Privacy Policy

1. Introduction

This privacy policy tells you what to expect when Simpson collects information about you.

It applies when we collect information about: -

- Visitors to our website
- People who interact with us on social media
- People who email us
- People whose images are captured by the CCTV at our head office
- People who use our services (ie. our clients and their employees)
- Suppliers and sub-contractors we use to fulfil our contracts
- Job applicants and current and former employees

2. Visitors to Our Website

2.1 Google Analytics

Our website, www.simpsonyork.co.uk, uses a third-party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site.

This information is only processed in a way which does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website. We will make it clear when we collect personal information and will explain what we intend to do with it.

2.2 Cookies

Cookies are small files saved to the user's computer hard drive that track, save and store information about the user's interactions and usage of the website. This allows the website, through its server to provide the users with a tailored experience within this website. Users are advised that if they wish to deny the use and saving of cookies from this website on to their computers hard drive they should take necessary steps within their web browsers security settings to block all cookies from this website and its external serving vendors.

We use tracking software to monitor website visitors to better understand how they use our website. This software is provided by Google Analytics which uses cookies to track visitor usage. The software will save a cookie to your computer hard drive in order to track and monitor your engagement and usage of the website but will not store, save or collect personal information.

You can read Google's Privacy Policy here for further information http://www.google.com/privacy.html

2.3 External Links

Although we take every effort to only include quality, safe and relevant external links, users should always adopt a policy of caution before clicking any external web links mentioned throughout this website.

The owners of this website cannot guarantee or verify the contents of any externally linked website despite their best efforts. Users should therefore note that they click on external links at their own risk and this website and its owners cannot be held liable for any damages or implications caused by visiting any external links mentioned.

2.4 Enquiry Form

When you volunteer information by completing our Enquiry Form, we will use this data to contact you regarding your specific enquiry. Simpson will not sell or rent your personally identifiable information, gathered as a result of filling out the site enquiry form, to anyone.

3. People Who Interact with Us via Social Media

Communication, engagement and actions with external social media platforms, that this website and its owners participate on, are custom to the Terms and Conditions as well as the Privacy Policies held with each social media platform respectively.

Users are advised to use social media platforms wisely and communicate/engage upon them with due care and caution in regard to their own privacy and personal details. Neither this website nor its owners will ever ask for personal or sensitive information through social media platforms and encourage users wishing to discuss sensitive details to contact them through primary communication channels such as by telephone or email.

If you follow or otherwise interact with us on social media, we will accept this as your consent to being contacted for the services we provide. We will never share your personal details with anyone else, and you may opt out by contacting us on the details below.

This website may use social sharing buttons which help share web content directly from web pages to the social media platform in question. Users are advised before using such social sharing buttons that they do so at their own discretion and note that the social media platform may track and save your request to share a web page respectively through your social media platform account.

3.1 Shortened Links in Social Media

We may, through our social media platform accounts, share web links to relevant web pages. Users are advised to take caution and good judgement before clicking any shortened URLs published on social media platforms by this website and its owners. Despite the best efforts to ensure only genuine URLs are published many social media platforms are prone to spam and hacking and therefore this website and its owners cannot be held liable for any damages or implications caused by visiting any shortened links.

4. People Who Email Us

We use Transport Layer Security (TLS) to encrypt and protect email traffic in line with Electronic Communications Act 2000. If your email service does not support TLS, you should be aware that any emails we send or receive may not be protected in transit.

We will also monitor any emails sent to us, including file attachments, for viruses or malicious software. Please be aware that you have a responsibility to ensure that any email you send is within the bounds of the law.

All emails sent to or from www.simpsonyork.co.uk are archived securely in a tamperproof device, in accordance with our retention policy of 20 years, following which they are removed from our archive device. Archived emails are only available to those included on the original distribution list, unless subject to authorisation from a Company Director.

5. CCTV

5.1 Head Office CCTV

We use closed-circuit security cameras at our head office, which comprises a number of cameras located externally around Chessingham Park, and one camera located internally within our Pearson Vue authorised Test Centre room. All footage is held on site, and not transmitted to any monitoring station or third-party. Please refer to company policy PD30 CCTV.

