Nutwood Pubs Data Protection Policy

Introduction

We hold personal data about our employees, clients, suppliers, and other individuals for a variety of business purposes. Personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards which are set out in the General Data Protection Regulations ("**GDPR**").

This policy sets out how we seek to protect personal data, comply with the GDPR and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Privacy Manager is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract, and other staff, clients, suppliers, and marketing contacts. Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offenses, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.
Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll , and business development purposes. Business purposes include the following: - Compliance with our legal, regulatory and corporate governance obligations and good practice - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests - Ensuring business policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as recording transactions, training and, quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring, and checking - Investigating complaints - Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration, and assessments - Monitoring staff conduct, and disciplinary matters - Marketing our business - Improving services

Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

The HR manager has overall responsibility for the day-to-day implementation of this policy.

The GDPR – general principles

The GDPR sets out six key principles which govern how any organisation is allowed to process personal data. We will process personal data in compliance with these principles. Personal data will be:

1. Processed lawfully, fairly, and in a transparent manner in relation to individuals.

2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Adequate, relevant, and limited to what is necessary for relation to the purposes for which they are processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Underpinning these is the principle of 'accountability'. This requires us to be able to demonstrate compliance with each of the principles above.

Processing personal data

Notifying individuals
In the general principles section above, we refer to the principle that requires personal data to be processed fairly, lawfully, and in a transparent manner.

A specific requirement of this principle is that we must provide detailed, specific information to data subjects about what we are doing with their personal data. Our notices must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

Our Terms of Business contains a Privacy Notice that covers both client and employee data. The notice:

- Sets out the purposes for which we hold personal data on customers and employees.
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers.
- Provides that customers have a right of access to the personal data that we hold about them.

Identifying a condition for processing

Another specific requirement of the principle that requires personal data to be processed fairly, lawfully, and in a transparent manner, is that we must be able to demonstrate that we have a lawful basis for the processing activity in question (known as a 'condition for processing').

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice. In summary, they are as follows:

- ***Personal data***: consent of the data subject; necessary for the performance of a contract, a legal obligation; the vital interests of the data subject; where it is in the public interest or our own legitimate interests; and

- ***Sensitive personal data****:* explicit consent of the data subject; obligations in the field of employment, social security, and social protection law; vital interests of the data subject; processing by not-for-profit bodies; personal data made manifestly public by the data subject; establishment, exercise or defence of legal claims; substantial public interest; preventative or occupational medicine; public health; research purposes.

Relying on consent

As set out above, one of the conditions for processing is consent and this is important to consider because we rely on consent for some important activities. For example, when we send marketing emails to customers, this will invariably be because we have asked and they have provided their consent.

Relying on explicit consent

In most cases where we process sensitive personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the HR Manager or Marketing Manager.

Our procedures and other practical issues to be aware of

Your personal data

You must take reasonable steps to ensure that the personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the HR or Marketing Manager so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the HR and Marketing Managers will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.

- Printed data should be shredded when it is no longer needed.

- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.

- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- The HR and Marketing Managers must approve any cloud used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the company's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets, or smartphones.
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the relevant manager, HR or Marketing.

Direct marketing

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Marketing Manager about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the Marketing Manager for advice on direct marketing before starting any new direct marketing activity.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar or directly with the HR Manager, on a regular basis.

It will cover:

- The law relating to data protection.
- Our data protection and related policies and procedures.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Marketing and HR Managers will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible, and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

Monitoring

Everyone must observe this policy. The HR Manager has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Responsibilities

Responsibilities of the HR Manager:

- Keeping the board updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from staff, board members, and other stakeholders.
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Nutwood Pubs Ltd.
- Checking and approving with third parties that handle the company's data any contracts or agreements regarding data processing.

Responsibilities of the IT Department

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services, such as cloud services the company is considering using to store or process data.

Responsibilities of the Marketing Manager

- Approving data protection statements attached to emails and other marketing copy.
- Addressing data protection queries from clients, target audiences or media outlets.
- Coordinating with the HR and IT Department Manager to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.

Responsibilities of all staff

As well as the specific responsibilities of the individuals mentioned above, all individual staff members should:

- Be aware of our responsibilities and obligations, which should include following the guidelines set out in this policy.
- Keep confidential any personal data held by us, including relating to customers and individuals from other entities (such as other employees, vendors, and clients).
- Enter records accurately and update records on becoming aware of any inaccuracy.
- Refrain from recording details and opinions of a racial, political, religious or sexual nature, or comments on physical or mental health, unless these details are strictly necessary for carrying out our work.
- Not remove personal data from the work-place, unless there is a legitimate reason for doing so and you are able to keep such data secure.

Individual's rights

Under the GDPR individuals are able to exercise various rights in relation to their personal data.

Subject access requests

One of the most far reaching of these rights is right of access under the right of access (commonly known as a Subject Access Request or "SAR") individuals are entitled to require us to provide a copy of the personal data we hold about them along with certain information about how such data is processed.

