GSS - Confidentiality Policy

Statement of this Policy

GSS (UK) Ltd define confidentiality as "ensuring that information is accessible only to those authorized to have access and is protected throughout its lifecycle ".

Confidentiality is an important principle in business because it functions to impose a boundary on the amount of personal information and data that can be disclosed without consent. This policy works in conjunction with GDPR 2018 and the necessity to protect data collected from individuals whatever the purpose.

Knowing that confidentiality practices are in place allows the person giving sensitive and personal information, to feel secure and that they can trust that their privacy is being protected. Throughout the course of work GSS staff have access to an enormous amount of information that must be treated as confidential. Mainly this information pertains to:

Monitoring

GSS being a Provider and Training organisation will effectively monitor its practices and annually review this Confidentiality Policy as well as reviewing its statement on an ongoing regular basis. Mainly this will affect confidential client information and or information received from our contractual partners on behalf of individuals and their circumstances but could also include other data provided to us. Also GSS will hold confidential information on staff, colleague, business partners and volunteers.

This policy sets out a framework for the expectations we have of all staff in our company. All sensitive information or information containing personal information will be held Securely and confidentially (usually within lockable locations), it will be obtained both fairly and efficiently, recorded accurately and reliably and used effectively and ethically as well as shared appropriately and lawfully.

Paperwork - Our office environment

All staff are responsible for ensuring the security for all documents containing confidential information about Clients and or customers wherever and however this may have been come by or have arisen. This covers all communication, paperwork pertaining to customers and information containing customer, client or staff personal information.

All files and paperwork containing any of the above information will be kept locked in secure cabinets (except when in use) and accessible by delegated key holders only.

Electronic Information

E-mails containing confidential information should not be sent unless you are confident that the relevant person will receive them internally or externally and will be flagged as confidential. Any information concerning personal information can only be forwarded on with permission of those concerned only. All emails pertaining to GSS work must be routed via GSS own email address and must always comply with GSS *Internet usage policy* and *Information and Data Security policy*.

Multiple Customer Emails

Where a single email is to be sent out to many customers the following procedures must be adhered to:

1. Customer email addresses must be collated from spreadsheets / information provided by GSS Management only
2. No more than 30 emails should be mailed at any one time in a single email mail out
3. Once the email has been constructed it must be double checked by a second Team member
4. All emails MUST BE SENT using the BCC function only
5. Emails must be fully checked prior to sending by a member of GSS Management Team to ensure that the email is
    a. Using bcc only as the send function
    b. it is grammatically correct
    c. It meets all GSS guidelines for emailing customers and does not contain any sensitive data

Electronically held data

All information held electronically containing sensitive information or personal data will be held under password protected files. Customer records are held on our own database through our own server with data only required for the purpose of the work at the time. GSS server is held in a secure manned office (this is locked when not manned) and is within an alarmed area of the premises. All data is backed up internally and daily back up tapes are only removed from the premises overnight.

Confidential data no longer in use or outdated/invalid will be held securely for a maximum of 12 months after the last usage at which point will be securely destroyed or disposed of unless by prior arrangement from GSS business, partners, contractors or other.

All electronically held data must also comply with GSS *GDPR and Information and Data Security Policy*.

Third Party Data

Information received via any third party which may include sensitive data, such as customers Date of Birth, National Insurance details or any identifying information must under no circumstances be emailed, or faxed to any other organisation or party without prior consent of the named individuals to which the data concerns. Information that needs to be passed to relating bodies (only) for verification can only be done through secure methods.

Any breaches to the above could constitute gross misconduct and where found, individuals could be subject to disciplinary procedures accordingly.

This policy is not exhaustive and is in conjunction with GSS *GDPR, GSS Encrypting documents policy and GSS Information and Data Security policy.*

Signed by Sonia Benjamin-Leach
Director
14.08. 2018
Updated v9