Young London Matters

Government Office For London
Riverwalk House
157-161 Millbank
London
SW1P 4RR

For further information about Young London Matters contact:
younglondonmatters@gol.gsi.gov.uk

www.younglondonmatters.org

Our Partners

MAYOR OF LONDON

department for children, schools and families

London development centre

DH Department of Health

ALDCS Association of London Directors of Children's Services

LONDON COUNCILS

NCVCCO

NHS London

capital ambition

Your Rights! Your say www.rights4me.org

Healthy Schools

cwdc Children's Workforce Development Council

VCS engage

TP-NST

VJB

April 2009

Young London Matters

GOVERNMENT OFFICE FOR LONDON

Mobility and Young London

Annex 4: Sharing Information Securely

ALDCS
Association of London Directors of Children's Services

Making Every London Child Matter

Annex 4: Sharing Information Securely

This annex outlines regional guidance for sharing information securely.

It is part of a series of annexes from *Working Across Borough Boundaries - The London Common Assessment Framework (CAF) Protocol*.

Background

It is the duty of every person who handles personal information to ensure that it is kept safe and secure and only shared with those who have a legitimate reason to see it. When information is in transit between individuals or information systems it is at risk of loss, damage, theft and inappropriate or accidental disclosure.

This guidance has been adapted from the guidance developed by London borough of Merton.

Important note:

THIS GUIDANCE DOES NOT OVERRIDE THE INFORMATION GOVERNANCE PROCEDURES OF INDIVIDUAL ORGANISATIONS OR CHILDREN'S TRUSTS. Please consult your own local procedures and be guided by your own professional code of conduct.[1]

Initiating a common assessment

Prior to initiating a common assessment, as a minimum requirement, a check must be made to find out if one already exists. This should also include a check to see if social care services are involved or have had prior involvement.

Until ContactPoint is available to all practitioners it is recommended that:

- any practitioner seeking to identify if a CAF is underway should contact their borough lead CAF contact;
- the lead CAF contact will need to be able to satisfy checks that the person making the request is a practitioner with a legitimate reason; and
- the lead CAF contact will contact their counterpart in the other authority[2] using LARA[3] where necessary.

If there are other practitioners or a Lead Professional currently working with the child, any information should be shared between them (with consent of the child or family) in order to gain the full picture of the child's situation. This will enable the practitioner to determine whether they need to remain involved, join an existing Team Around the Child or begin a common assessment.

[1] This guidance can be applied to sharing information securely both within and across authority boundaries
[2] authority of residence
[3] LARA is a national database of ContactPoint implementation managers and CAF coordinators. If LARA is removed once ContactPoint is available to ALL practitioners the lead CAF contact can be accessed by the authority's service directory

Sharing information

- As with any other personal information, a practitioner undertaking a common assessment should only share information with a third party with the explicit consent by the child, young person and/or family to do so, unless in the practitioner's judgment there is sufficient public interest to share information without that consent.
- Good practice indicates that the child, young person and/or family should be aware of how information may be shared. This should be noted on the common assessment or recorded on a sharing information register.
- Practitioners should only share information with a third party where they have confirmation that the requesting practitioner has a legitimate reason for requiring that information and the consent of the child, young person and family, unless they judge there is sufficient public interest as above. Where there are any doubts, this confirmation should be provided by the lead CAF contact in the authority where the practitioner is based prior to any sharing.

Please refer to Annex 1 for guidance on the process to use when working across authority boundaries.

Sharing information securely – practical steps

The following section is a step-by-step guide for practitioners who need to share information via post, telephone, fax or email or in person.

Sharing personal information by Post

Posting documents can be one of the most secure ways to securely exchange documentation. If you are a practitioner sending information by post, you must:

- confirm the name, department and address of the recipient;
- seal the information in a robust envelope;
- mark the envelope '*Private and Confidential – To be opened by Addressee Only*' and place this inside a larger envelope with only the correct name and address on it - this adds an additional level of security as the package is not easily identifiable as 'valuable' and administrative staff should only open the outer envelope;
- consider sending the package as registered or 'signed for' delivery or by courier if confidential;
- send the information by recorded delivery when appropriate;
- ask the recipient to confirm receipt; and
- record the disclosure.

