



## ILKLEY IT SERVICES LTD

### PRIVACY NOTICE

#### Who does this apply to?

This policy applies to clients, customers, suppliers and any other category of 'data subject' for whom Ilkley IT Services Ltd provides a service, and we have a duty to notify you of its content. A copy can be found on <https://www.ilkleyitservices.co.uk/compliance-centre/>

#### General

We intend to comply with our legal obligations under the Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR) in respect of data privacy and security.

Ilkley IT Services Ltd takes the security and privacy of your data seriously and as part of the service we provide to you it will be necessary for us to: -

- a) Have access to your IT systems, equipment and software whether that be on site or remotely;
- b) Have knowledge of and to retain passwords for computers and other electronic equipment;
- c) Have sight of personal or sensitive data about your business, employees, customers and any other third party with whom you engage via electronic means, such as but not limited to financial information, names and addresses, dates of birth, health records, pricing, stock, etc.

We will not collect or retain any personal data from you that we do not need to enable us to provide and oversee this service to and for you.

#### Confidentiality

Whilst it is never our intention to snoop or to take note of such information, we would not be able to do our job without on occasion seeing this information in the course of checking, improving, restoring or protecting your IT systems and their contents. We therefore take confidentiality and discretion seriously and commit to ensuring that each and every member of our team is not only trained on understanding our requirements of confidentiality but also exercises the utmost of professionalism and integrity in their day to day work when supporting you to maintain your IT systems.

Every member of our team is required to sign a confidentiality agreement when they start with us and given training on how to ensure confidentiality within our Company. We discuss and review this in appraisals to ensure that it is always at the forefront of every employee's mind and any breach or potential breach will be acted upon immediately and the client informed within 24 hours.

#### Who is the Data Controller?

The Company is a 'data controller' for the purposes of any personal data which means that we determine the purpose and means of processing personal data. If you have any queries in relation to this policy or any data protection or processing issue, please contact Warren Lloyd on 07734 214351 or email [warren@ilkleyitservices.co.uk](mailto:warren@ilkleyitservices.co.uk).

#### What we do with personal/confidential information

Any data we process is done in the UK however for the purposes of IT storage, hosting and maintenance this information is located on 'OneDrive for Business' which is the Microsoft 'Cloud' storage service. This means we can securely store all your files in one place, share them with others with your consent, and get to them from anywhere. No third parties have access to, or will be given access to, that personal data, unless authorised personnel within my client company, or the 'data subject' themselves give consent, as is appropriate, or as the law requires.

### **What data do we collect?**

In addition to the necessary personal data we require from all our employees, we also collect the following data in order to provide a service to our customers/clients.

- Personal data: -
  - Company Name
  - Employee names
  - Business related phone numbers
  - Employee company Email address
  - Employee position in the company
  
- Username and password data: -
  - All usernames and password relating to the company are gathered, except
  - Occasionally we will ask user for their PC logins but are not stored on our system.
  
- PC & Hardware Information: -
  - Audit Information about PCs and Hardware

### **Why is data collected and how is it used?**

In addition to enabling us to provide the best possible service to our clients we occasionally send out newsletters to company owners with industry news, company news and sometimes informing customers of new and/or existing services. We never sell or pass on your personal or company details to a third party without your consent.

You are able to opt-out of this facility or change your mind and to unsubscribe at any time by emailing [warren@ilkleyitservices.co.uk](mailto:warren@ilkleyitservices.co.uk).

### **How long do we keep data for?**

- Customer information is stored in Xero and will be retained for a minimum of 6 years at which point we will ask that Xero confidentially destroy the information.
- If you would like us to remove your information from our records you should write/email Warren Lloyd, Managing Director.
- All usernames and passwords are confidentially retained as long as the client uses Ilkley IT Services.
- If a client tells us that they do not wish to use our services, or after a period of 60days we have no contact from a client, the credentials we hold will be removed from our live system within 7 days of termination. However, they will remain stored confidentially in our backup provider (Skykick) for 24 months after which time it will be permanently deleted
- Freshdesk Ticket System - Data is kept indefinitely as long as the clients use our services. If they no longer use Ilkley IT Services all data relating to that company will be removed within 60days.
- Email enquiries made via the website contact form - Data is sent securely and stored in our mailboxes indefinably, unless requested to be removed. Data is only used to response to the request and will never be used for marketing purposes.

