[t]P IT Consultation & Support
Websites design & hosting
Application development

Public Confidentiality Agreement

IT Services 2019 - 2020

Introduction

This document is an agreement between the all clients and IT ‘service provider’ Tom Poole. During the course of providing IT services the service provider will be entrusted and exposed to the clients personal, and commercial data; this agreement explains the terms of clients confidentiality.

The term ‘client’ in this agreement will refer to any individual or corporation accepting a tender for contract from the service provider. The terms in this agreement should be considered part of the overall contract and accepted up on the clients commission of work.

The term ‘data’ in this agreement refers globally to all information seen or acquired while carrying out duties in line with IT services being provided by the ‘service provider’.

Terms

a) Global Data Policy

All clients data is treated with respect and never wilfully shared to a third party. With the exception of approved marketing material and data designed for public broadcast, all recorded and seen information is covered under this privacy agreement. No recorded data is stored for longer than it is required and all notes and physical data is securely shredded / destroyed prior to going on to waste management services.

i. Digital information
   This includes electronic communications, text message, and files transfers and back-ups. All of this type of data when stored for the purposes of providing services will kept on a secure and encrypted system or encrypted external drives.
   i. All digital data will be archived locally and securely for up to 12 months whilst active. Automated systems will move documents and messages to secure archive locations when they are 12 months or older.
   ii. All archives are vetted and removed once annually. No exact date for this task is specified however it is historically in the final quarter of each year. Archives and backups are audited and development systems reinstalled or upgraded for maintenance.

ii. Privileged knowledge
   This is defined as information not recorded but perhaps spoken or seen and considered of a sensitive nature. This may include credentials or the ‘clients’ client base.
   i. The service provider adopts all privileged information as private and will not re-disclose with prior instruction to do so.

ii. Privileged data seen either on-screen or written down will not be recorded in anyway and rarely remembered when it does not affect the functionality of the system.
iii. Whilst not recorded some passwords and other credentials may be remembered but never shared or used outside of providing a service to the client.

iii. Paper notes

A handwritten notebook may be used for meetings and taking notes on telephone calls.

i. Paper material and notes will only be kept for as long as it is required to complete a project or provide a service but may exist as archive in a current notebook.
ii. Notes covered here may be taken by the service provider or supplied by the client.
iii. Sensitive notes are to be removed as soon as they are no longer required, this includes credentials and personal information.
iv. Destruction of physical (paper) data is done via cross-cut shredder and waste management leading to recycling.

b) Credentials

Data given to the service provider for accessing clients systems and services (3rd party) will be stored in an encrypted database designed for credential storage and saved on a cloud service for access while mobile. Passwords may also be saved on local password protected devices in encrypted password managers for ease of access when required.

i. Credentials stored on behalf of a client are only stored for as long as required.
ii. The service provider is not responsible for long-term password storage or retrieval.

c) Backups

The service provider may make / take backups of client systems / servers / databases onto his own backup equipment. This data will be stored for a temporary purpose only.

i. The service provider backups are not to be relied upon for disaster recovery as they will be in the form a snap-shot to recover from a procedure.
ii. Backups made for recovery will be formatted as soon as they are no longer required.
    i. Secure formatting is always practised when removing sensitive data. This means data is overwritten prior to being removed from the disk / media.
    ii. Unwritable media such as CD/DVD will be shredded.

d) GDPR Compliance

The client DCO (registered Data Control Officer) can liaise with the service provider to confirm in-house data practices that will maintain compliance for all information covered in this agreement. The service provider only provides help and advice to a client DCO and does not register or take on the clients DCO responsibilities or liabilities.