Registered post is the best way to send confidential data on an encrypted CD.

Different levels of security can be used depending on the information being sent:

- Reliable transport couriers should be used at all times. Consult with your Post Room.
- Confidential information sent electronically must be protected by encryption.
- Packaging must be adequate to protect the contents from damage during transit.

Sharing information by Telephone

If you are a practitioner who has received a request to share information via the telephone, you must first confirm that the practitioner requesting has a legitimate reason for contacting you.

Once you have confirmed this:

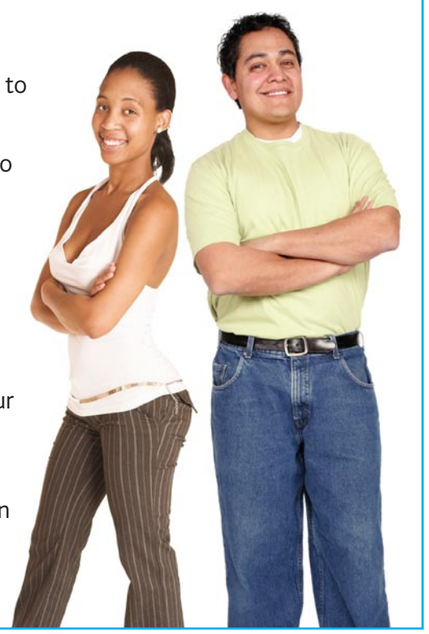
- be sure you know who you are talking to - where possible use the main switchboard number of their organization and confirm with the operator the name, job title, department and organization of the person with whom you wish to share information;
- do not share information when a return telephone number cannot be supplied - call the practitioner back via the switchboard;
- only provide the information to the person who has requested it - if they are not there you should leave a message for them to call you back;
- do not leave a message with someone else or on a voicemail;
- be aware of who might overhear your call;
- keep a record of any confidential information disclosed during the call; and
- record the time of the disclosure, the reason for it and if appropriate, who authorized it.

Sending information by Fax

Paper documents are often sent by fax. Precautions must be taken when sending information by fax because the receiving machine may be sited in an open office, meaning the document is visible to other staff, contractors or visitors. Where possible any information should be shared via a dedicated CAF FAX.

If you are sending information by fax you must:

- telephone the recipient of the fax to let them know you are about to send it;
- check the fax number. If the information is confidential ask them to wait by the fax;
- consider asking the recipient to confirm receipt of the fax; or call them to ensure the fax has arrived;
- use pre-programmed fax numbers where possible to reduce the chance of the fax being sent to the wrong machine;
- ensure that you use an appropriate fax cover sheet. Make sure your cover sheet states who the information is for, and mark it 'Private and Confidential';
- ensure you do not refer to the names of the person(s) concerned in the subject heading or on the cover sheet of the fax; and
- keep a record that you have sent the fax.