## Where is the data stored?

The data we collect is stored securely in the following locations: -

- Helpdesk software – Freshdesk - <https://www.freshworks.com/privacy/gdpr/>
  - Staff name, email address, site address, business phone numbers.
- Microsoft Office 365 - <https://servicetrust.microsoft.com/ViewPage/GDPRGetStarted>
- Backup data is stored in
  - Microsoft Azure - <https://servicetrust.microsoft.com/ViewPage/GDPRGetStarted>
  - Skykick - [https://support.skykick.com/hc/en-us/articles/115005074553-General-Data-Protection-Regulation-GDPR-Compliance?flash\\_digest=cb2ae15466bb18964ca6357c906ce5c21c26e5dc](https://support.skykick.com/hc/en-us/articles/115005074553-General-Data-Protection-Regulation-GDPR-Compliance?flash_digest=cb2ae15466bb18964ca6357c906ce5c21c26e5dc)
- Monitoring software – Autotask – Although no personal information is stored in this location, computer information is, although the system can only be accessed via Ilkley IT authorised personnel using a secure login and 2-factor authentication.
- Remote access software – ConnectWise Control – Self hosted on an Ilkley IT Azure server. A screenshot is taken of the user's PC every 10mins (when online). Only the latest image is stored and is replaced by the next screenshot and would only ever be viewed by Ilkley IT Services authorised personnel. See below to know who has access to this data.
- Xero – Accounts Software - <https://www.xero.com/uk/campaigns/xero-and-gdpr/>
  - Client company name, address, accounts person contact name and email address.
  - Supplier's company name, address and email contact details.
- GoCardless – Payment Collection (like DirectDebit).
  - Client company name, address, accounts person contact name and email address.
  - Supplier's company name, address and email contact details.
- Directli – Connects Xero to GoCardless.
  - Client company name, address, accounts person contact name and email address.
  - Client payment info (not accessible by anyone at Ilkley IT)
- ESET Remote Administrator
  - Computer information

## Who has access to the data?

- Currently all staff members have access to customer information. Via Freshdesk, Office 365, ConnectWise Connect and ESET RMA. This is essential to enable us to provide a service to our clients. However, every member of staff is trained appropriately and is required to sign a 'confidentiality agreement'.
- Staff/payroll and financial information is only accessible by Warren and our bookkeeping/ accounts providers via Xero who have provided us with a Privacy Notice including confidentiality agreement.
- Junior staff members or staff on apprenticeships will not be given access to customer username and passwords until they have successfully completed their probationary period and have signed and understand the requirements of a confidentiality agreement.
- Risc IT Services is a data processor and has access to customer information via Office 365 services. <https://www.riscitsolutions.com/en/compliance-centre>. They have also provided details of their Privacy Notice and Data Protection Policy and comply with all requirements relating to confidentiality.

## Who we share data with?

- NO customer username and passwords are ever shared with anyone outside of Ilkley IT Services unless consent is given in writing from the client.
- Pennyhole Bookkeeping services access financial info, but only to carry out the bookkeeping services they are hired to do.

## How is data protected?

Protecting all the data that see or have access to is essential for us to meet our clients' expectations in relation to handling data appropriately and confidentially. For that reason the following sets out how, the data is protected: -

- Freshdesk
  - Each staff member has individual logins with a strong password which is changed every 90 days.
  - 2FA to be introduced by Freshdesk in 2018.
  - Warren and Will are the only administrators
- Autotask
  - Each staff member has individual logins with a strong password.
  - 2FA enabled on all accounts.
  - Warren is the only person with full administrator rights
- Office 365
  - Each staff member has individual logins with a strong password.
  - 2FA enabled on Primary accounts. Warren, Will and Accounts have access.
  - MDM policy applied to mobiles. Devices are encrypted and password/biometrically protected.
  - Only Warren is administrator.
- Xero
  - Warren and Pennyhole have a login with a strong password.
  - 2FA enabled on all account.
- GoCardless
  - Warren and Pennyhole have a login with a strong password.
- Directli
  - Pennyhole have a login with a strong password.
- ConnectWise Control
  - Each staff member has individual logins with a strong password.
  - 2FA enabled on All accounts.
  - Server is hosted on an Ilkley IT Azure Server using Duo 2 Factor Authentication, which is only accessible by Warren

## Our Use of Cookies

Our site may place and access certain first party Cookies on your computer or device. First party Cookies are those placed directly by us and are used only by us. We use Cookies to facilitate and improve your experience of our site and to provide and improve our products and services. By using our site, you may also receive certain third-party Cookies on your computer or device. Third party Cookies are those placed by websites, services, and/or parties other than us. Third party Cookies are used on our site for marketing and performance management purposes. In addition, our site uses analytics services provided by Google, which also use Cookies. Website analytics refers to a set of tools used to collect and analyse usage statistics, enabling us to better understand how people use our site.

## What are your rights?

If at any point you believe the information we hold or process for you or about any of your employees or other relevant contacts is incorrect, you have the following rights:-

- to be informed about how, why and on what basis that information is;
- to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request;
- to have data corrected if it is inaccurate or incomplete;
- to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim; and
- to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).
- If you wish to exercise any of the rights above, please contact Warren.

## Complaints procedure

If you wish to raise a complaint on how we have handled any personal, sensitive or confidential data, or indeed any data relating to your business, you can contact Warren on 01943 601601 or email [warren@ilkleyitservices.co.uk](mailto:warren@ilkleyitservices.co.uk) who will investigate the matter and respond wherever possible within 4 weeks. If this is not possible we will notify you with updates.

If you are not satisfied with our response or believe we are not processing data in accordance with the law, you can complain to the Information Commissioner's Office (ICO) on 0303 123 1113.

A handwritten signature in black ink, appearing to read "W Lloyd".

Warren Lloyd –  
Managing Director  
Ilkley IT Services Ltd