'How To' Guide: Transferring Personal Information Appropriately

This best practice guide provides managers and staff with practical advice and information to help you determine the most appropriate, safe and secure way of transferring personal information.

The guidance covers the typical methods for transferring personal information by:

- Email
- Post
- In person
- Telephone
- Fax
- Internet

The guidance aims to highlight the potential risks associated with each of these transfer methods and raise awareness of the measures to support the mitigation of those risks. This will enable you to make better informed choices based on the sensitivity and the urgency of the information being transferred.

Remember!

Personal information must only be shared with those who are entitled to see it.

If in doubt always seek advice from your Line Manager or your Service Group Information Management lead.

What is personal information?

In simple terms it means information, whether in paper, electronic (computer), photographic, audio or other format, which relates to an individual (the data subject) and from which that individual can be identified. It can include facts, descriptions, opinions or relationships about an individual.

Why do we need to safeguard personal information?

The Data Protection Act states that organisations must have appropriate technical and organisational measures in place to prevent unauthorised or unlawful access to personal information and to prevent accidental loss, destruction or damage to personal information.

What are the consequences if we fail to safeguard personal information?

If we fail to safeguard information it can affect all those involved:

Data Subject (the individual whose personal information we've failed to safeguard) - if personal information is lost or is accessed by someone who isn't entitled to see it, then the data subject could potentially be at personal risk, suffer damage to their reputation, fraud or identity theft.

Staff Member - The Council has a number of Information Management policies and procedures in place which govern how we manage information and helps us to comply with the requirements of the Data Protection Act. If these policies are breached, it may be necessary to undertake a formal investigation.

The Organisation - The Information Commissioners Office, who oversees the Data Protection Act, can take action against an organisation for breaching the Act. In serious cases this may include issuing a monetary penalty notice of up to £500k.

Deciding on the most appropriate transfer method.

Deciding on the most appropriate way to transfer personal information and the level of security required must be done on an individual basis. You must always take into consideration:

- The **sensitivity** of the information
- The **urgency** of the situation and the tools available to you
- The potential risks associated with each transfer method

Sensitivity of the information

Always consider the **sensitivity** of the information you're sending and ask yourself the following questions:

- Does it contain personal information?
- Does it contain personal sensitive information (e.g. racial or ethnic origin, political opinions, religious beliefs, trade union membership, medical details, sexual orientation, and criminal offences -alleged or convicted)?
- How many individuals does the information relate to?
- What would the impact be if this information was inadvertently shared with the wrong people, lost or stolen? What would the impact be on the data subject?
- Think about the impact it would have on you as the person sharing the information and the Council?

The higher the numbers of individuals involved and the more sensitive the information - the greater the impact it could have on those involved.

Urgency of the situation

Often the transfer method is determined by how quickly the recipient needs to receive the information. It may also be determined by what tools are available e.g. email, secure email, internet etc.

Potential risks should always be considered on an individual basis without exception.

If in doubt always seek advice from your Line Manager or your Service Group Information Management lead.

Potential Risks VS Transfer Method

Some transfer methods carry more risks than others and should be subject to very careful consideration. The table below (appendix 1) provides you with further guidance regarding this.

Record personal information being transferred.

You must always ensure that you record the fact that information has been shared. Include the following information as a minimum:

- Who you shared the information with (be specific)
- The reason for sharing
- If appropriate details of who authorised it
- Details of what information you shared
- The date and time the information was shared
- Why this method was chosen and, if appropriate, what was done to reduce the risks?

You should refer to local protocols or seek guidance from your Line Manager as to where this information should be recorded e.g. client record, customer contact history etc as arrangements will vary between services.

Remember!

Such information may contain personal or sensitive information. Managers should ensure that this information is recorded in a secure environment and is only accessible by those staff that are entitled to see it.

What happens if things go wrong?

If you encounter a problem when transferring personal information you must notify the ICT Service Desk on 01443 425080 and your Line Manager immediately.

The types of things we need to know about are:

- Where personal information has been shared inadvertently.
- Where personal information has been sent or copied to the wrong person.
- Where personal information has been shared excessively i.e.
    - too much information has been shared (over and above what's required)
    - additional information has been shared outside limits of authorisation
    - information has been shared with too many individuals
- Where personal information has been lost, stolen or hasn't arrived at it's intended destination.

For further information on how to report a security breach, please see the Council's 'Information Incident Security' policy on Inform.

Always report lost or missing information immediately.
The consequences of not doing this could be far worse.

Appendix 1

Transferring Personal Information:

