

EMPLOYEE PRIVACY POLICY

Fuller, Smith & Turner P.L.C. is a family-controlled business, with a listing on the London Stock Exchange. We respect the privacy of our team members and do our utmost to ensure that your privacy is protected at all times.

We have developed this Employee Privacy Policy to explain to you how and why your personal data is processed by Fuller's.

WHO COLLECTS THIS INFORMATION?

Fuller, Smith and Turner P.L.C. (the Company) is a 'Data Controller' and gathers and uses certain information about you. This information is also used by our affiliated entities and group companies (our 'group companies') and so, in this Policy, references to 'we', 'our', 'Fuller's' or 'us' mean the Company and our group companies.

Fuller's is the parent company Griffin Catering Services Limited (company number 01577632), B & D Country Inns I Limited and B & D Country Inns II Limited (company number 07292333 and 08029280 trading as Bel & The Dragon), and Cotswold Inns and Hotels Limited (company number 03309179 – trading as Cotswold Inns & Hotels). Therefore, Fuller's is the Data Controller for personal data that is processed at all the limited companies listed.

Our Head Office is located at: Pier House
86-93 Strand-on-the-Green
London, W4 3NN

Our Phone number: 020 8996 2000

If you want to get in touch with our Data Protection Officer about this Privacy Policy, or for any other data protection matters, you can do so by emailing: privacy@fullers.co.uk.

PERSONAL DATA WE COLLECT ABOUT YOU

We may collect the following information about you during your employment:

- **Contact data** – Address(es), personal and work email address(es), personal and work telephone number(s), emergency contacts (e.g. name, relationship and home and mobile phone numbers).
- **Criminal convictions & offence data** – Details of unspent convictions.
- **Education data** – Qualifications achieved, school, college, university attended.
- **Emergency contact / Next of Kin data** – Details of any person who is your Next of Kin or emergency contact which may include, for example, your spouse/partner and any dependents.
- **Health data** – Information in your sickness, absence and accident records (including sensitive personal data regarding your physical and/or mental health).
- **Identity data** – Name, title, image data, driving license number, NI number, DOB, nationality, passport, birth certificate, signature, racial or ethnic origin, gender, biometric data, religious or similar beliefs, nationality, immigration status and information from related documents.

- **Job data** – Current job title, department you work in, employment history, references, job description, site location you are employed at, your contracted hours, your start date, performance rating, internal vacancies applied for, progression opportunities, information collected through the recruitment process.
- **Leave data** – Dates of absences, reason for absence (sickness, holidays or otherwise).
- **Payment data** – Sort code, account number, bank branch, tax code, tax contributions, P11D, P60 and P45 forms.
- **Personnel data** – Interview notes, grievances, comments on specific situations, disciplinaries, performance appraisals, performance reviews, any training undertaken, uniform size (where a uniform is needed), Company shares and details of your use of business-related social media, such as LinkedIn.
- **Salary data** – Yearly salary or hourly wage, pension deductions, clock in time, clock out time, hours worked, holiday pay and sick pay.
- **Social media data** – Your use of public social media (only in limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur).
- **Technical data** – Information about your use of our IT, communication and other systems, and other monitoring information.
- **Trade union data** – Information on an employee's trade union membership and their representative.

HOW WE COLLECT YOUR PERSONAL DATA

Your personal data is collected in a variety of ways, both before and throughout your employment.

Your personal data is collected from you when you:

- Complete a Fuller's job application and submit it to us;
- Send us your CV;
- Use your available benefits with Fuller's;
- Sign your employment contract;
- Submit holiday or leave requests;
- Provide us with a sick note;
- Clock in/out for your shift;
- Correspond with us via email, text, telephone or post; and
- Use/ Log into Fuller's IT systems and software.

We collect personal data about you when we:

- Operate CCTV;
- Provide you with employee training;
- Complete employee appraisals; and
- Complete disciplinaries and grievances.

HOW AND WHY WE USE YOUR PERSONAL DATA

In accordance with UK data protection legislation, we make sure that we have a lawful basis for processing your personal data.

The following personal data is collected from you for the **legal obligation** we have as an employer:

- Your identity, contact, job, leave and health data are used to document accidents that happen on site in accordance with our obligations under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR).
- Your identity data is used to ensure you have the right to work in the UK. This is in accordance with our obligations under the Immigration, Asylum and Nationality Act 2006.
- Depending on your role in the business, your identity data may be used for diversity and inclusion reporting purposes in accordance with regulatory requirements.

