Information Security:
Practical Guidance

1. Sharing service user information over the telephone

Throughout the course of our working day we may receive requests, over the telephone from third parties, external partners and/or providers. We may already be familiar with some of the callers having dealt with requests in the past. It is however vital that we are consistent in our approach to all callers who are requesting information on service users.

Any request for service user information made during a telephone call should not be replied to without identifying who is requesting the information and verifying that you have consent to release information to them.

Staff should ask the caller to confirm their name and contact number and where relevant job title, department, organisation. Personal details of the service user should also be taken i.e. name and D.O.B (reference number if they have it)

Confirm the reason for the request.

Ask for a contact number so that the call can be returned. This must not be a direct line or mobile number if the caller is from an external partner or provider but the organisations switchboard so that the caller's identity can be confirmed.

Confirm with a senior member of staff e.g. Team Manager/Line Manager/Service Manager that it would be okay to share this information. Always ensure if you are returning a call to a third party that you have the service users consent to share their information.

Return the call only to the person who requested the information.

Ensure that you record your name, date and time of disclosure, reason, who authorised it (if authorisation was sought), as well as the recipient's details in the service user's record.

2. Letters & Correspondence

Families move around Leicestershire all of the time, professionals who are directly involved with a child or young person are usually the first to be aware when a family changes address. We may write to a family in one week and the following week we find that they have moved. It is vital to maintain the security of our information that:

.

Staff always check name and address details against the primary database; always use the latest address, don't rely on previous correspondence and if there is a query or contradiction ask the professional involved for clarification.

Staff checks that the address on correspondence matches the envelope – where possible use a window envelope or print an address label.

Take personal responsibility to amend any details that you discover are incorrect.

Amend details on any appropriate databases promptly.

3. Post & Envelopes

Schools and colleges send out and receive a significant amount of post on a daily basis, often related to specific children and students. Ensuring that it reaches its correct destination is often vital and there are many simple steps to ensure that this happens.

For incoming post - date stamp and check against primary database (if appropriate) to ensure it reaches the correct member of staff.

For external post containing personal/sensitive personal information- always use the envelopes with the pre-printed messages 'if you are not the intended recipient please return unopened to sender' and on the back 'If undelivered please return to: [school/college address]'

Take care with window envelopes to ensure that the correspondence has been correctly folded to reveal the full name and address including post code and make sure personal details are hidden.

Posting sensitive personal information– Remember mail that is correctly addressed can still be wrongly delivered, damaged or delayed. consider alternatives where necessary e.g. recorded or special delivery.

Consider the contents of the information you are posting out. Would the letter lose value if some of the more sensitive and/or personal information was removed and consider de-sensitising your information

4. Sensitive and/or Personal Information:

It is usual throughout our working day to process personal and sensitive information.

Are you aware of what this means?

Personal information: identifies a living individual

Sensitive Personal information: identifies a living individual and can be used in a discriminatory way. It is likely to be of a private nature and needs to be treated with greater care than other personal data.

Examples of sensitive information defined within the Data Protection Act 1998 includes: Political opinions, Criminal proceedings, Trade union membership, Ethnicity, Sexual orientation, Gender, Disability, Religion

Always ensure that the safest method of communication is used:

a) emails

Secure email - sensitive personal information to partner agencies should be sent by secure email only. Personal details should be limited to UPN or initials where possible and easily identifiable details should not be included. Follow up the email to

the recipient with a telephone call to confirm the subject of the email, if required.

Take care when replying to external emails – is the recipient correct? Could it be a generic email account? (Consent should always be obtained before responding to a generic e-mail address).

Do not make assumptions. Just because someone e-mails in doesn't mean you can click on reply or forward. Always start a new e-mail, copying and pasting any information that is necessary from the original e-mail.

Is sensitive information contained within the mail? (de-sensitise as much as possible) Delete the email 'trail' if sensitive or inappropriate.

b) Faxes

 Sending Faxes – always ensure that safe haven practices are in place to protect information. To maintain security there are certain safeguards that should be in place, these may include:-

The fax machine being sited in a secure room or cupboard

The receiving organisation has a written policy for handling faxes that the staff have been informed about and understood.

The staff that collect the faxes are responsible for delivering the faxed information to the appropriate person.

Staff should telephone the recipient if they have any doubt regarding the security of the fax machine and ask the following questions to ascertain whether or not the fax machine is a Safe Haven fax.
Is the fax machine sited in a secure office?
Is it used by more than one department?
Are there designated people who collect the faxes?

Where the answers given indicate that the fax is not a Safe Haven the following procedure should be followed.

Telephone the recipient and advise that confidential service user information is about to be sent to them.

Confirm the fax number

Request a receipt from the intended recipient.

Ensure a cover sheet is sent including the name of the recipient and the following wording:

> ***The information contained in this fax is STRICTLY PRIVATE AND CONFIDENTIAL and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender immediately. Thank you***.

Double check the fax number to ensure that the correct number has been dialled before sending the fax

If the fax number is used regularly, ensure that it is programmed into the machine and available on speed dial

Always test speed dial numbers on initial set up by sending a cover sheet

Wait for the machine to confirm transmission

Receiving Faxes – do not leave faxes unattended on the fax machine.

Always make sure that the quality of the ink is readable to avoid making assumptions.

Make sure that the fax machine has enough paper, this avoids missing pages that can either change the context of the information that you are receiving or appear at a later stage when the machine is restocked and not received by the intended recipient.