Typical Transfer Method	What could go wrong	How to reduce the potential risk of things going wrong
Fax	Greater potential risks are associated with this method as the:- • Fax number could be misdialled. • Fax machine may be shared by others. • Fax output could be collected or seen by others Generally the method should only be used if no other more secure method available and then used with extreme caution.	• Use tested pre-programmed numbers wherever possible. - if this is not possible • Double check the fax number and be careful when dialling. • Double check that the correct information is being faxed. • Phone the recipient to let them know that the fax is being sent. • Ask them to wait for the fax by the fax machine and acknowledge receipt. • Use the Councils standard fax cover sheet. • Ensure the fax cover sheet is fully completed and addressed to an individual officer as opposed to company or department. • Request delivery confirmation if possible.
Telephone Call	• Caller may not be who they say they are • Caller may not be entitled to the information • Others may over-hear the call	• You must verify the caller's details - are they who they say they are? • If the caller is a customer or client and is not known to you, verify their personal details - name, address, DOB, NINO, reference number etc. • If the caller is acting on behalf of a customer or client check there's consent to share the information before disclosing. • If the caller is from another organisation and is not known to you, take their switchboard number and ring them back. If in any doubt, confirm the identity with the organisation. • Ensure that your conversation can't be overheard. • Provide the information only to the person who has requested it and is entitled to receive it - never leave the information as a message with colleagues, another person or on an answer phone.
In Person	• Information could be lost in transit. • Information could be stolen in transit • Risk to personal safety.	• Transfer information electronically on an encrypted device wherever possible. • Only leave the information with the intended recipient - verify their identity upon delivery. • Paper information must be transported in a sealed file/envelope. • Perform double checks to ensure that correct information is being sent. • Information must not be left unattended. • When transporting by car ensure the information is placed in the boot and locked. • If transporting on foot ensure the information is stored out of sight in a bag etc. • Plan your route ahead and go directly to the drop-off point. • If information is being transported on a regular basis go at different times/ days each week/month.

Typical Transfer Method	What could go wrong	How to reduce the potential risk of things going wrong
Email	• The email could be sent to the wrong email address • Emails sent outside of the Council **(that are not encrypted)** are considered generally "unsecure" as emails are transferred via the public accessed internet and could potentially be intercepted.	• Ensure that the email is addressed to the correct recipient • Ensure that the correct information is being sent • Double check you have the correct email address or if selecting from a user list or directory that the correct person is actually selected **(be aware of users with the same/similar names).** • Do not send personal or sensitive information to a distribution list, unless you are absolutely sure that the members are up-to-date. Remember Distribution Lists are managed by you not central systems. • Beware of auto-populate when selecting the recipients name. i.e. an email address maybe suggested to you upon typing the first few characters of a name. Ensure it's the correct address. • Clearly mark the subject heading of your email 'confidential'. • If sending external, personal information must be sent via an attachment and must not feature in the body of the email text. The attachment must be password protected. • Send the password to the recipient separately i.e. in a second email for additional security (a 2 email rule). • Double check that the correct information is being sent. • Request a delivery and read receipt.
Secure External Email e.g. GCSX - enables secure interactions between connected Local Authorities and organisations such as Department of Works and Pensions (DWP). For more information visit the GCSX page on Inform	• The e-mail could be sent to the wrong email address Sender uses normal RCT email account by mistake (rctcbc.gov.uk) • Recipient emails address is not secure. This can be one of the most secure ways to transfer personal/sensitive information providing care is taken when selecting the recipient.	• Ensure that the email is addressed to the correct recipient - double check you have the correct email address. • Ensure that the correct information is being sent • Ensure that the email address is secure (e.g. GCSX.gov.uk etc) - seek support from the ICT Service Desk if in doubt. • Double check you have the correct email address or if selecting from a user list or directory that the correct person is actually selected **(be aware of users with the same/similar names).** • Do not send personal or sensitive information to a distribution list, unless you are absolutely sure that the members are up-to-date. Remember Distribution Lists are managed by you not central systems. • Beware of auto-populate when selecting the recipients name. i.e. an email address maybe suggested to you upon typing the first few characters of a name. Ensure it's the correct address. • Clearly label the email in accordance with the HMG Security Policy Framework (SPF) • Double check that the correct information is being sent. • Request a delivery and read receipt. ****** In the case of GCSX secure email account holders only, the above guidance should be read in conjunction with the GCSX Information Acceptable Use Policy & Personal Commitment Statement ******

Typical Transfer Method	What could go wrong	How to reduce the potential risk of things going wrong
Postal or Courier Service	Potentially higher risk if sending hard copy paper information. Risk can be reduced if using an encrypted portable device. • Information could be lost in transit. • Information could be stolen in transit • Information could be delivered to wrong address/recipient. • Receipt of information can't be guaranteed.	• Encrypted portable devices must be used wherever possible & password provided separately - email/telephone call etc. • Mark the envelope for the attention of a named individual not just the company or department name. • Ensure the address is correct and clearly stated - always include a postcode. • Seal the information in a double envelope. • Double check that corrects information is being sent. • Ensure a return address and contact name is marked on both the outer and inner envelope in case of non-delivery. • Ensure the envelope is fit for purpose and can withstand transit - use tamper proof envelopes where required. • Use recorded or special delivery where appropriate so that the parcel can be tracked. • Request confirmation of receipt.
Website Upload / Database Access Some organisations have secure websites for uploading data to. This can be a lower risk option providing that the database is secure and appropriately managed.	• Could be intercepted if no secure connection. • Site could be accessed by individuals who are not entitled to see the information. • Must rely on recipient to verify that site is secure.	• Seek advice from ICT before sharing any data. It is recommended that transfer by this method is authorised by a Senior Officer and in consultation with ICT • Request written confirmation that site is secure. • User access controls must be in place to limit access to information.

Version No.	Valid From	Valid To	Changes Made
1.0.0	1/7/13	29/5/14	First draft published
1.0.1	30/5/14	12/8/14	Typing errors corrected
1.0.2	13/8/14		Version Control added