Information Sharing

How to share information securely

How to share personal information securely, on a case-by-case basis

This guide describes how to share personal information securely and professionally, on a case-by-case basis, via telephone, hand, post, email, using removable electronic devices or by fax, each of which is described below.

It should be read in conjunction with the other Information Sharing 'How to' guides, *Information Sharing: Guidance for practitioners and managers*[1] and any relevant local organisational or professional guidance.

This guide is for practitioners and managers who may have to make decisions and share information on a case-by-case basis. It does not relate to bulk or pre-planned sharing of information between organisations or systems. This guide describes best practice; however you must make sure you follow your organisation's information security policies and procedures.

Best practice principles for sharing personal information securely

Appropriate technical and organisational measures should be taken to prevent unauthorised or unlawful access to personal information, and to prevent accidental loss, destruction or damage to personal information. For example, the Government's Protective Marking System[2] – e.g PROTECT, RESTRICTED, CONFIDENTIAL - is designed to ensure that access to information is correctly managed and safeguarded.

In deciding the most appropriate way to share personal information and the level of security required, you must always take into consideration the sensitivity of the information and the urgency of the situation, i.e. take a risk based approach to determining appropriate measures.
If you are unsure of how to share information securely you should consult your manager or information security officer.

[1] *Information Sharing: Guidance for practitioners and managers* (HM Government, 2008) http://www.education.gov.uk/publications/standard/publicationDetail/Page1/DCSF-00807-2008
[2] *HMG Security Policy Framework* (May 2010) http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-security-policy_0.pdf

Department for Education

When sharing personal information, you must ensure the recipient of the information understands:

- the purpose for which the information is being shared; and
- any limits to consent given, i.e., what information may or may not be shared and the circumstances under which it may or may not be shared with other agencies; and
- the need to ensure that any further handling of the information is fair and secure.

Sharing personal information securely by telephone

- Verify the name, job title, department and organisation of the person requesting the information and the reason for the request.
- Take a contact telephone number, preferably a main switchboard number. Try to avoid a direct line or mobile telephone number wherever possible. If you are in any doubt, confirm the requestor's identity with their organisation.
- Consider whether the information requested can be provided in response to a telephone request and in a telephone conversation. If in doubt, tell the enquirer you will call them back later.
- Ensure that your conversation cannot be overheard by anyone who should not hear it.
- Provide information only to the person who has requested it (do not leave information as a message or share with another).

Transporting personal information securely by hand (only where completely necessary)

- Only where completely necessary, should personal information be taken off site by hand.
- Record when you are taking any personal information off site, the reason(s) for doing so and the date when the information was returned, if appropriate.
- Paper based information should be transported in a sealed file or envelope.
- Electronic information must be protected by appropriate security measures (see section below on using removable electronic devices).
- Information should be kept safe and close to hand. Never leave information unattended unless properly secured.
- When transferring information by car, ensure it is placed in the boot and is kept locked.
- Return the information to your site as soon as possible and file or dispose of it securely.

Sharing personal information securely by post

- Confirm the name, department and address of the recipient.
- Seal the information in a double envelope, ensuring the packaging is sufficient to protect the contents during transit.
- Mark the inner envelope 'Private and Confidential – To be opened by Addressee Only'.

- Make sure that there is nothing on the outer envelope that would indicate that it contains personal information.
- Ensure a return address is included on both the outer and inner envelopes in case it has to be returned for some reason.
- When appropriate send the information by recorded delivery or by locally approved courier;
- When necessary, ask the recipient to confirm receipt.

Sharing personal information securely by email

- Unencrypted email is not a safe or secure method of transporting personal information. To share securely by email the following measures should be applied.
- Confirm the name, department and email address of the recipient.
- Use a secure email connection where possible (if unsure, you should consult your manager or IT department to find out whether you have access to secure email).
- Ask the recipient to confirm receipt e.g. use delivery and read request settings.
- Include the personal information in a document to be attached to the email, save it as "Read Only" and use encryption or electronic document password protection. Inform the recipient of the password by telephone or, once receipt of the document is confirmed, in a separate email. You should follow your organisation's policy on encryption or consult your manager / IT department for further guidance.
- Clearly mark the subject 'Private and Confidential'.
- Save an audit trail of your email communications.

Sharing information securely using removable electronic devices, e.g. USB memory sticks, Blackberrys, CDs

These devices are particularly vulnerable to loss or theft. Your organisation's policies and procedures should provide guidance on when it is appropriate to use portable electronic devices for sharing or storing information and how to protect the information stored in them. You must refer to that guidance to ensure you are following the correct procedures.

The following measures should also be applied when using such devices:

- The information must be transferred securely using the portable electronic devices approved by your organisation.
- Care must be taken with the use of any portable electronic devices as they may not provide adequate protection. If it is necessary to use a portable electronic device then the personal information must be securely encrypted or password protected in line with your organisational policies.
- Ensure any loss or suspected loss is reported immediately.
- After use, the personal information must be securely deleted off the device. It is unacceptable to continue to carry personal information on a portable electronic device beyond the required or necessary time.

Sharing personal information securely by fax

- Telephone the intended recipient of the fax to inform them that you will be sending personal information.
- Ask them to wait at the fax machine and acknowledge receipt of the fax.
- Double check the fax number. Use pre-programmed numbers wherever possible.
- Ensure the fax cover sheet clearly states who it is for, and mark it 'Private and Confidential'.
- If possible, request a report sheet to confirm that the transmission was successful.

Receiving information securely by fax

- If receiving information by fax, consider the location of your fax machine. Is it in a secure environment?
- If not in a secure environment then you must ensure that you are on hand to receive the fax. If you do not have a secure fax or if you receive faxes outside of office hours, you should consider a 'fax-to-email' solution.

Recording the information sharing

No matter how you share the information, you must ensure that you record the date and time, the reason for sharing, what type of information you shared, if appropriate who authorised it, how you shared the information and the recipient's name, job title, organisation and telephone number. For more details, see the companion *Information Sharing - How to record decisions.*

January 2011

Department for
Education