Regulation on use of email

Version: 1.01 Release date: April 2019 Review date: March 2020
Authorised by: Darrell Smith

Regulations on Use of E-mail

1. Introduction

These guidelines are intended to assist School\Trust staff to manage their e-mail in the most effective way and must be used in conjunction with your School\Trust policies on the use of ICT.

Information about how your e-mail application works is not included in this document.

2. Eight Things You Need to Know About E-mail

E-mail has replaced telephone calls and memos as the main communication method in many organisations including schools.

As communicating by e-mail is quick and easy, many people have replaced telephone conversations and memos with e-mail discussions. However, the language in which e-mail is written is often less formal and more open to misinterpretation than a written memo or a formal letter. Remember that e-mail should be laid out and formulated to the School\Trust standards for written communications.

E-mail is not always a secure medium to send confidential information

You need to think about information security when you send confidential information by e-mail. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could invoke a financial penalty from the Information Commissioner or it could end up on the front page of a newspaper. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Never put personal information (such as a student's name) in the subject line of an e-mail. Please refer to the School\Trust data protection policy for information on sending personal or sensitive information.

E-mail is disclosable under the access to information regimes

All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

E-mail is not necessarily deleted immediately

E-mails can remain in a system for a period after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the General Data Protection Regulation (GDPR).

E-mail can form a contractual obligation

Agreements entered into by e-mail can form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.

E-mail systems are commonly used to store information which should be stored somewhere else

All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files. Email accounts should not be used for storage of attachments. Email systems like Office 365 and Google offer user and central cloud storage locations which are secure and should be used for file storage and management.

The School\Trust must be careful how it monitors e-mail

Any employer has a right to monitor the use of e-mail provided it has informed members of staff that it may do so. Monitoring the content of e-mail messages is a more sensitive matter and if you intend to do this you will need to be able to prove that you have the consent of staff. If you intend to monitor staff e-mail or telephone calls you should inform them how you intend to do this and who will carry out the monitoring.

The Information Commissioner's Employment Practices Code is an excellent guide to this subject.

E-mail is one of the most common causes of stress in the work-place

Whilst e-mail can be used to bully or harass people, it is more often the sheer volume of e-mail which causes individuals to feel that they have lost control of their e-mail and their workload. Regular filing and deletion can prevent this happening.

Guidance on the Use of E-mail

Here are some steps to consider when sending e-mail.

Do I need to send this e-mail?

Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.

To whom do I need to send this e-mail?

Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is necessary. Never send on chain e-mails.

When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official School\Trust business must be sent from an official domain address.

If you receive an email containing personal or sensitive information via an unsecure method. You should delete the email and contact the sender, highlight your concerns with the unsecure method of transfer and request the information be resent in a secure way.

Use a consistent method of defining a subject line

Having a clearly defined subject line helps the recipient to sort the e-mail on receipt. A clear subject line also assists in filing all e-mails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.

Ensure that the e-mail is clearly written

- Do not use text language or informal language in School\Trust e-mails.
- Always sign off with a name (and contact details).
- Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
- Never write a whole e-mail in capital letters. This can be interpreted as shouting.
- Always spell check an e-mail before you send it. Do not use the urgent flag unless it is necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.
- If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

Sending attachments

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on the School\Trust network. Where possible, put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it. If you are sending personal information then you must encrypt the file, sending large amounts of personal data over email has its risks and could cause a data breach. There are other methods of sharing information by using secure shared cloud platforms.

Disclaimers

Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient, or helps to clarify the School\Trust position in relation to the information being e-mailed. The disclaimer explains the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the School\Trust.

Sample exclaimer text –

Disclaimer: The information in this e-mail, together with any attachments, is confidential. If you have received this message in error you must not print off, copy, use or disclose the contents. The information may be covered by legal and/or professional privilege. Please delete from your system and inform the sender of the error. As an e-mail can, be an informal method of communication, the views expressed may be personal to the sender and should not be taken as necessarily representing the views of Castlefield school. As e-mails are transmitted over a public network Castlefield school cannot accept any responsibility for the accuracy or completeness of this message. It is your responsibility to carry out all necessary virus checks.

4. Managing received e-mails

This section contains some hints and tips about how to manage incoming e-mails.

a) Manage interruptions

Incoming e-mail can be an irritating distraction. The following tips can help manage the interruptions.

- Turn off any alert that informs you e-mail has been received
- Plan times to check e-mail into the day (using an out of office message to tell senders when you will be looking at your e-mail can assist with this).

b) Use rules and alerts

- By using rules and alerts members of staff can manage their inbox into theme-based folders. For example:
- E-mails relating to a specific subject or project can be diverted to a named project folder
- E-mails from individuals can be diverted to a specific folder
- Warn senders that you will assume that if you are copied in to an e-mail, the message is for information only and requires no response from you.
- Internally, use a list of defined words to indicate in the subject line what is expected of recipients (for example: “For Action:”, FYI:”, etc)
- Use electronic calendar to invite people to meetings rather than sending e-mails asking them to attend

c) Using an out of office message

If you check your e-mail at stated periods during the day you can use an automated response to incoming e-mail which tells the recipient when they might expect a reply. A sample message might read as follows:

Thank you for your e-mail. I will be checking my e-mail at three times today, 8:30am, 1:30pm and 3:30pm. Thank you for your patience.

If you require an immediate response, please contact reception on 01494 436018

5. Filing e-mail

Attachments only

Where the main purpose of the e-mail is to transfer documents, then the documents should be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The e-mail can then be deleted.

E-mail text and attachments

Where the text of the e-mail adds to the context or value of the attached documents it may be necessary to keep the whole e-mail. The best way to do this and retain information which makes up the audit trail, is to save the e-mail in .msg format. This can be done either by using the "save as" function to save the e-mail in an electronic filing system on your network drive.

Where appropriate the e-mail and the attachments can be printed out to be stored on a paper file, however, a printout does not capture all the audit information which storing the e-mail in .msg format will.

E-mail text only

If the text in the body of the e-mail requires filing, the same method can be used as that outlined above. This will retain information for audit trail purposes.

The technical details about how to undertake all these functions are available in the email Help function.

How long to keep e-mails?

E-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in storage areas meeting records management storage standards.

E-mail that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these e-mails will then correspond with the classes of records according to the School\Trust Record Retention Policy. These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

Identifiable information in emails

As a general rule all information relating to data subjects should be anonymised if possible. Emails are accessible under a Subject Access Request if they contain information relating to data subjects, anonymising names and identifiable information will remote them from the request. This is not always possible but should be a default rule when referencing individuals in email communications.

Further information

Contact

If you would like to discuss anything in this safe use of email policy\guidance, In the first instance please contact the School lead below:

Position	Name	Email	Phone
School lead	**Mr A Kann**	**dpo@castlfield.bucks.sch.uk**	**01494 436018**
Data Protection Officer	**Mrs J Smith**	**Dpo@castlefield.bucks.sch.uk**	**01494 436018**

Policy\procedure update information (policy number GDPR-106)

This safe use of email policy\guidance is reviewed annually and updated in line with data protection legislation.

Policy\procedure template review information

Review date	Reviewed by
02-05-2018	turn IT on

Policy\procedure template update information

Review date	Revision	Description on change	By
02-05-2018	1.00	Draft release	turn IT on
03-05-2018	1.00	Full release	turn IT on
15-05-2019	1.01	Updated following review	Turn IT on