School of Visual Arts

Email Encryption Policy	Created: 10/25/2019
Section of: Corporate IT Policies	Target Audience: Staff
CONFIDENTIAL	Page **1** of **3**

SVA Email Encryption Policy and Guidelines

The Administrative & Network Services Office has implemented a new service – "Virtru" – which integrates with the existing Gmail and Google Drive platform to give users the option to send emails and share files with people inside and outside of the SVA environment in a secure manner.

What is "secure email"?
Secure email provides a way to send encrypted messages containing sensitive and/or private data to people inside and outside of SVA (i.e. to addresses other than @sva.edu).

When should you use "secure email"?
While it is a good rule of thumb to avoid using email to send sensitive or private information if possible, if you need to provide the information to a person inside or outside of SVA, secure email now provides you with a solution.

Before using email to share sensitive and/or private information, it's always important to consider government and industry laws and regulations, College and local policies, guidelines and practices.

Use of SVA's secure email system is intended to address the need for communicating high risk/confidential data (i.e. personally identifiable information or private data) in a safe and secure manner and in compliance with the Gramm-Leach-Bliley Act of 1999 (or **GLBA**), European Union General Data Protection Regulation of 2018 (or **GDPR**), California Consumer Privacy Act of 2018 (or **CCPA**), Health Insurance Portability and Accountability Act of 1996 (or **HIPAA**), Family Educational Rights and Privacy Act of 1974 (or **FERPA**) and US PRIVACY SHIELD of 2016. However, it can also be used to secure other sensitive information including, but not limited to, personal identifiable information (PII), financial or student information. You are required to use secure email whenever you send a message that contains sensitive information such as PII to a recipient inside or outside of SVA (i.e. to addresses other than @sva.edu).

How to send secure email?
By default, all users in the sva.edu domain can read encrypted emails. In order to be able to send encrypted emails you need to contact helpdesk@sva.edu to request an upgraded account. Virtru is integrated with the Gmail interface. Please navigate to the link below for instructions how to add it to your Google Chrome browser.

https://support.virtru.com/hc/en-us/articles/115012442108-Installing-and-activating-Virtru-for-Gmail

Can users who need to communicate securely outside SVA initiate secure messages to me?
No. The sva.edu account holder will need to initiate the encrypted email to the external recipient. All subsequent communication following the original email thread will remain encrypted end-to-end (including any attachments). Encrypted emails can be set to have an expiration date and/or protected against email forwarding. The sender always controls the encrypted message.

What will happen if I attempt to encrypt an email to someone with a SVA email address?
Email encryption compliance includes two separate requirements: **encryption in transport** (messages should remain encrypted in transit while routing to the end recipient) and **content encryption** (message body and attachments).

Emails sent within the SVA email system is secure during transport by default. This satisfies the general compliance requirement for “encryption by design”. Virtru email encryption should be enabled if the content of the message transmitted falls into the PII / private data category for additional protection of the data being sent.

Can I send attachments?
Yes, the total size of attachments you send must not exceed 25 megabytes.

Are encrypted attachments safe?
All files attached in Gmail or shared via Google Drive that are encrypted by Virtru have persistent protection. If downloaded or forwarded to someone other than the intended recipient, access to see the content will be denied. Only the intended parties can access the files.

Can the recipient forward the message?
Yes, if forwarding is enabled in Virtru Settings prior to sending the message.

Why does the message show an expiration date?
In Virtru Settings, a message expiration date can be set prior to sending. The recipient can still read the message and download the attachments while it’s valid. Once expired, the message cannot be accessed.

Can the message be read on a smartphone?
Yes, via an HTML browser like Safari and Chrome. The secure email will launch a web page where the message can get read.

What is “sensitive data”?
Sensitive data is defined as information that is protected against unwarranted disclosure. Access to sensitive data should be safeguarded. Protection of sensitive data may be required

for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations.

Sensitive Information includes all data, in its original and duplicate form, which contains:

- Personal Information, as defined by the North Carolina Identity Theft Protection Act of 2005
- Private Data, as defined by the European Union General Data Protection Regulation of 2018
- Protected Health Information, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Student education records, as defined by the Family Educational Rights and Privacy Act (FERPA)
- Customer record information, as defined by the Gramm Leach Bliley Act (GLBA)
- Card holder data, as defined by the Payment Card Industry (PCI) Data Security Standard
- Confidential personnel information, as defined by the State Personnel Act
- Information that is deemed to be confidential in accordance with the North Carolina Public Records Act

What are special categories of private data as defined by GDPR?
GDPR special category data is personal information of data subjects that is especially sensitive, the exposure of which could significantly impact the rights and freedoms of data subjects and potentially be used against them for unlawful discrimination. Information containing this type of data is subject to the same encryption requirements as PII and private data.

GDPR special category data includes the following information:

- Race and ethnic origin
- Religious or philosophical beliefs
- Political opinions
- Trade union memberships
- Biometric data used to identify an individual
- Genetic data
- Health data
- Data related to sexual preferences, sex life, and/or sexual orientation

For additional questions or help please reach out to helpdesk@sva.edu or via phone at (212) 592-2400 option 1.