5.2 External CCTV

Our external CCTV is intended to deter those of criminal intent, to assist in the detection and prevention of crime, and facilitate the identification, apprehension and prosecution of offenders. It is in operation 24 hours

each day, 365 days of the year but will only record when movement is detected. Records will be kept for approximately five weeks, at which point they will be recorded over. Actual timescales may vary due to the amount of movement detected in the period.
Only appointed persons may view the material recorded, and the details of any viewings are logged, but it may be handed over to law enforcement if required.

5.3 Internal CCTV

The internal CCTV within the Authorised Test Centre will only be in operation during CSCS Health & Safety tests. Its intention is to identify any activity in the test room that would disqualify the result of an individual's test. Records will be kept for 30 days at which point they will be deleted by the Training Advisor.
Only appointed persons may view the recordings from the Test Centre, however part of our agreement with CITB means that we are required to release the footage to CITB at their request.

Further information on our CCTV can be found in our comprehensive CCTV policy document, available on request.

6. People Who Use Our Services

6.1 Existing Clients

SIMPSON offers various fit-out and construction services to both businesses and individuals. We have to hold the details of the people who we are dealing directly with in order to fulfil our contract. However, we only use these details to provide the service the person or company has requested and for other closely related purposes. Once a contract is complete, we have a requirement to retain details, including some personal information and associated paperwork, for a statutory period of 12 years post completion. Details relating to accidents and asbestos have a statutory retention period of 40 years.

6.2 Potential Clients

If we are asked to tender a price for a potential client we will keep details of the contacts we deem necessary in order to carry out the pricing of the works. If we are not successful with our tender we will keep these details for up to 5 years, in the event that we are able to successfully bid for further projects. If you do not wish for this to happen, you should contact us at the address below.

We also operate a list of people who have expressed interest and opted-in to our newsletter. We do not use mass-mailing software for this purpose, and the list of people will never be shared. Those on the list may opt out at any time.

7 Suppliers and Sub-Contractors

SIMPSON use various suppliers and subcontractors during our work and need to keep records of which companies and individuals have quoted or supplied us with materials or labour, even if that tender was unsuccessful. We will normally retain personal details for all tenderers in order that we may invite you to quote for further work. If you would like to be removed from our list of potential tenders, please contact us using the details below.

8. Job Applicants and Current and Former Employees

8.1 What Will We Do with The Information You Provide to Us?

All of the information you provide during the process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide during the recruitment process with any third parties for marketing purposes or store any of your information outside of the European Economic Area. The

information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for.

8.2 What Information Do We Ask For, and Why?

We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary.

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for but it might affect your application if you don't.

8.3 Application Stage

We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for. Our recruitment team will have access to all of this information.

8.4 Assessments

We might ask you to participate in assessment days; complete tests or occupational personality profile questionnaires; and/or to attend an interview – or a combination of these. Information will be generated by you and by us. For example, you might complete a written test or we might take interview notes. This information is held only by SIMPSON.

If you are unsuccessful following assessment for the position you have applied for, we may ask if you would like your details to be retained in our talent pool. If you say yes, we would proactively contact you should any further suitable vacancies arise.

8.5 Conditional Offer

If we make a conditional offer of employment we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity and reliability.

You will therefore be required to provide:

- Proof of your identity – you will be asked to attend our office with original documents, we will take copies.
- Proof of your qualifications – you will be asked to attend our office with original documents, we will take copies.
- You may be asked to undergo a Disclosure Barring Service (DBS) check to confirm any unspent convictions as required for the role. (see Criminal Records Check below)

We will contact your referees, using the details you provide in your application, directly to obtain references. We may also ask you to complete a questionnaire about your health. This is to establish your fitness to work. This is done via a data processor (see Athena Occupational Health Ltd, below).

If we make a final offer, we will also ask you for the following:

- Bank details – to process salary payments.
- Emergency contact details – so we know who to contact in case you have an emergency at work.

