## AA Global Language Services

# Data Protection and Data Security

At **AA Global Language Services Ltd** we realise the importance of confidential information whether it is industrial, commercial, legal or personal. All work undertaken by **AA Global Language Services Ltd** is treated with strict confidentiality. It is built into our contracts with our staff and translators that all information that they have access to must be treated as strictly confidential and must not be disclosed to any third parties under any circumstances without express written permission of **AA Global Language Services Ltd**. In turn, AA Global will never give permission for any disclosure without clearance from the client. In more delicate circumstances, we will be happy to sign a confidentiality agreement for complete peace of mind.

**Data Protection:**

AA Global are registered under the **Data Protection Act 1998 registration no:** Z1887071

We conduct interpreting and translation work for a number of central government departments, and in legal proceedings where data protection is of paramount importance.

**AAG Code of Ethical Practice**

AA Global has a code of ethics (outlined below) for interpreting sessions conducted with ethnic minority groups and vulnerable individuals that all our interpreters observe, and which includes issues of confidentiality. It forms part of our interpreter induction programme, and the general points and specific issues are always included in the team briefings for each assignment. In addition, we also observe the Home Office Guidance on the Interviewing of Victims of Torture, where applicable.

**Data Security/Confidentiality**

We acknowledge, respect and highly value the preservation of the confidentiality of data and information. All clients' documentation, tape recordings and transcripts of interpreted sessions, correspondence, data, reports, are all treated as strictly confidential. **Data security and transfer and client/respondent confidentiality is covered in our staff induction programme and is reiterated in team briefings for individual projects**. We always have at least two key members completely briefed on all the projects and clients' requirements and fully involved with all aspects of past, present and future project booking and business activities.

**AA Global Head Office** – Our offices are located in secure premises, with industry standard alarms. Cleaning of our offices is carried out while a key member is present – **thus no cleaning company or any other third party has access or the keys to our offices**.

All the data and document files are saved on our Network Server, which is setup with a secured automatic daily back-up system (starts at 6:00pm, every evening). In addition to our daily backup, we use an off-site weekly backing up system - another back up copy is stored off-site.

**Insurance Policy** – We hold Commercial Indemnity Insurance, which also covers any loss or damage to premises and office contents (including client's materials, documents, etc), which is renewed annually. We also hold current Employers, Public and Third Party Liability Insurance Cover.

**Paper Documents** – During the life of an assignment all paper documents; (such as translation transcripts, end user contact information) are kept in locked storage units, such as secure metal filing cabinets (BISLEY) and are only retrieved by authorised staff for the purposes of resource allocation and conduct of assignments. Only two key members have the keys to these storage units and only 2 key members have the keys to the AA Global offices.

**Electronic Documents** e.g end user contact details and transcripts of interpreted sessions captured in electronic format, is stored using industry standard encryption software. The decryption keys for this information are stored off site and access is electronically controlled and only available during the

working hours of 8:30am and 6pm Monday to Friday. In the event of a break-in the keys can be quickly and easily removed rendering the encrypted data useless.

**No data which can be used to identify an individual is ever transmitted electronically**. Our internal strict procedures for delivery and retrieval of sensitive data of this type are to encrypt the file(s) using the 256-bit encryption software: TrueCrypt. We also have worked with contractors to transfer transcribed taped interview data via secure web server using PGP encryption software (preferred by central government).