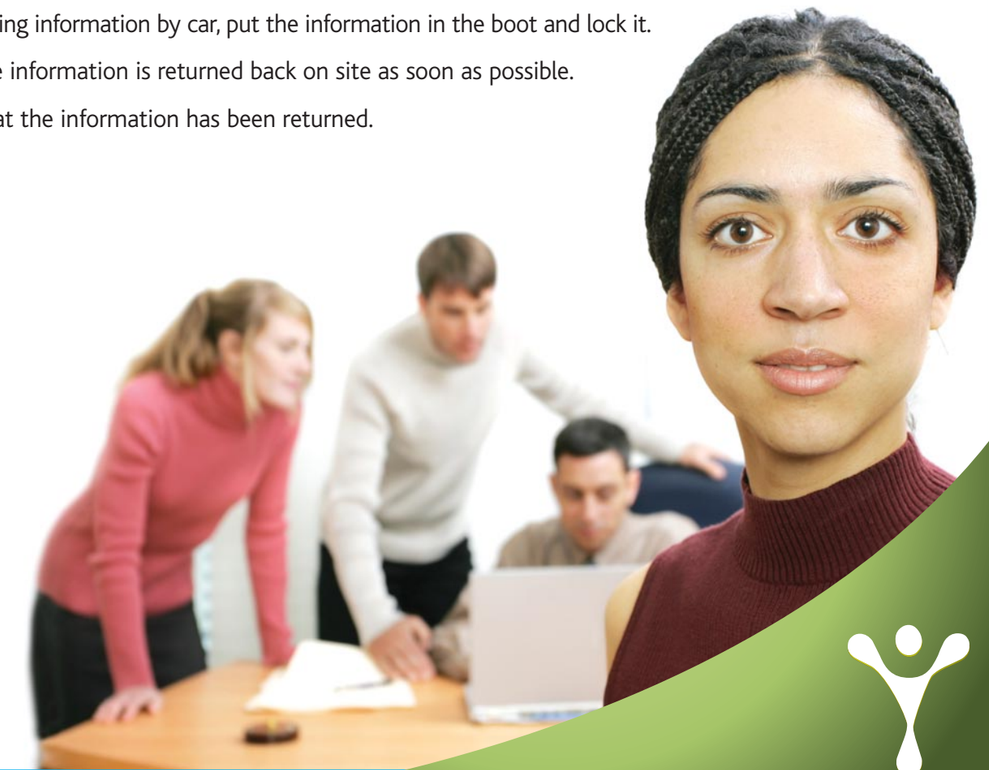
Receiving information by Fax

- if the information is not for you, either pass it to the proper recipient or inform the sender - please do not ignore it;
- consider the location of your fax machine - Is it in a secure environment?;
- If your fax machine is not in a secure environment or you receive faxes outside office hours, you should consider a 'fax to e-mail' solution.

In Person

Confidential information may be delivered personally by members of staff. Such information may be held in paper or electronic form. Where laptops, PDAs or other electronic devices are used precautions must be taken to ensure the security of your agency's IT systems as well as any data held on the device itself.

- Personal information should only be taken off site where necessary, either in accordance with local policy or with the agreement of your line manager.
- Log any confidential information you are taking off site and the reason why.
- Paper based information must be transported in a sealed file or envelope.
- Electronic information must be protected by appropriate electronic security measures – password or encryption.
- If transferring information by car, put the information in the boot and lock it.
- Ensure the information is returned back on site as soon as possible.
- Record that the information has been returned.



Sending information by email

Huge amounts of information are sent by email, within and across agencies. Whilst internal messages are reasonably secure (e.g. within the council or within health services secure platforms), those sent to external addresses are not considered secure enough for confidential information. Confidential information must be sent by other methods, some of which are outlined in this section.

When sending information via email, you should

- ensure all recipients need to receive the information - think twice before responding to a group email or copying others in;
- confirm the name, department and email address of the recipient;
- mark the message 'confidential';
- do not include confidential information in the subject field; and
- use a secure email connection and ask the recipient to confirm receipt (e.g. use delivery and read request settings).

Using password protected files

- If you have to send personal information to an external recipient, use a password protected file. Further, when this information is confidential, encryption should be used. One option is to use WinZip: some guidance on using WinZip for encryption follows below but DO consult your own agency for further guidance, or other options, as well.
- Remember to use a different password to anything you may use for other tasks because you will have to share the password when you disclose the document.
- Always save the passworded version of the document as a new file and retain the original safely. IT Services will not be able to open passworded or encrypted documents without the password. Passwording and encryption are not necessary for information shared between those within a secure platform (e.g. within the council, within health, within the police: further in Secure Email below).
- Do not send the password by the same email - either send by separate email, or preferably use the telephone, making sure you know who is receiving the information.
- Record what information has been sent.
- After receiving a password protected file, re-save the information without the password in a new secure place. Do not rely on remembering the password.
- Save an audit trail of your email communications. This could mean saving a copy of all sent and received emails in a separate folder.

