Guidance for Handling Personal or Sensitive Information

<table>
<thead>
<tr>
<th>Version</th>
<th>1.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>Information Governance Officer</td>
</tr>
<tr>
<td>Issue Date</td>
<td>12 October 2011</td>
</tr>
</tbody>
</table>
Table of Contents

1. Introduction 1
2. Confidentiality: 1
3. Face to face contact 2
4. Telephone 2
5. Post & Couriers 3
6. Email 4
7. Fax 5
8. Removable Media 6
9. Encryption 7
10. Information for Collection 7
11. Personal information online 8
12. Office Moves 8
13. Travelling with information & Home Use 9
14. Use of contractors & third-parties 10
15. Partners & Government Agencies 10
16. Disposal of information 11
17. Incidents 11
1. Introduction

The Data Protection Act requires that all organisations have appropriate security in place to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage.

The following guidance, which supports the Council’s Data Protection and Information Security Policies, sets out how personal or sensitive information should be processed to ensure our data is properly secured. This includes the transferring, storage and disposal of information and information held on our behalf by contractors.

If you have personal information that is currently stored or transferred insecurely, you must secure it immediately.

All staff handling personal information about members of the public, staff, or individuals from other organisations are required to complete the online Protecting Information training [intranet link to training information].

2. Confidentiality:

All staff have a duty to ensure that information about members of the public, staff and sensitive non-personal Council information is handled appropriately. Sensitive information should only be made available to people authorised to view it.

The following principles should be followed wherever you communicate sensitive\(^1\) personal information:

- justify the purpose for sharing the information
- don’t use information that personally identifies individuals unless necessary
- always limit the personal information to what is required for that particular enquiry
- information should be disclosed on a ‘need to know’ basis
- everyone should be aware of their responsibilities to use and share information appropriately
- if you are unsure check with the business owner (Information Asset Owner) of the information if you have authority to disclose it (bulk transfers of personal data must be approved by the relevant Information Asset Owner prior to disclosure)
- understand and comply with the law (such as the Data Protection Act)
- if unsure then seek guidance on appropriate action

---

\(^1\) Sensitive information, as defined in the Data Protection Act, means information relating to: physical/mental health, ethnicity data, trade union, sexual life, political opinions, criminal proceedings and religious beliefs. Although, information such as National Insurance numbers, bank account and credit card details should also be treated sensitively.
Please consider the following when communicating information:

3. **Face to face contact**
   Take into account that the person you are speaking to may not wish their personal information to be shared in front of others. Please ensure that:
   
   - you are not disclosing or requesting the other person to disclose sensitive information about themselves in front of others, e.g. in reception areas or open-plan offices
   - personal information, in any format, cannot be viewed by others

4. **Telephone**
   Personal information should only be disclosed over the telephone to a third-party where the following procedure has been adhered to:
   
   - the identity of the other party has been confirmed by verification. The type of verification will differ by service and the sensitivity of the information being disclosed. Each service area should determine the type of authentication required for their own particular service information and ensure that all their staff are aware of the requirements. The type of authentication required may also be dictated by external partners or agencies.
   - the reason for requesting the information has been established and is appropriate
   - where appropriate, contact details have been requested and their identity checked by calling the person back via the main switchboard and asking for the person by name
   - provide personal information only to the person who requested it
   - do not leave any confidential information on voicemail or answering machines as it may be accessible by others
   - when in conversation take precautions to ensure that information is not shared inappropriately with others, e.g. when using mobile phones, travelling on trains, etc.
   - sensitive personal information should not be sent via text messaging as it may be accessible by others
5. Post & Couriers

Postal services should be used as follows:

- sensitive information relating to a single individual can be posted using standard Royal Mail letter post.
- care should be taken to ensure envelopes and packaging offer suitable protection and are not overfilled or likely to break open in transit
- check that the item is correctly addressed.
- check that the information being sent is correct and that no other information has been included in error (use PIN code retrieval to collect information from printers where possible and carefully check information collected from printers).
- consider the impact on individuals of the data being lost, e.g., the loss of a lower number of highly sensitive records is likely to have a greater impact than the loss of a greater number of less sensitive records. Where information is provided in bulk or where the information is of a sensitive nature make an assessment on the protection to be applied. If in doubt, err on the side of caution and send via Special Delivery post and confirm delivery.
- consider what procedures should be in place to maintain a record of the collection and delivery of the information.
- tamper-proof packaging is available from the Central Post Room (telephone: 01743 252732) if required.
- when using the internal post to deliver sensitive information, seal the envelope and mark it ‘Private & Confidential’. The envelope should be addressed to a named person and department.
6. Email

Email services should be used as follows:

- when emailing sensitive information to organisations connected to the secure Government network ‘Government Connect (GCSx)’ check that the correct secure email address is used (please refer to Government Connect intranet guidance if you require access to send information via GCSx).

- sensitive information relating to a single individual can be sent via email to the subject of the information if they have requested it to be sent by email or with their agreement.

- care should be taken when addressing email messages to ensure a correct, current address is used and the email is only copied to those with a legitimate interest.

- when you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg “Dave” - the auto-complete function may bring up several “Daves”. Make sure you choose the right address before you click send.

- use (bcc) when sending email to a group of personal email addresses to avoid revealing addresses to other recipients. When you use (cc) every recipient of the message will be able to see the other email addresses the message was sent to.

- be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

- confirm delivery of sensitive information as there is no guarantee that an email will be delivered.

- if information is transmitted and not received by the intended recipient, check that contact details and email address are correct for the receiving party before re-sending.

- consider the impact on individuals of the data being lost or misdirected. Where information is provided in bulk or where the information is of a sensitive nature make an assessment on the protection to be applied. If in doubt, err on the side of caution and send information in an encrypted attachment to the email (please refer to the Council encryption procedures) or check if alternative means of secure data transfer is possible.
• avoid putting sensitive personal information about more than one person in an email as this will lead to difficulties in maintaining accurate and relevant individual client or staff records.
• ensure that records are managed properly and transferred to the proper filing system promptly or destroyed when no longer relevant. Consider if it was your own sensitive information, would you like it to remain in someone’s email inbox?
• when transferring data be aware of who has permission to view your emails or who might be able to view your recipient’s inbox.

7. Fax

Sending sensitive information via fax is acceptable providing appropriate steps are carried out. If it is possible to send the information via encrypted email this method should be used in preference.

The following steps should be followed to when sending a fax containing sensitive personal information:

• telephone the recipient to let them know you are about to send them sensitive information and check someone will be able to collect it
• check whether the receiving fax machine is in an open or shared area
• ask the recipient to acknowledge receipt of the information
• double check the fax number
• if using pre-programmed fax numbers check that you use the correct programmed number
• ensure the fax cover sheet is marked “Private and Confidential” and states clearly who the information is for and provide contact details in case the fax is received in error.
• check to confirm the transmission was successful
• if information is transmitted and not received by the intended recipient, check that the contact details and method of communication are valid for the receiving party before re-sending
8. Removable Media

Mobile and removable media can be classified as any portable device that can be used to store and/or move data. Media devices come in various shapes and forms, including:

- laptops
- memory Sticks (pen drives, etc)
- CDROM
- DVD
- mobile phones
- PDAs (Personal Digital Assistants)
- memory cards (such as those found in cameras, mobile phones)
- magnetic tapes and cassettes
- floppy Disks

Only encrypted laptop computers or memory sticks are permitted for use within the Council. This is regardless of whether the information to be stored on them is sensitive or not. The use of encrypted memory sticks must be approved at Group Manager level.

If personal data has to be stored on other types of portable media, eg CD/DVD, it must be encrypted.

Where it is essential to store sensitive information on removable encrypted media it must be transferred onto the Council network as soon as possible and promptly removed from the device. This is to ensure backups of the data are maintained.

Only Council provided memory devices are to be used by staff. If a memory device is no longer being used and needs to be disposed of please contact the IT Help Desk for disposal instructions.

Power-on passwords must be activated on laptops, mobile phones and PDAs. Managers are responsible for ensuring that all information and storage devices are returned by staff that leave the authority or move to a new role where they no longer need to access the information.

Be aware that information can be recovered from un-encrypted computers and storage devices even after it has been deleted.

Where it is necessary to use unencrypted portable media for operational reasons, a disclaimer form is available via the Information Governance team.
9. Encryption

Encryption is a means of converting information into a format that prevents it being understood by anyone who isn’t authorised to read it. Having a password to access information on a computer does not mean that encryption is being used.

Only Council approved encryption software or memory sticks should be used, where it is necessary to use encryption.

When encrypting information, the Council procedure should be followed. Procedures for using encryption are available on the Information Governance intranet site.

The procedure specifies:
- the minimum level and type of encryption to be used
- password length and format
- sign-off and receipt of information

Please note that simple password protection of documents is not sufficient for the transfer of sensitive information.