The following personal data is collected from you for the **performance of a contract** which we have entered into with you:

- Your identity, job, education, criminal convictions & offence data are used to determine your suitability for a role within Fuller's prior to your employment and are subsequently maintained within your personnel file.
- Your identity, contact, job and personnel data are used to contact you if we want to communicate with you about your employment;
- Your identity, contact, payment and salary data are used to administer payments and benefits to you in line with your employment contract and ensure that payments are accurate;
- Your identity, contact, job and personnel data will be used to administer training to you in line with your employment contract;
- Your identity, emergency contact / Next of Kin and health data will be used to contact your emergency contact/Next of Kin if necessary (e.g. if you have been injured while on shift);
- Your identity, salary, personnel, leave, health, social media, technical, trade union membership and job data are used to manage and monitor your employment; and
- Your identity, contact, technical and job data will be used for login IDs in order for you to access Fuller's internal systems.

- Your identity, contact, job, personnel and health data is used to ensure that you are able to perform your role and responsibilities.

The following personal data is collected from you for Fuller's **legitimate interests**:

- Your identity, contact and personnel data will be used to conduct employee engagement surveys;
- Your identity, job and personnel data will be shared with relevant managers following your exit interview to help provide feedback on how management and affected departments can improve. If you don't want your personal data to be shared for this purpose, you have the right to opt-out of this processing;
- Your identity, contact and job data may be processed if you decide to make a report using the various arrangements under our Whistleblowing Policy. This only applies where you have not decided to make an anonymous report;
- Your identity and social media data will be processed if your use of social media negatively affects the organisation and this needs to be investigated.
- Your identity, contact and technical data are used to provide you with complimentary Wi-Fi; and
- Your identity data will be collected when you are captured on CCTV while visiting a Fuller's venue. The CCTV footage will be used for the purposes of the prevention and detection of crime and to protect our employees and guests while on site. If requested, CCTV footage may be provided to the police.

Fuller's will collect your **consent** in order to use your identity data for diversity and inclusion reporting purposes where it is not legally required.

If you fail to provide the personal data required, we may be unable to offer or continue your employment at Fuller's.

Your personal email will be required as a login ID for access to various Company software and/or websites.

Special Category Data

Details relating to your health, trade union membership, racial or ethnic origin, religion or similar beliefs is considered special category data under UK Data Protection Law and as such, we must have a special category condition to process this information. If we are required to process your special category data, we will rely on the following conditions:

- Employment, Social Security and Social Protection;
- Health and Social Care; and
- Substantial Public Interest Condition(s):
 - Equality of opportunity and treatment;
 - Racial and ethnic diversity at senior levels.

SHARING YOUR PERSONAL DATA

In order to run our business and employee operations efficiently, we require the involvement of third-party organisations. This is so Fuller's can operate parts of the business which include:

- Administering e-learning to employees;
- Administering employee benefits to employees;
- Administering our recruitment platform;
- Providing a HR portal to employees;
- Administering employee share plans;
- Measuring employee engagement;
- Administering the various arrangements under our Whistleblowing Policy;
- Conducting identity verification checks; and
- Obtaining advice from our legal or professional advisors.

If requested, we will share your personal data with authorities such as:

- Your trade union representative;
- The Police;
- The Health and Safety Executive;
- Local Authorities;
- Her Majesty's Revenue and Customs (HMRC);
- The Courts; and
- Central or Local Government Bodies.

TRANSFERS OF DATA OUTSIDE THE EEA

The European Economic Area (EEA), consists of the EU Members States, Iceland, Liechtenstein and Norway. If we transfer your personal data outside of the UK and the EEA, we have to tell you and we will use one of the following bases:

- **Adequacy decision:** The country we send your personal data to must provide an adequate level of protection which has been approved by the European Commission.
- **Standard Contractual Clauses:** The recipient of your personal data has provided us with signed Standard Contractual Clauses which has been approved by the European Commission. This holds the recipient accountable to safeguard the personal data.

