PAPER RECORDS
SECURE HANDLING AND TRANSIT POLICY
CORPORATE POLICY
This Policy outlines how the Council and all of its employees must ensure the secure handling and transit of all Paper Records

Any queries arising from this Policy or its implementation can be taken up directly with the Information Governance Unit at informationcompliance@manchester.gov.uk

The Information Governance Team is the responsible for this document and has approved management responsibility for its development, review and evaluation.
1 Introduction and Scope ..................................................................................................................4
2 Taking paper records/hard copy material off-site ....................................................................4
   2.1 Principles to be adopted .........................................................................................................5
   2.2 Approval of requests/Paper Tracking Procedures .................................................................5
   2.3 Managers responsibilities .....................................................................................................5
   2.4 Best practice guidance .........................................................................................................6
3 Dispatching records to staff working from home and home workers ....................................6
   3.1 Protocols to be adopted .........................................................................................................7
4 Training and information .........................................................................................................7
5 Disciplinary action and criminal offences .............................................................................8
6 Reporting a data loss ................................................................................................................8
7 Review .......................................................................................................................................8
8 Advice and Contact Information ............................................................................................8
1 Introduction and Scope

With home and mobile working on the increase we need to be more aware of the limited circumstances in which paper records/hard copy material containing personal or other confidential data may be taken out of, or accessed away from the office. This policy sets out the nature of those limited circumstances and details the security measures that we need to adopt when transporting or storing papers/hard copy material off-site, particularly when such records contain personal or confidential data.

This Policy covers all unencryptable data and includes paper records, photos, 3rd party unencrypted cds/dvds, etc. (which will be referred to as paper records throughout this policy)

These security methods must be robust enough for the type of information in the records. This involves considering in each case:

- the value, sensitivity and confidentiality of the information being taken off-site
- the risk of the information being lost or stolen
- the damage or distress that could be caused to individuals if their personal or other confidential data were to be lost or stolen, and
- the reputational and financial damage that could be caused to the Council or other agencies or organisations as a result of a breach.

This policy applies to all Council employees, including placements and temporary staff, agency workers, consultants or third party contractors accessing or using personal or confidential information held by the Council or doing so whilst otherwise acting on behalf of the Council.

Whilst primarily aimed at ensuring compliance with the Data Protection Act 1998 (“DPA”), the measures in this policy must equally be applied to the transit and storage of other types of confidential information.

2 Taking paper records/hard copy material off-site

All Council employees and others covered by the policy, must always consider whether it is necessary to take paper records/hard copy material containing personal data or other confidential information off-site. The reasons for taking such paper records off-site must always be one of necessity and not convenience.

Taking paper records off-site should only happen when it is absolutely essential to do so and there is no alternative method for accessing or recording the information required. Where paper records have to be taken off-site, only the minimum amount of personal or other confidential data necessary for the job in hand should be removed and, where possible, data should be anonymised.

All employees and others covered by the policy are individually responsible for ensuring
the adequate protection of information in their possession and ensuring its safe return.

The principles below are to be adopted and adhered to, to minimise the theft, loss or unauthorised use of personal or other confidential data whilst in transit or off-site:

2.1 Principles to be adopted

1. There is a presumption against taking personal or other confidential data contained within paper records off-site.

2. This material should only be taken off-site when it is a necessity and not a convenience.

3. Where data contained within paper records is taken off-site it should be kept to a minimum both in terms of content and duration. Consider how much information is actually required and avoid taking the whole case file unless this is absolutely essential.

4. Whilst off-site paper records that are not being actively worked upon, must be kept secure and stored separately from encrypted portable laptops which given their obvious value, are more likely to be of interest to thieves. This applies to papers records temporarily in the employee’s home as well as when the employee is on the move.

5. Where paper records are in transit from one location to another, they should be transported in a way that mitigates against the risk of theft or loss and stored in a separate folder away from other valuables, including portable equipment and other electronic devices.

2.2 Approval of requests/Paper Tracking Procedures

Before taking paper records off-site you must:

- Ensure you are authorised for the purposes of your job role to remove paper documents containing protected information
- Ensure you comply with the minimum standards set out in this policy
- Comply with business procedures established within your service area, including local monitoring systems for tracking the physical movement of confidential information (i.e. logs kept on site accounting for the movement of physical records removed from or transferred between secure environment).

2.3 Managers responsibilities

Managers must have proper business approval procedures and controls in place within their teams to ensure that personal data or other confidential data contained in paper records is only taken off-site:

- when it is necessary, rather than merely convenient, to achieve a specific task;
- for the minimum time necessary to achieve that task, and
- in circumstances where removal is limited to the minimum amount of information necessary to achieve that task.

