



ENCRYPTION

When sending or responding to sensitive professional email communications, the Ethics Committee suggests that AATA members encrypt such email in order to protect professional confidentiality. Instructions on how to encrypt have been prepared by Amanda Alders, chair of the Technology Committee.

Elizabeth Stone, LP, LCAT, ATR-BC, Ethics Chair

The following links have encryption options, which would enable supervisors and supervisees to e-mail safely regarding clients:

<http://www.hushmail.com/>

<http://www.zipmail-for-yahoo.com/>

<http://www.instructables.com/id/Send-and-Receive-Encrypted-E-mail-in-Gmail/>

<http://www.getmailcloak.com/>

Securing email involves 1.) Digitally Certifying the e-mail and 2.) Encrypting the e-mail for both the sender and recipient.

STEPS:

1.) Digitally Certifying

Digital Certificates or signatures verify the identity of the sender and recipient. To get a digital signature, you will have to apply for one at a company, which supplies free digital signatures ([Thawte](#) and [Comodo](#)). You could find other free companies by Googling, "digital certificates."

[VeriSign](#) offers certificates for commercial purposes and charges.

2.) Encryption

When you encrypt a mail message, the receiver will be the only person who may open the e-mail or access the information. In order to encrypt messages, both you and the recipient, should have first exchange "Digitally Signed" messages.

To send the message:

Click the "New Mail" button and click the "Sign and Encrypt" buttons. Encrypted emails can be opened on a computer with a "certificate" installed (see above).

Compiled by: Amanda E.M. Alders, M.S., ATR
Technology Chair
The American Art Therapy Association