Limited situations where your personal data may be transferred outside of the EEA are as follows:

Purpose of Processing	Nature of the information	3rd Party	Location	Appropriate and suitable safeguards
Administration of the HR Portal	<ul style="list-style-type: none"> • Identity data • Contact data • Payment data • Salary data • Job data • Personnel data • Leave data 	Fourth Enterprises LLC	United States	Standard Contractual Clauses
Sharesave Scheme	<ul style="list-style-type: none"> • Identity data • Contact data • Payment data • Salary data • Job data 	Equiniti Limited	India	Standard Contractual Clauses
Recruitment platform	<ul style="list-style-type: none"> • Identity data • Contact data • Job data • Education data • Personnel data • Health data 	Harri US LLC Harri Ramallah	United States Palestine	Standard Contractual Clauses
Share Incentive Plan (provision of 2 factor authentication)	<ul style="list-style-type: none"> • Identity data • Contact data 	Computershare (Twilio)	United States	Standard Contractual Clauses

KEEPING YOUR PERSONAL DATA SECURE

We protect the personal data that you have entrusted to us by using appropriate technical and organisational security measures, as well as ensuring that those organisations we share your personal data with are just as careful with your personal data as we are.

Your personnel files are stored securely both manually and within Fourth HR and only authorised members of staff can access these. If you are an employee within one of our Managed Houses (e.g. Front of House Team or Kitchen Team), your personnel file is maintained by your General Manager.

RETENTION OF YOUR PERSONAL DATA

We will only retain your personal data for as long as necessary to fulfil the purpose(s) for processing. This includes satisfying any legal, accounting, or reporting requirements.

When we assess the retention of your personal data, we will take the following into consideration:

- Nature of the information;
- Sensitivity of the information;

- Potential risks if the information was breached;
- The purpose(s) for which we initially processed the information;
- Whether we can achieve the purpose(s) through less invasive means; and
- Any applicable legal requirements.

Your employee records will be kept by us for the duration of your employment plus a minimum of six years following termination.

After this period has expired, we will review the data records and securely delete your records where required.

YOUR RIGHTS

Everybody has rights relating to the collection and use of their personal data. These are the rights that apply to your personal data held within Fuller's:

- **The right to be informed** – you have the right to know what information we hold and process about you which is why we have provided this Privacy Policy.
- **The right of access** – you have the right to ask for a copy of the information we hold regarding yourself.
- **The right to rectification** – you have the right to ask for us to correct any information we hold which may be inaccurate or incorrect.
- **The right of erasure** – you have the right to have your personal data 'erased' in the following situations:
 - Where the personal data is no longer required for the purpose(s) for which it was originally collected or processed;
 - Where the processing was based on consent and you have withdrawn your consent;
 - When the personal data was unlawfully processed; and
 - When the personal data has to be erased in order to comply with a legal obligation.

We will erase your records when one of the above situations apply.

- **The right to object** – you have the right to object to the processing of your personal data in the following circumstances:
 - The purpose of the processing activity is direct marketing;
 - Where the processing is based on legitimate interests; and
 - Processing for the purposes of scientific/historical research and statistics.
- **The right to restriction of processing** – you have the right to ask us to restrict the processing of your personal data in certain situations such as:
 - Where you contest the accuracy of your personal data, we will restrict the processing until you have verified the accuracy of your personal data;

- When processing is unlawful, and you oppose erasure and request restriction instead; and
 - Where we no longer need the personal data, but you require the information to establish, exercise or defend a legal claim.
- **The right to data portability** – You have the right to request that we transfer your personal data to a third-party. This right only applies to automated personal data which you have either provided your consent for us to use or where we have used your personal data to perform a contract with you.
 - **Rights in relation to automated decision-making including profiling** – you have the right to question decisions being made about you without any human involvement.

If you would like to exercise any of these rights, please get in contact with us using the details found at the bottom of this Privacy Policy.

UPDATES TO OUR PRIVACY POLICY

We may update this Privacy Policy from time to time. If we make changes to this Privacy Policy, the updated version will be made available to team members through publication on FUSE.

CONTACT INFORMATION

If you have any questions about this Privacy Policy or how your data is processed, please contact us at Fuller, Smith & Turner P.L.C., Pier House, 86-93 Strand on the Green, London, W4 3NN, or phone on 020 8996 2000 or email to privacy@fullers.co.uk.

Should you have any concerns about this Privacy Policy or the way that we are processing data you have the Right to Lodge a Complaint with the Information Commissioner's Office. Please look at <https://www.ico.org.uk> for more detail.

VERSION CONTROL

Version	Date	Approval by	Detail
1	31 May 2022	Executive Committee	Policy Adopted
2	September 2022	Executive Committee	Policy amended