City of New York

Administration for Children's Services

Policy 2010/07

SUBJECT:	**Security of Confidential, Case Specific and/or Personally Identifiable Information**
APPROVED: John B. Mattingly	**PAGE: 1 of 4 (1 attachment)**
DATE: December 6, 2010	**IMPLEMENTATION RESPONSIBILITY: All ACS and Provider Agency Staff**

PURPOSE: In the course of our service to families and children, ACS and provider agencies staff work with confidential client data. This policy articulates standards and best practices for protecting the security of such materials.

SCOPE: These policy guidelines apply to all ACS and provider agency staff. The implementation of this policy is the responsibility of all divisional and provider agency managers. This policy is effective immediately.

POLICY: **Security of Confidential, Case Specific and/or Personally Identifiable Information**

All Children's Services and provider agency staff should be aware of the need to protect case specific information that identifies clients and the types of services being provided to them. Managers and supervisors should share and discuss this policy with their staff so that it is understood and followed by them. To maintain the security of case and individual client information, all ACS and provider agency staff are required to communicate through CONNECTIONS, whenever possible, when sharing such data.

The CONNECTIONS system is the most secure method of sharing case information. By assigning staff a role in the case, he/she will be able to access the information with ease without compromising the client's confidentiality. Staff should use the *To Do* tool and/or if possible enter a progress note in CONNECTIONS, to allow access to the information that they wish to convey.

Best Practice Guidelines for Securing Confidential Information if CONNECTIONS Cannot be Utilized

If CONNECTIONS cannot be utilized, staff should follow these guidelines in selecting and using another mode of data/information sharing.

*A. **Non Electronic Data Sharing Methods***

Non Electronic modes of exchanging information should be utilized where

feasible; examples are:

i. using phone conversations to share information;
ii. hand-delivering the information; or
iii. mailing the information via a surface carrier (e.g. USPS, UPS etc.)

B. Electronic Data Sharing Methods

If for efficiency, record keeping or other reasons, it is necessary to share data in electronic form, the following options are available to staff:

1. **Establishing an Electronic Shared Folder**

   If possible, use a shared folder that is designated solely for users of the information within the folder. Using a shared folder with appropriate security permissions allows users who regularly use the same computer information system to review information and documents without the need to mail or send them.

   If sharing a folder, staff should take steps to protect the integrity of the data as this is a very important part of electronic communication. If installed software that allows password-protecting WORD documents or converting the document to PDF format is available, staff should consider utilizing these options on the documents before sharing them. This will ensure that electronic communication is not easily modified by the recipient and then shared by others, See Attachment 1 for further information on **how to utilize these security options.**.

2. **Faxing**

   When faxing confidential or case specific information, always verify the fax number, alert the person to whom the data is being sent before it is faxed, and confirm that the information was received by that individual. Use a cover sheet when faxing confidential information. If possible, fax to a fax machine in a secure location.

3. **E-mail**

   Please note that there are security risks associated with using email to share confidential, case specific and/or personally identifiable information; therefore, users must always exercise caution. Best practice suggests that the following guidelines be utilized to the extent possible:

   - Send information to individual recipients instead of using a distribution list.

   - When filling in the subject line in an email use information that is not confidential, case-specific or personally identifiable.

   - In the subject line, never use a person's full first and last name; use only first name and last initial or case number. If necessary, it is permissible to use the combination of both first name and last initial and case number.

- In cases when the client's name is unique and the use of his/her name in the subject line could easily identify the individual, the sender of the email may not include that name. Instead the sender of the email must only use the client's first and last initials along with the client's case number.

- Full case information should not be disclosed in email correspondence to the extent possible. Use information that identifies the specific case for the recipient with as little personal information as possible. For example, a CONNECTIONS Case Number would be sufficient for someone who has CONNECTIONS access, along with a secondary partial identifier such as "Jane. D." (first name and initial of last name) to ensure that the case is identified correctly.

- **Before** hitting the **Send** button, it should be ascertained that the name of the desired recipient is accurate.

NOTE: There may be people in an Address List with the same or similar names. This heightens the risk of sending information to the wrong person. In order to confirm the identity or email address of the person in the Address List, right click on the name and then on Properties. If there is still uncertainty, call the person first to verify that they are the appropriate recipient of your email.

- Remind the person(s) to whom the information is being sent that it is not to be forwarded without consideration of all issues contained in this policy and procedure. This can be done through a Signature Security Tag (created by clicking on Tools/Options/Mail Format. An example is:

  Jane Doe
  ACS [Title]
  212-555-5555
  This E-mail, including any attachments, may be intended solely for the personal and confidential use of the sender and recipient (s) named above. This message may include advisory, consultative and/or deliberative material and, as such, would be privileged and confidential and not a public document. If you have received this e-mail in error, you must not review, transmit, convert to hard copy, copy, use or disseminate this e-mail or any attachments to it and you must delete this message from any device or media where it is stored. In addition, you are requested to notify the sender by return e-mail that you received it in error.
  Please do not print this email unless necessary

- When attachments are used to share confidential, case specific and/or personally identifiable information, staff should to the extent possible, password-protect the attached files before sending them out. See Attachment 1 for information on password protecting a WORD document or Excel Spreadsheet.

- To the extent possible, share passwords through telephone or disclose the password in person to avoid sending both, the password protected files and the password inadvertently to someone who was mistakenly

included on your distribution list.

- Staff may also use an agreed upon standard for passwords. It might include the day sent plus the case number or some derivative that would be easily remembered by the recipient but not easily guessed by someone trying to crack the password.

For further information on creating a shared folder or password protecting a document please open a Help Desk ticket via the ACS Intranet or contact the Help Desk at (877) 227-5566.

• Converting Files into PDF

1. Click on your **Internet Explorer** on your desktop or from a Provider Agency go on the **ACS Intranet**.
2. Click on **Tools**
3. Click on Convert to **Adobe PDF** Online
4. Select document to convert from the Browse drop down menu
5. Type your email address into the box provided
6. **Send** request

The converted file will be delivered to your email address that you can rename and file.

•Password-Protecting a WORD Document or Excel Spreadsheet that you are sending:

- Open the document.
- On the **Tools** menu, **select Options**
- Select the tab labeled **Security**
- Under heading file encryption options for this document, (file encryption settings for this workbook for Excel) in the **Password to open box,** enter a password
- Click **OK**
- In the **Confirm Password** dialogue box where it says **Re-enter password** to open, (**Re-enter password** to **proceed** for Excel) re-enter the password
- Click **OK**
- ***Email*** *the password protected document or spread sheet*
- ***Call*** *the person to whom you are sending the document and give him/her the password*

NOTE: Do not email password if you have shared a password-protected document through email.