10. Information for Collection

Where sensitive information is to be collected:

- agree a procedure to confirm identity of the person collecting the information
- a procedure should be in place to ensure a record is maintained at the point of collection and for confirmation of receipt on delivery of the information
- information should not be left in reception or non-secure areas for collection. Arrange to be contacted when the person arrives to collect the information and provide it personally when the identity of the person collecting the information is confirmed
11. Personal information online

If you are collecting and using personal data online, refer to the 'Personal information online code of practice' issued by the Information Commissioner's Office.


Before posting personal information about someone online, make appropriate checks to ensure you are not putting an individual's privacy at risk, ie when posting planning applications online, only publish the minimum required set of personal data, excluding any personal information contained in correspondence which is not relevant for the planning application.

12. Office Moves

It is the responsibility of local office managers to ensure that all information is collected and delivered as planned, by:

- ensuring all information is removed from cupboards and cabinets.
- packing information in storage crates securely.
- marking the crates appropriately.
- ensuring that all individual crates/items are collected and delivered to the correct location.
- checking all information is accounted for.

Where sensitive information is no longer required it must be disposed of securely and not left in non-secure waste.
13. Travelling with Information & Home Use

When taking personal or sensitive information outside of the office, in any format, please ensure you have permission from the Information Asset Owner in advance. If you are not sure who the Information Asset Owner is, please refer to your Line Manager.

File movements should be recorded, confirming who transferred files in and out of offices.

Help minimise the risk of loss by following these steps:

- ensure items are stored out of sight to deter theft when not in use
- if you are travelling via public transport don’t leave information or equipment unattended
- if records must be temporarily left in unattended cars they must always be out of sight in a locked boot
- files or equipment should not be left in a car overnight

Privately-owned personal computers or personal email accounts should not be used for Council business unless information is considered to be in the public domain.

Homes do get burgled and information can be stolen in the process. Please ensure that:

- all reasonable precautions are taken to maintain confidentiality of personal or sensitive Council information in the home environment.
- sensitive records are removed from the office for the minimum amount of time possible
14. Use of contract & third-parties

If you use another organisation to process personal information on your behalf you must ensure:

- you choose an organisation that offers you guarantees about the security of the processing they will do for you
- you have a written agreement with the organisation that sets out what you allow them to do with the information. At a minimum the agreement should be clear about their use and disclosure of the information and must include security measures that are the equivalent of those you would need if you were doing the job for yourself.
- you must take reasonable steps to check that the organisation is complying with agreed security measures (this can be co-ordinated by the Information Governance Team)

Standard terms and conditions are included in Council contracts although there may be occasions when a separate agreement is required, such as prior to the formal contract being agreed. Model agreements are available on the Information Governance intranet site.

15. Partners & Government Agencies

When transferring or sharing information with other organisations (such as Partners and Government Agencies or Departments) you should be clear in what circumstances you are able to share the information. Please:

- ensure you have authority to transfer the information (all bulk transfers of personal data must initially be authorised at Group Manager level)
- refer to any information sharing procedures that are in place with the organisation
- comply with any additional procedures for securing information in transit that may be specified by that organisation

Please refer to the Information Governance Team if you require assistance.
16. Disposal of information

Information and records should be retained according to the Corporate Retention Schedule. All documents and records retained by the Records Management Service requiring destruction are disposed of by confidential means. Please contact the Records Manager (tel: 01743 252855) if you require assistance and guidance on retention and disposal matters.

Paper-based personal or sensitive information must be shredded or disposed of via secure waste disposal facilities.

All forms of removable media that have been used for storing sensitive information will need to be disposed of securely. Most of the time the best method of disposal is to physically destroy it. This includes:

- CDs/DVDs
- Floppy disks/magnetic tape
- memory sticks, etc.

17. Incidents

If the incident involves the loss or suspected loss of personal information, or other information considered sensitive, the incident should be reported immediately to:

Roy Morris, Information Governance Officer – Tel: 01743 252774

or

Claire Porter, Head of Legal & Democratic Services – Tel: 01743 252763

Other security incidents must be reported immediately to the IT Help Desk:

Tel: 01743 252200

This will enable the Council to manage incidents appropriately.

Failure to comply with the Council’s Data Protection and Information Security Policies may result in disciplinary action being taken.

If further guidance is required on any of the above, please contact the Information Governance team,

Contacts

Information Governance
Tel: 01743 252774/252179

Intranet: http://notes2/intranet/infoman.nsf