

DATA PROTECTION POLICY

Contents

Practical measures you can take to implement data security	2
What to do if you lose personal data	2
Personal data must be kept secure	3
Personal data shall be processed fairly and lawfully	3
Personal data shall be 'adequate, relevant and not excessive'	3
Penalties	4
Declaration	4

Data Protection Policy

This document is designed to help you understand your responsibilities as one of the team at McGowan Transcriptions regarding Data Protection.

The government has many guidelines on Data Protection and they can be found in the Data Protection Act 1998. The act covers "Personal Data" (any information that identifies a living person, i.e. addresses, CCTV footage or salary information). "Sensitive Data" (information about criminal proceedings, ethnic or political opinions) as well as going into detail on the hefty fines and other serious penalties that can come from not handling these forms of data properly, which is why it's important to make you aware of the practical steps needed to keep McGowan Transcriptions in line with the 1988 Act.

1. *Practical measures you can take to implement data security*

The 1988 Data Protection Act states that Data Security is "the prevention of unauthorised access to, the abuse of, misuse of or loss of personal data." Data must be kept secure in order to prevent loss or unauthorised disclosure. All businesses are asked to have a written and active policy on data security, especially where they are handling sensitive personal data which transcripts and recordings can hold.

For McGowan Transcriptions this translates into the following steps that you need to take to keep information safe:

- Shredding all confidential waste - digital and paper.
- Checking the security of your house and work area.
- Using strong passwords and changing them monthly.
- Installing a firewall and virus checker on your computer.
- Using an anti-spyware tool. We can help you find software and take you through the process of adding it to your computer system.
- Encrypting personal information held electronically.
- Disabling any 'auto-complete' settings.
- Holding business telephone calls in private areas. Please remember the sensitivity of the information you are dealing with.
- Making sure that information you see on the computer stays on the computer.

2. *What to do if you lose personal data*

If your laptop/PC is lost please report it to the Police. Should the laptop/PC be found the Police will hack into it and find out who it belongs to. If they can get to your personal data on the hard drive they must report the matter to the Information Commissioner's Office (ICO). The laptop/PC will be returned, along with a fine and attention from the ICO.

If personal data held by you is lost through theft, a deliberate attack, unauthorised use or equipment failure, then McGowan Transcriptions will take the following steps.

- A recovery plan, including damage limitation.
- A re-assessment of the risks related to the breach.
- Informing the appropriate people and organisations to which the breach has occurred, including the ICO.
- A review of how you dealt with the situation with an appraisal of how security can be improved.

3. *Personal data must be kept secure*

The level of security should reflect the potential harm that could result from misuse or loss of the data. Remember, this will include security of both computer and manual records, such as secure servers, back-up, and arrangements for confidential shredding.

McGowan Transcriptions have kept to the 1998 Act by appointing Joe McGowan as Information security liaison in the company. She will help you find the right technology and keep policies and procedures up to date so that you can respond properly to any security breaches.

We also have security measures in place so that loss or unauthorised disclosure is prevented at the main office of McGowan Transcriptions. We only allow certain people access to data and use computer security programmes.

4. *Personal data shall be processed fairly and lawfully*

The 1988 Act stresses the fact that there must be a legitimate reason for processing the data. This basically means that this kind of information must only be used for the particular project you are working on. The information data must not be used unlawfully to improperly exercise power, infringe copyright, breach a contractual agreement or breach the Human Rights Act.

5. *Personal data shall be 'adequate, relevant and not excessive'*

According to the 1988 Act you should only keep personal information for the amount of time needed to complete the original, intended purpose. After this time the data should be destroyed. McGowan Transcribers cannot hold on to data thinking it may be useful in the future. Once a project is wrapped up then the personal data must be securely deleted or destroyed.

You should also only hold as much personal data as you need for the purpose - no more or as the 1988 Act puts it - "the information has to be relevant and sufficient enough to be able to complete the intended purpose."

6. Penalties

McGowan Transcriptions would be breaking the law if we didn't register with the ICO or adhere to the Data Protection Act. The Information Commissioner's Office can fine and prosecute us.

Penalties may arise from situations such as:

- Sending unsolicited marketing emails.
- Failing to dispose of confidential paperwork securely.
- Not having adequate access rights in place.
- Carelessly leaving data, such as laptops/transcripts, lying around.
- Selling data without seeking permission.

Declaration

Please sign below to acknowledge that you have read and understood your responsibilities outlined in the McGowan Transcriptions Data Protection Policy.

Signature:

Name (in block capitals):

Date:
