McGowan Transcriptions Limited
Meads Business Centre, The Financial Management Centre, 19 Kingsmead
Farnborough, Hampshire, GU14 7SR United Kingdom
t: 0800 158 3747 **e:** enquiries@mcgowantranscriptions.co.uk
www.mcgowantranscriptions.co.uk

Compliance Manual

McGowan is very security conscious and takes its client's privacy very seriously. As all transcribers must. Transcribers will be handling sensitive and personal information so must follow the procedures below and those included in the 'Information Security For Transcribers' document in order to keep client and McGowan data safe and protected.

All Transcribers must sign and adhere to a legally binding Confidential Disclosure Agreement before commencing any work for and on behalf of McGowan Transcriptions. Transcribers may also be asked to sign further client or project-specific non-disclosure or similar agreements from time-to-time.

Information Asset Management

1.1. McGowan Transcriptions prohibits the sharing or distribution of McGowan Transcriptions personal or confidential information.
1.2. No transcripts must ever be emailed, copied, transferred, printed or documentation taken out of your office or normal work environment.
1.3. You must not use removable media such as hard drives/memory sticks etc. to move data, and transcripts and recordings and must be omitted from any back-up systems you run to ensure that transcripts and recordings are only on McGowan Transcriptions' systems 10 days after receipt.
1.4. All data must be 'shredded', not just deleted after work is complete and signed off. Our recommended data deletion software is FileShredder v2 which adheres to US DoD (7 pass) standard. Please ensure you select '7 pass' when you install the software. www.fileshredder.org.
1.5. Should you at any point spot a possible security weakness it is your responsibility to inform McGowan Transcriptions immediately.
1.6. Should you at any point have a security breach, it is imperative and your responsibility to inform McGowan Transcriptions immediately and zuutech who provide Managed Security. Thereafter you will be asked to complete and sign an Incident Report Form which you must do without delay.

Devices - PCs/laptops used to transcribe

All Transcribers' PCs/laptops that are used to hold or process information received from McGowan Transcriptions must have Managed Computer Security (MCS) running on them, which McGowan Transcriptions provides you. The MCS protects your computer and keeps its security current and up to date. MCS provides managed anti-virus, operating system updating and software updating, phishing protection and firewall. Managed Computer Security is solely focused on security – it is NOT remote monitoring software. The software scans your computer and files for security purposes – it cannot open or read your files. If there is ever a need for manual intervention by the technicians to fix a security issue remotely, your consent is required first in order for them to be able to connect. You can request support and then allow this from the support icon on your computer desktop. After connecting, all activity by the technician can be seen by you.

Physical and environmental security

1. Only authorised personnel should have access to McGowan Transcriptions and client information.
2. Your computers should all have strong user passwords to login (minimum 8 letters and alphanumeric). It is strongly recommended that transcribers use a password manager. McGowan recommend Bitwarden https://bitwarden.com/
3. Transcribers must lock computers by logging out if they are not in use.
4. If you are on a public network (eg. airport, coffee shop, shared offices) you must use a VPN (Virtual Private Network) as these locations are not secure. If you do not have a VPN in place already, we recommend Nordvpn https://nordvpn.com/
5. Be extremely careful when installing new software or plugins. You must ensure they are safe and legitimate prior to installation.
6. Should your computer be lost/stolen, it must be reported to McGowan Transcriptions immediately.
7. Should your master password for your password manager, computer or any other password be compromised, you must inform McGowan and zuutech immediately.
8. Your computer must have Managed Computer Security on it, which McGowan provide you through zuutech.
9. If you have a problem and have reason to believe you may miss a deadline on any project you must inform Joe McGowan and Julia Page immediately.

Access, Audits and Log Files

Our Global Lounge system also has a record of when the recordings were uploaded and transcripts received by the client. We have advanced reporting for each recording received, who it has been assigned to, when it was received by the Transcriber, when it is due back to McGowan Transcriptions, when it has been uploaded/downloaded and when it has been deleted from the system.

The audit trail on Sharefile/Global Lounge is checked regularly for all client projects and any unpredicted events will be investigated fully.

1. Access: Using our Sharefile/Global Lounge systems we can track who has uploaded or downloaded files. Each file is encrypted at source before going onto the Sharefile/Global Lounge System so there is no risk of data retrieval with unauthorised access.

2. Audits and Logs: Our systems report information on all of these factors for each user and file.
   2.1. Files browsed
   2.2. Files created
   2.3. Files downloaded
   2.4. Files updated
   2.5. Files deleted

Incident Management

Joe McGowan is responsible for handling security incidents within McGowan Transcriptions. If there is a security incident that is in breach of this document and/or our Information Security Policy it will be fully

investigated and if deemed accidental then there will be one formal warning given, if breached a second time the Transcriber will no longer be able to work with McGowan Transcriptions.

If there is a security incident due to any of the specifications regarding security in this manual not being adhered to, the Transcriber will immediately cease working with McGowan Transcriptions.

Continuity management

In the event of a disaster that will affect or delay any transcription projects or security, you must inform McGowan Transcriptions immediately via email or telephone.

Data Protection

Please be aware that voice recordings are considered personal data and therefore must be treated appropriately as per the GDPR Act 2018. We have a separate policy in place with more information but you will find the general principles here. Please familiarise yourself with them and treat all voice files, templates, discussion guides and transcripts as personal data:

Please familiarise yourself with all areas of protecting personal data:
http://www.ico.org.uk/for_organisations/data_protection/the_guide/the_principles
http://www.ico.org.uk/for_organisations/data_protection/security_measures

Declaration

By signing below I confirm that I understand the responsibilities laid out in this Compliance Manual and that all work undertaken on behalf of McGowan Transcriptions will be undertaken to the principles and standards defined within this document.

Signature:

Name (in block capitals):

Date:

This document is valid for as long as you are involved with McGowan Transcriptions and may be updated from time to time.