Using WinZip to encrypt information

Use WinZip to encrypt copies of files that you are sending or taking out of your organisation, but not for files which remain on your network. WinZip version 9 or above allows users to use 256-bit AES encryption which is recommended. The recipient will also need WinZip 9 or later, so check this with them first. Earlier versions will handle the older 'zip 2.0' encryption, as will Windows XP.

(Discuss with your IT department, if you don't already have this facility installed: WinZip in a Google search will bring up several options.)

The encryption can be done from within or outside the Office application.

(1) To encrypt the information from outside the Office application:

- Open WinZip (version 9 or later).
- Create a new archive (File menu), navigating to an appropriate location within your filing system, and give it a name.
- In the 'Add' window, locate the file you want to encrypt and highlight it. Tick the box 'Encrypt added files', and click 'Add'.
- If WinZip warns you about the implications of encrypting files, click on 'OK '.
- Enter a password that has a least 7 characters and preferably a mixture of numbers and letters. Re-enter the password to confirm it.
- Ensure 'Mask Password' is checked, and choose the option '256-bit AES encryption'. Click on 'OK '
- In the archive, the filename is followed by an asterisk to show it has been encrypted. Close WinZip.

(2) To encrypt the information from within the Office application:

- Open the application that contains the information to be emailed. (Word, Excel, PowerPoint etc)
- Click 'File ' then 'Open'.
- Locate, then right click the document to be sent.
- Click 'WinZip' then click the option 'Add to (name of the document).zip'.
- It may now be necessary to change the 'File of type' at the bottom of the box to 'All files' to see the new Zip file.
- Right click the Zip file.
- Click 'Encrypt' (cancel the box offering information about the different encryption methods if it appears)
- Enter a password that has a least 7 characters and preferably a mixture of numbers and letters.
- Re-enter the password as requested.
- Ensure 'Mask Password' is checked.
- Check the option '256-bit AES encryption (stronger)' then click 'OK '

Distributing encrypted information

Whichever method you use for encryption, you now have an archive file to send or transport. When sending, let the partner who is to receive the information know the password. This can either be achieved by telephone to a known and authorised person; or by separate email that is acknowledged before the archived information is sent. For regular transmissions, it is recommended that passwords are changed at least every three months.

The recipient will be able to open the encrypted WinZip file using the password already agreed with them at the start of the process.

Sending information by Secure Mail

What is secure email?

- When a regular email is sent between different organisations it is transmitted over the Internet. This means that the contents of that email are not particularly safe. Email can be intercepted or misdirected, either by accident or for criminal purposes.
- While the risk of interception is quite low – a 2006 estimate placed the number of emails sent daily at 183 billion – the public expect public bodies to keep sensitive personal information confidential. They also expect information that identifies large numbers of people to be protected. Therefore a secure email facility should be used to send information identifying large numbers of people as well as sensitive or confidential information about a single individual.
- Secure email involves sending information to trusted partners through a network of secure, encrypted servers. The secure email facility encrypts the contents of an email when it is sent. This encryption ensures that the email, if intercepted, will be unreadable. Once the email reaches its secure destination it will be decrypted so that the intended recipient can read it.

When should I use secure email?

- An email sent within large organisations such as NHS, Police, Central Government, the court service or within a local authority is secure because it stays within that network's firewall security system. So an email sent from colleague.one@nhs.net to colleague.two@nhs.net is secure.
- Similarly when shared between colleague.three@merton.gov.uk and colleague.four@merton.gov.uk an email will be secure.[4]

Also, sharing across SOME of these platforms is secure – such as for NHS, Police and Central Government who are all part of the Governments Secure Community. Thus colleague.five@met.pnn.police.uk can securely exchange with colleague.one@nhs.net

BUT sharing between any of those above within that Government Secure Community platforms with a local authority colleague, such as colleague.one@nhs.net sharing with colleague.four@merton.gov.uk, is NOT secure because the bridge between these separate secure platforms is through the internet which is not itself secure.