8.6 How Long is Information Retained?

If you are successful, the information you provide during the application process will be retained by us as part of your employee file for the duration of your employment plus 12 years following the end of your employment. This includes your criminal records declaration, fitness to work, records of any security checks and references.

If you are unsuccessful at any stage of the process, the information you have provided until that point will be retained for 6 months from the closure of the campaign.

Email correspondence will be retained according to our email retention policy previously stated. However, we will respect your request not to be contacted if you advise us as such.

8.7 How We Make Decisions About Recruitment

Final recruitment decisions are made by hiring managers and members of our recruitment team. All of the information gathered during the application process is taken into account.

You are able to ask about decisions made about your application by speaking to your contact within our recruitment team.

9. Other Employment Related Information

9.1 Trade Union Membership

Some employees may wish for us to deduct UCATT membership fees from their salary. If you wish for us to do this we will require written authorisation and your membership details. Trade union membership is regarded as a Special Form of Personal Data and is held in confidence. We will not use details of individuals' trade memberships to influence any decision-making.

9.2 Criminal Records Checks

Some of our work is undertaken in schools or other areas where there is access to vulnerable children and adults; as such extra security measures must be put in place.

If your role requires it, you will need to complete an application for a Criminal Record check via the Disclosure and Barring Service, or Access NI, which will verify your declaration of unspent convictions. The report will come direct to you from the relevant authority, and we will get a notification of whether you are clear for this type of access or not – we will not get details of any actual convictions.

A record of who is available for this type of work will be kept securely in an encrypted file, with access restricted to those approved by DBS.

9.3 CUBE

If you accept a final offer from us, some of your personnel records will be held on Cube which is an internally used ERP system incorporating some HR records. Cube is our name for the combination of Summit 3000 and Xcipio, which is software provided by RedSky IT, whose details you will find below.

9.4 Armstrong Watson

If you are employed by Simpson, relevant details about you may be provided to Armstrong Watson who provide payroll services to Simpson. This will include your name, bank details, address, date of birth, National Insurance Number and salary.

9.5 Aviva and B&CE

Likewise, your details will be provided to Aviva or B&CE who are the administrators of the Simpson pension schemes.

You will be auto-enrolled into one of the pension schemes and details provided to the administrator will be your name, date of birth, National Insurance number and salary. Your bank details will not be passed to the administrator.

9.6 Peritus Health Ltd

Peritus Health Ltd provide our Occupational Health assessment service.

If we make you a conditional offer, we may ask that you complete a questionnaire which will help to determine if you are fit to undertake the work that you have been offered or advise us if any adjustments are needed to the work environment or systems so that you may work effectively.

The information you provide will be held by Peritus Health Ltd who will provide us with a Fit to Work Certificate or a report with recommendations. You are able to request to see the report before it is sent to us. If you decline for us to see it, this could affect your job offer.

9.7 Insurance

For those employees with access to a company vehicle, we are required to hold copies of driving licenses with details of motoring offences and accidents for the employee (and their partner, if we agree to allow them use of the vehicle), which will be revealed to our insurance broker and insurance company at regular intervals.

In the event of a claim against our insurances, we may be required to release your details to a third party or their insurer.

9.8 Mobile Phones and Mobile Wi-Fi Devices

If you use a smartphone for company emails, text messages or storing other company data, we need to ensure the security of that data.

We do this with the use of up to two apps installed on all mobile devices containing company data. The Maas360 app will need to be installed on both corporate devices and employee devices with access to company data and report many basic details about the phone or tablet, such as serial number, operating system version and encryption level.

If the device has location data turned on, this will also be reported for the purposes of recovering the device if it is lost or stolen (location history is not maintained), and company-owned devices will also report a list of other installed apps.

In the event of the device being lost or stolen we have the ability to: -

- Lock the device
- Wipe the company data
- Wipe the entire device

We will not wipe the entire device without talking to you and you agreeing that this is the best course of action.
Some phones may have fingerprint or iris scanners as optional methods of unlocking a device; if you choose to use these functions, the details are securely stored locally on the device, and we do not have access to any of the details.

