



## ***Technology Office***

*181 Encinal Avenue  
Atherton, CA 94027  
650-326-5164 x116  
fax: 650-326-6302*

### **BOARD OF EDUCATION**

**Mark Box**  
**Jeff Child**  
**Deborah Fitz**  
**Maria Hilton**  
**Laura Rich**

**Kenneth Ranella,**  
**Superintendent**

**Jo Sauer Mitchell,**  
**Ass't Supt. of Curriculum  
& Instruction**

**Diane White,**  
**Chief Business Official**

**Olivia Mandilk**  
**Dir. of Student Services**

**Jim Bowlby**  
**Dir. of Technology**

**Kathryn Tinio**  
**Human Resources**

**Ahmad Sheikholeslami**  
**Dir. of Facility Planning  
& Construction**

**Dennis Hatfield**  
**Supervisor, Maintenance,  
Operations &  
Transportation**

### **Attachment Guidelines**

An email attachment is a file or document that gets sent along with ("attached to") an email message. Since email messages consist of text only (or sometimes html code to add pictures and formatting), it is sometimes necessary to send an attached file with additional data or formatting to someone. The file might be a Word document, an Excel spreadsheet, a picture (usually in "jpeg" or "gif" format), or something else.

You should always be careful if you receive an unexpected attachment, because this is the most common way that viruses are spread. Some attachments are programs that "execute" when you open them. Our email server automatically scans all attachments for viruses and removes them if they are infected. Though we are reasonably secure, you should always be careful when opening an attachment. If you are checking email from a non-district account, you should always scan it for viruses before opening it. (Yahoo mail accounts do this for you automatically.) Note that opening the email message itself (which is just text) generally cannot infect you with a virus.

If you need to send an attachment to someone, there are some general guidelines that you should follow to increase the odds that the file gets through and can be read/opened by the recipient. Remember that email messages pass through many computer systems on the way to their final destination. An attachment is generally "encapsulated" during transit (similar to putting it into an envelope), so that if various computers do things to the "package" as it is traveling, such as a security scan, it will not affect the contents. You also may not know what kind of computer system (Windows, Macintosh, Linux) or software the recipient has. With these things in mind, you should:

1. Always state in the email text that there is a file/document attached and state what type of file it is (e.g. Word document, Excel spreadsheet, jpeg picture).
2. Make sure the file is of a reasonable size (less than 1MB or 1000KB). Big files take a long time to download and take lots of travel bandwidth on the Internet. Some Internet Service Providers will only allow files up to a certain size to be sent or received. With a Word document, you are generally fine if it is less than 100 pages and does not contain lots of graphics. With a picture that you have scanned or downloaded from a digital camera, however, the resolution is generally set high for print quality, which makes a large file. If you only intend for someone to view the picture on their computer, use an image editing program (such as Photoshop or one that came with your camera or scanner) to reduce the resolution to 72dpi. This is the standard for pictures viewed on the web.
3. Always name the file with an extension at the end (e.g. ".doc" for Word documents, ".xls" for Excel spreadsheets, ".jpg" for jpeg pictures). Though this is generally a DOS/Windows convention, it helps systems recognize the file (so that it is easier to open), and prevents some security systems from flagging your attachment as an "unknown" type and, therefore, potentially dangerous.
4. Make sure there are NO SPACES or unusual characters (such as punctuation, dashes, slashes) in the file name. These symbols may have a particular meaning to the computers that pass on your message, and files with spaces may be flagged as a potential security threat.
5. Keep the filename to 8 characters or fewer (not including the extension). This is not as critical since most systems now handle long file names consistently, but it may help to insure that your file gets through in a readable form.