How managers implement the necessary arrangements and monitor compliance with this
policy is for them to decide, taking account of the particular requirements of the services that their teams deliver and minimum standards set out in this policy. However, in the event that a team, for which they are responsible, suffers a loss of paper/data they will need to be able to satisfactorily demonstrate that they had ensured

(i) proper approval procedures and controls were in place and
(ii) the procedures and controls were adhered to through adequate and appropriate checks and considerations prior to the removal in question.

2.4 Best practice guidance

If it is determined that it is unavoidable to take paper records off-site, there are many practical actions which can be taken to minimise the risk of a data loss. For example:

- Do not carry ‘loose’ paper records as this increases the risk of dropping or losing them, make sure they are safely within a folder or other appropriate container
- Do not carry paper records in any bag containing valuables, as these are often the primary target for thieves
- Ensure paper records are not in transit for any longer than is necessary, and they are delivered to their destination at the earliest opportunity
- Ensure paper records are not away from the office for longer than is necessary and return them as soon as possible
- Do not leave bags or cases containing paper records visible in a car; if it is unavoidable to store paper records in a car, lock them in the boot
- Do not leave paper records stored in the boot of an unattended vehicle
- When travelling on public transport ensure that the contents of paper records are not visible
- When travelling on public transport keep bag/case containing paper records close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of loss or theft
- Treat paper records as you would your cash. Remember personally identifiable information about individuals is valuable in the wrong hands and if sensitive personal information is compromised the Council could suffer a heavy fine
- Ensure confidential paper waste created away from the office environment is securely disposed of using a cross cut shredder or ensure this is safely returned to Council premises for secure destruction.

3 Dispatching records to staff working from home and home workers

There will be occasions where paper records need to be sent off-site to another person
who is either working from home or is a home based worker.

3.1 Protocols to be adopted

Personal or other confidential data should normally be transferred through a secure network connection or by secure email.

Paper records containing personal or confidential information must only be supplied where there is necessary and there is no other alternative.

In such cases you must: -

- consider and adopt the protocols stated in 2.1
- choose a method of delivery appropriate to the nature of the information in the records, ensuring its security at all times.
- choose a method of delivery that ensures confirmation of receipt of paper records
- make the recipients of the information aware of their, and the Council’s responsibilities under the DPA.
- ensure the recipients adopt adequate security measures for the protection of the data whilst in transit and storage.

4 Training and information

All employees and others covered by this policy, with access to personal or other confidential data, must be made aware by their line manager of the existence of this policy via their team induction and other briefing processes.

Managers must highlight to individuals their responsibility and the importance of data protection/security.

The Council provides e learning on Protecting Information and Data Protection Essentials which all users of IT with access to personal or other confidential data must undertake. Whilst some face to face awareness briefings may be organised corporately (especially for workers who do not have access to the Council’s network), line managers and senior officers within Directorates must ensure that those with access to personal or other confidential data receive appropriate instruction on how to handle confidential information securely.

Employees who consider they have not received adequate training or information, must raise this with their line manager.

The following on line training is mandatory for all employees who are authorised to use the Council’s network:

- Protecting Information - Level 1 (All users)

Managers must also all complete:
Directorates will be planning the priority order in which business areas need to undertake this training in 2012-2013 and how this training supports the appraisal process.

This training is accessible via the following intranet page:

http://intranet.mcc.local/Learning_and_Development/Pages/E-learning.aspx

Managers of employees handling personal and confidential information who do not use the Council’s network should contact the Corporate Information Governance Manager to arrange alternative training. Email address: informationcompliance@manchester.gov.uk

5 Disciplinary action and criminal offences

Serious breaches of this policy caused by deliberate, negligent or reckless behaviour could result in dismissal and even give rise to criminal offences.

6 Reporting a data loss

Should an incident occur it is important that we know immediately what information has potentially been lost or stolen. This allows us to properly assess the risks and issues involved and, where necessary, to notify the data subject and any affected third parties including the Information Commissioner’s Office and other relevant agencies.

All data losses and other security breaches, including breaches of this policy, must be reported immediately by following the Council's Incident Reporting Procedure.

The promptness of reporting is vital in ensuring quick containment of the breach and, where possible, recovery of personal/confidential information. Any delay in reporting is likely to have a detrimental effect on the breach management process.

7 Review

This policy will be reviewed on an annual basis.

8 Advice and Contact Information
Further Data Protection advice and associated policies can be located on the Corporate Information Governance intranet pages, or from your local [Directorate Senior Information Risk Owner where this role has been established] or Information Governance lead.

Advice and guidance is also available from the Corporate Information Governance team:
Tel No: 0161 234 4415
E-mail: informationcompliance@manchester.gov.uk