at home on dial-up
- Sending attachments to large numbers of users puts considerable strain on the email server. Consider putting the attachment(s) on the public drive or **sharing the document via cloud storage** and directing people to it.

- In haste, particularly if you are angry - wait to calm down so your response is more measured

### **And lastly ...**

- Do not open attachments from people you don't know. They can be used to spread viruses
- Always use the default email font
- Always use the 'subject' field with a clear indication of what the message is about. This helps recipients prioritise emails and find the one they need amongst all the others
- Be aware that whilst IT do all they can to block out spam and are largely successful, trying to block the remaining 1% that does get through would result in some genuine emails being blocked. For example, incoming emails with no subject field may not get through as the spam filter may block them thinking they are junk
- Incoming and outgoing emails over 10MB will be blocked. If you need to receive emails larger than this, contact the IT Helpdesk
- Do not store documents attached to emails in your email folders. This creates individual islands of data, which are hugely inefficient in terms of IT storage and can cause version control issues. Save documents on the local network drives instead
- If replying to an email, include enough, but not necessarily all, of the original message in your response to keep the thread of the conversation clear
- Apply the same professionalism you do to other forms of communication such as telephone and letter
- With external emails, ensure you include a signature that includes a minimum of your contact name, title and telephone number. All outgoing emails are automatically stamped with the school's main contact details and standard disclaimer.
- Do not print out all emails you receive. This wastes paper, toner and time and is usually unnecessary as most emails can be dealt with on screen
- That using 'return receipt' increases traffic unnecessarily, please only use when essential and be aware that it often won't work if sending external emails
- If you receive an email that was sent to you in error, stop reading it as soon as this becomes obvious. Then return it to the sender and delete it
- Be on your guard for scam emails, asking you to enter personal information, for example your bank security details
- Also be wary of alarmist emails that are often hoaxes

### **Further information**

If you require training on how to use the email system, ask your line manager to arrange training from IT Support

## **APPENDIX A**



# Acceptable Use Agreement – ICT and eTechnology

### Members of staff:

- Must only use the school's ICT technologies for professional purposes or for uses deemed 'reasonable' by the head teacher or Governing Body. Individual employees' internet, email and other related technologies are monitored and logged and can be made available, on request, to their line manager or head teacher.
- Must only use approved, secure school provided communication systems for any school business.
- Must **not** browse to, download or send material that could be considered offensive or illegal, and should report any accidental access of inappropriate materials to their line manager.
- Must **not** attempt to implement to install any IT software or hardware for use in school without first consulting IT Support.
- Must **not** attempt to circumvent any security restrictions that have been implemented to protect systems and / or information.
- Must supervise students in IT suites **at all times**.
- Must **not** allow students to use staff designated workstations and / or equipment.
- Must **not** disclose their password to anyone, including IT Support.
- Must consider copyright implications when using or requesting resources to be used within the school environment.
- Must report problems with IT equipment as soon as they are able to via the IT helpdesk.
- Should **not** use school information systems or resources (e.g. cameras, laptops, memory devices) for personal purposes without specific permission from the head teacher. Such items should only be used for professional purposes.
- Are only permitted to use personal portable media for storage of school related data / images that has been encrypted with Bitlocker Drive Encryption.
- Are only permitted to use school provided cloud storage for school related data / images. Currently staff are granted access to OneDrive using their school login credentials.
- Should ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off school premises, or accessed remotely. Personal data can only be taken out of school if it is stored on a memory device encrypted Bitlocker Drive Encryption or stored and accessed from OneDrive.
- Are **not** permitted to use personal digital equipment, such as mobile phones and cameras, to take images of students or record videos, including when on external trips / visits. With the written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
- Should ensure that their use of web technologies, including social networking sites, do not question or bring their professional role into disrepute. Members of staff:

- Are advised to consider, and set appropriately, their privacy settings on such sites.
- Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
- Should **not** communicate with students, in relation to either school or non-school business, via personal social media accounts. A limited number of staff are allowed to contact students via school sanctioned accounts as part of their remit.
- Members of staff should only communicate with students using the appropriate communication platforms or other systems approved by the head teacher.
- Are **not** permitted to contact or communicate with students, parents or conduct school business using personal email addresses or telephones, without specific permission from the head teacher. Permission to contact parents is granted only to a limited number of colleagues to contact parents from personal telephone numbers outside of school hours, if appropriate safeguards are taken.
- Should **not** give out their own personal details, such as personal telephone / mobile number or personal email address, to students. **School email addresses should be used where contact with parents (eg. at subject level) is necessary.**

## Declaration

I agree to follow this user agreement, and understand that failure to do so may result in disciplinary proceedings in line with the school's disciplinary procedure.

**Full Name (Printed):**

**Signature:**

**Date:**

**Job Title:**

*This Policy was reviewed by the Resources Committee on a 2 yearly cycle and must be signed by the Chair of Governors and Head Teacher.*

Policy Reviewed:	
Next Review:	
Signature of Chair of Governors:	Signature of Head Teacher:

--	--

**Please ensure you complete the Equality Impact Assessment below**

**Equality Impact Assessment Form**

1. Title of policy, project or practice being reviewed or planned

Email protocol and guidance
-----------------------------

2. Outline the aims, objective and purpose of the change including any positive impacts on equalities groups.

N/A
-----

3. Which groups of people (if any) are most likely to be affected by the planned changes, positively or negatively?

N/A
-----

4. Does, or could these changes have an adverse effect on members of an equalities group? Identifying a negative impact is not a problem, as it gives you an opportunity to remove the barrier, find a way around it, or offer an alternative.

Protected Characteristics / Group	Yes (brief explanation)	No
Age (staff only)		X
Disability		X
Gender		X
Gender reassignment		X
Marriage / civil partnership		X
Pregnancy / maternity		X
Race / ethnicity		X
Religion / belief		X
Sexual orientation		X

5. Is there a way to modify the decision to remove or mitigate the negative impact on protected groups while still achieving this aim? How can you maximise positive outcomes and foster good relationships?

N/A
-----

6. Outline the decision made and actions planned.



The policy will be monitored by the ICT Manager and also be subject to annual in order to ensure Equalities Legislation is adhered to.