[4] Please note that this may not apply to all London local authorities therefore you must check with your lead CAF contact.

Sending information by Secure Mail

HOWEVER, a facility provided by the Criminal Justice IT system (CJIT) called CJSM (Criminal Justice Secure Mail) allows for secure exchange between local authorities, education and some Third Sector organisation with the above group within the Governments Secure Community platform.

Who has secure email?

Contact your lead CAF contact to find out if you have access to a secure email address.

What addresses can those with CJSM addresses send email to securely?

Other organisations that are signed up to secure sharing with CJIT system include those shown below:

Organisation	Normal email Suffix	email suffix for secure sharing with CJSM
NHS	@nhs.net	@nhs.net.cjsm.net
Metropolitan police	@met.pnn.police.uk	@met.pnn.police.uk.cjsm.net
Government depts	@gsi.gov.uk	@gsi.gov.uk.cjsm.net
Other Councils	@gsx.gov.uk	@gsx.gov.uk.cjsm.net

How do I (with CJSM address) send secure email?

To send to someone with an @nhs.net or @met.pnn.police.uk email address you need to add the secure email suffix @nhs.net.cjsm.net to the address field e.g. Joe.Bloggs@nhs.net.cjsm.net

Can I add .cjsm.net to any .gov.uk address to make it safe?

No, not automatically. An @authority.gov.uk email addresses needs to be registered with CJSM before it becomes secure.

Before sending confidential information to @borough.gov.uk address you need to check first with the recipient whether they have a cjsm.net address.

If they do not you need to use another method of transfer. See the other procedures above for more details on options.

Are attachments protected?

Attach it to an email and send it to a cjsm.net address, it is likely to be rejected by the virus checking system and returned to you. Attachments sent through the CJSM system do NOT need to be encrypted. You cannot receive emails from non-secure email systems at a cjsm address.

How can I tell if an email has come through the CJSM system?

If an email comes through the CJSM system the Subject Field will begin with [CJSM]

What if I need to send information securely to someone who does not have secure email?

You need to use another method of transfer. See the above procedures for more details on options.

Blackberry, Memory Sticks, CD's and other removable media and mobile devices

Mobile Devices include Blackberry, iPod, mobile phones and other gadgets. Removable electronic storage media include CD or DVD, Memory stick and even floppy discs. These devices and media are particularly vulnerable to loss or theft. Any confidential information on them must be protected by 256 bit AES Encryption in accordance with local policy. See WinZip guidance above as one option. General guidance may be found at http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf

Additionally, the following principles must be followed when using removable media

- The information must be backed up automatically, so that if the device is lost a risk assessment will facilitate appropriate follow-up action.
- Any loss must be reported immediately.
- Information must be securely deleted after use. It is not acceptable to carry confidential information on a mobile device or memory stick any longer than necessary. CD's or DVD's should be broken before disposal.

National eCAF

In July 2007, the Government announced that it would provide assistance to front-line professionals in children's services by implementing a single national IT system to support the Common Assessment Framework (CAF). The National eCAF system is the e-enablement of CAF.

National eCAF

- National eCAF will allow a practitioner to electronically record and share CAF information securely, with the consent of the child, young person or family.
- It will give practitioners from different sectors, who are approved and trained to use the system, appropriate access to key information concerning the assessment, action plans and progress reviews. This will allow them to participate in the delivery of the most appropriate services.
- In order to gain access to the episode information on National eCAF, practitioners will have gained explicit consent from the parents or carers and/or the young person who is the subject of the CAF episode.
- National eCAF will be deployed in a phased approach and the DCSF is working with a National eCAF Early Adopters Group to help shape the overall implementation approach. It is expected that the system will begin to be available from 2010.