If you receive a subject access request, you should refer that request immediately to the HR and Marketing Managers. We may ask you to help us comply with those requests.

Please contact the HR Manager if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Additional rights

Individuals also have the following rights:

- ***Right to be informed*** – data subjects have the right to know the identity of the data controller, the reason for processing and any other information which ensures that their data is processed in a way that is fair and transparent.

- ***Right to rectification*** – data subjects are entitled to require data controllers to correct any errors in their personal data.

- ***Right to erasure*** – data subjects are entitled to require a controller to delete their personal data if the continued processing of that data is not justified (commonly known as the 'right to be forgotten'). If we receive a right to erasure request it must comply where the ground for processing the personal data is the individual's consent (and there are no other grounds (for example, legitimate business interest) for processing the data) or, more generally, where the personal data is no longer needed for the purpose for which it was collected or is now being used.

- ***Right to restrict processing*** - data subjects may, in certain circumstances, be able to limit the purposes for which a data controller processes their data.

- ***Right to data portability*** – data subjects have the right to transfer their personal data between controllers (e.g. to move account details from one entity to another).

- ***Right to object*** – there are certain situations in which data subjects may be able to object to the processing of their data, this will only apply where the controller's basis for processing the data is either public interest or legitimate interest. Notwithstanding this, if an individual objects to processing

for direct marketing purposes (i.e. they object to us sending marketing emails, mailshots etc) then the right to object is absolute.

- ***Right to not be evaluated on the basis of automated processing*** – data subjects have the right not to be evaluated in any material sense (e.g. in connection with discount offers) solely on the basis of automated processing of their personal data.

Keeping records of our data

As part of our obligations under the GDPR, we will maintain records of our data processing.

An example of the level of detail covered in these records is shown below. If you are responsible for processing data about a particular category of individuals, you may have your duty to help keep these records up to date. If you have any questions, please contact the Privacy Manager.

What information is being collected?	**Employee data, Guest data**
Who is collecting it?	HR/Payroll, Marketing, Pubs, Inns
How is it collected?	Payroll uses S4 to collate and record employee information. The information is input (predominantly) by Pub Managers. Payroll information may be passed onto an external accounting firm if required. Marketing Dept. and Pubs canvas guests for limited personal information for marketing purposes via email, online and sign-up cards in pubs
Why is it being collected?	Employee records and pay Guest Marketing
How will it be used?	Internal use only
Who will it be shared with?	Nobody has access to guest information. Employees, contractors and payment agreement information may be passed onto an external accounting firm if required.
Identity and contact details of any data controllers	TBC
Details of transfers to third countries and safeguards	None. The systems are password protected
Retention period	TBC

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the HR Manager.

Recruitment

This privacy notice tells you about the information we collect from you when you apply for a job role through our websites, agencies, job boards or, in person applications. By collecting this information, we are acting as a data controller and, by law, we are required to provide you with information about us, about why and how we use your data, and about the rights you have over your data. We ask for your consent before collecting or processing any of your personal information.

What is the purpose of this document?

Nutwood Pubs Ltd (UKCRN 06917649) is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

It applies to all employees, workers, and contractors.

Nutwood Pubs Ltd is a 'controller'. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers, and contractors. This notice does not form part of any contract of employment or another contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation. Information about criminal convictions also warrants this higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Next of kin and emergency contact information.
- National Insurance number.

- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Recruitment information (including copies of right-to-work documentation, references, and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.

  We may also collect, store and use the following more sensitive types of personal information:
- Information about your health, including any medical condition, health and sickness records, including:
- details of any absences (other than holidays) from work including time on statutory parental leave and sick leave;
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations or exercise rights in connection with employment.

3. Where it is needed in the public interest, such as for equal opportunities monitoring.

4. Where it is necessary to protect you or another person from harm.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Situations in which we will use your sensitive personal information

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for the processing, such as it is in the public interest to do so. The situations in which we will process your particularly sensitive personal information are listed below.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence, and to administer benefits including statutory maternity pay, statutory sick pay, and pensions.

- If we reasonably believe that you or another person are at risk of harm and the processing is necessary to protect you or them from physical, mental or emotional harm or to protect physical, mental or emotional well-being.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.]

- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your well-being and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, pension administration, IT services.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service

providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the HR Manager.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the HR Manager in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the HR Manger. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this Data Privacy Notice, please contact your line manager.

To submit a request by email, post or telephone, please contact the Data Protection Officer on the details below:

Email: hr@nutwoodpubs.com

Tel: c/o The Woodman Inn, Marketing Manager 01763 848328

Postal address: Nutwood Pubs Ltd (UKCRN 06917649), 291 Green Lanes, London N13 4XS, England

Your right to complain

If you have a complaint about our use of your information, you can contact the Information Commissioner's Office via their website at www.ico.org/concerns or write to them at:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF