Silverhill School

8.03

Email Best Practice Guidelines for Staff

Introduction

Email can provide an invaluable means of communication, but our emails need to be clear and concise if we want them to be effective. These guidelines outline email best practice for Silverhill School & Day Nursery staff.

Is email the correct tool?

Before drafting an email pause and consider if it is the most appropriate communication method. Face-to-face or a quick telephone call may be more effective, particularly if the topic is sensitive or confidential or very urgent.

Writing an email

Action: Consider what action you would like the recipient to take when they receive the message and make this clear (if you don't know neither will they).

Subject line: Treat this as the label on the tin. Include (concisely) as much information as possible about what the recipient is required to do, including for example, dates, deadlines, times and locations.

Suffix: Useful tool for the subject line to indicate what is required of the recipient. Suffix can then be used as a tag to sort emails into folders. Examples include [Info], [action] [urgent] [project code]

Email length: Avoid lengthy emails as the message or action can become lost or confused. If you are communicating complex information then consider using an attachment or link to a document. Avoid replying with email history unless it is necessary.

Attachments: Avoid sending large attachments or documents of a sensitive nature. If this is considered necessary then password protect the document. An alternative is to use a shared folder within the Intranet system and direct the recipient to this folder.

Email signatures: All emails (including replies and forwards) should include an email signature which includes the school's standardised signature and job title. If this has not already been set up on your email, please refer to the school office. Email signatures can also be used to convey other information such as working hours and working days.

Final check: It is advisable to re-read your emails before sending to check that the email recipient is correct, that the message is clear and that attachments have been inserted and spelling has been checked.

Recipients, reply all and automatic replies

Recipients: Consider the recipients of your email and be clear what – if anything – you want them to do.

• The "To" field should only be used for recipients who you are asking to take action.

• The "Cc" field is for recipients who need to see the information. Think carefully about who you need to communicate with and limit the 'Ccs' to this group only. The "Bcc" field should be used if you do not wish to share an email address(es) with other recipients.

Reply all: "Reply all" creates large numbers of emails which are often irrelevant. Before using the "reply all" consider if all the recipients need to know or take some action. Also consider whether they should have access to all of the information contained in the message.

Automatic replies: When you are away from the office for a full day or longer, your "out office" should be enabled as a response for all internal and external emails. It should contain the date you will return to work and an alternative contact.

Responses

When responding to an email, double check that you have addressed all the points/questions that were raised – this reduces the need for further emails seeking clarification.

Response time expectations

The use of mobiles and tablets has led to people expecting a very fast response to emails – even at evenings and weekends. During the working week it is not reasonable to expect a response in less than 24 hours. It is certainly not reasonable to expect a response in the evenings and at weekends. If a response is required in minutes or hours, then email is probably not the most effective communication tool.

Inbox Management

Frequency of checking emails: Checking emails numerous times during the working day, out of working hours and during leave can lead to stress. It is recognised that most staff involved in the care of young children will not be working in a computer based environment. The School recommends that staff directly involved in the day-to-day care of children check their emails 1-2 times a day. This will allow you to focus on specific tasks without constant interruption.

Email preview: The email preview bubble can often cause a distraction if you feel this is the case then it is advisable to turn this off.

Organising email: Avoid letting unread emails build up in your inbox. Here are three rules for creating and maintaining an organised inbox:

1. Deal with emails which only need a quick response as soon as possible
2. File emails requiring a longer, more considered response in a pending file
3. Archive old emails which you need to retain and delete all others

('Pupil Rules for Responsible Internet Use' can be found under **APPENDIX 1** in the **Internet Policy)**

How to deal with Suspicious Attachments

If you receive an email with a file attachment – or any file format, for that matter – caution is the best policy. You must alert the Front Office who will report this email to our IT provider for further investigation.

Unexpected or suspicious email attachments should never be opened. They may execute a disguised program (malware, adware, spyware, virus, etc.) that could damage or steal your data. If in doubt, call the sender to verify. A good rule of thumb is to only open file attachments if you are expecting them and if they are relevant to the work you are doing.

Signs of a Malicious Attachment

- .exe Files: .exe files are executable files - meaning that they can run a program; while .exe files are not inherently malicious, they can be used to install malware on your computer; there's no reason for an .exe file to be shared via email, so if you receive one, you should delete it
    - Google has a filter in place that prevents the sending of .exe files
    - .exe files can also be disguised in .zip folders - if you receive an email with a .zip, and open the folder to find an .exe, you shouldn't run the file
    - Be careful, some attachments might show the icon for a document, powerpoint, etc., but they still have the .exe extension
    - Just because a file isn't an .exe, doesn't mean it's not malicious - there have been instances of macro-viruses that hide themselves inside of Office Documents
- Unsolicited Email/Strange "From" Field: don't open attachments that you're not expecting, or from users who you don't know (be especially cautious of anyone outside of the @silverhillschool.co.uk environment)
- Strange "To" Field: if the email has a long, alphabetical list of recipients , or if the "To:" field is blank, then the email is probably illegitimate, and the attachment shouldn't be opened
- Vague Subject Line/Body: if the subject line or the body text is vague, then the attachment probably is illegitimate
- Missing Salutation: most legitimate emails have some kind of a salutation
- Poor Grammar/Spelling: legitimate emails are carefully proofread before they're sent out; if the email has a lot of spelling/grammatical errors it's probably not legitimate
- Sense of Urgency: (i.e. - "this attachment will expire in 24 hours", "you have an unpaid invoice") most illiterate emails try and create a sense of urgency so that the recipient will download and run the attachment without carefully looking at it

Still not Sure?

If the email has passed the "tests" above, but you're still not sure, alert the Front Office who will contact the school's IT provider. The IT company will advise on whether the email should be investigated in situ or forwarded to them for further investigation.

Whatever you do **DO NOT OPEN** a suspicious (even mildly suspicious) attachment.