Devices on our company mobile phone contract will also have the Moda app installed, which is used to monitor website usage on mobile data only. We do this to prevent inappropriate use of our phone contract and to ensure we are within the data limits set in that contract. It also prevents access to categories of

website deemed unsuitable, by warrant of either being malicious or adult in nature and retains details of the top domains visited and blocked domains.

The Moda app only tracks the use by domain so, for example, the system administrators would only see www.facebook.com, not www.facebook.com/yourname. This app may restrict data speeds once a limit is reached and, like Maas360, retains a last-known location in the event of loss or theft. The monitoring and restrictions only apply to mobile data usage, and data will not be collected or filtered when connected to a private Wi-Fi network.

Mobile Wi-Fi devices may be issued to employees who are regularly working outside our head office. This will also report through Moda with a last-known location and website usage, and will filter inappropriate web traffic, as detailed above.

9.9 Disclosure to Other Parties

There may be other circumstances, not specifically declared above, in which we will need to disclose other information to third parties. This information will always be proportionate and be backed up by either your explicit consent or legal or contractual obligations.

10. Information We Collect on Our Sites

10.1 Health and Safety Information

In order to comply with health and safety legislation, we are required to keep some information on everyone who comes onto one of our construction or fit-out sites.
We keep records of: -

- Inductions (including medical conditions, medications, emergency contacts and CSCS cards)
- Attendance
- Night worker's health assessments
- Young person's risk assessments
- Construction Phase Plan contact details
- Accident details

The original documents are held securely on site, with access limited to those who would require them – usually the site manager and first-aiders. Paper records are also scanned to our document management system, Cube. Original paper records are shredded at the end of the project, but held electronically for the following retention periods: -

- 40 years for accident records and night worker health assessments
- 12 years following project completion for all other records

None of this information will be sold or otherwise made available to any third party, unless required to in order to make or defend any litigation, or unless required by a governmental authority.

10.2 Biometrics

On some occasions, we may deem it necessary to control access to our site by use of either fingerprint or facial recognition software. This is to ensure the security of the site, and no personal details gained by this software will be shared with anyone. The details will be kept for the duration of the project, after which they will be securely deleted.

11. Subject Access Requests

Simpson is open and transparent about the personal information we hold, this is in line with the General Data Protection Regulation 2016. Individuals have the right to make a 'Subject Access Request'. If we do hold information about you we will:

- give you a description of it;

- tell you why we are holding it;
- tell you who it could be disclosed to; and
- let you have a copy of the information in an intelligible form.

To make a request to Simpson for any personal information we may hold, you need to put the request in writing by addressing it to our Best Practice Department at the address provided below. You can also request a form to complete. On receipt of your request we will have a period of 1 month to respond

Subject Access Requests by their very nature will need to be supported by proof of ID, to ensure data is divulged only to the individual to whom it relates.

Please refer to BP16 Data Subject Access Request Process.

12. Third-Party Software

We use several online software providers during the course of our business, all of which have their own privacy policies in place: -

Company	Product	Privacy Policy
RedSky IT (Hemel) Ltd	Summit 3000 / Xcipio	http://www.redskyit.com/company/privacy.htm
Microsoft UK	Azure Hosting	https://privacy.microsoft.com/en-gb/privacystatement
IBM	MaaS360	https://www.ibm.com/privacy/us/en/
Asavie Technologies Ltd	Moda	http://modasupport.asavie.com/service-support/privacy-statement/

Data Processing Agreements are in place with all relevant processors.

12. Complaints

If you wish to make a complaint about the way we have processed your personal information, you can contact us using the details below. We have robust procedures in place and believe we can rectify any issues you may have. In the event that we are unable to resolve your issue satisfactorily, you can contact the UK Information Commissioner's Office at https://ico.org.uk/.

14. Changes to this Privacy Notice

We keep our Privacy Policies under review. This Policy was last updated on 22 February 2023.

15. How to Contact Us

For further information or to contact us regarding our privacy policy you can email us at dataprotection@simpsonyork.co.uk or write to: -

Best Practice Department
SIMPSON (York) Ltd
10 Hassacarr Close
Chessingham Park
York
YO19 5SN