Warren Policies & Procedures
Updated (07/09/23)

Contents…

1. Tips
2. Breaks
3. Clothing
4. Discounts
5. Mobile Phones
6. Safe Policy
7. Vouchers
8. Staff Food and Drink
9. Smoking
10. Sickness
11. Disciplinary
12. Privacy Notice
13. IT, Social Media, and Communications Systems Policy
14. Data Security

1. Tips

Cash Tips: I understand that cash tips will be evenly distributed among all members of staff and management who were working during a particular shift. These cash tips will be paid to me once they are ready.

Card Payment Tips: I understand that card payment tips will be distributed based on the number of hours I have worked during the designated period. These card tips will be included in my monthly wage payment.

2. Breaks

Duration of Breaks: I understand that, in accordance with company policy:

- During shifts lasting more than 6 hours, I am entitled to take an uninterrupted 20-minute break.
- For shifts lasting less than 4 hours, I have the option to take a 10-minute break.
- In the case of split shifts, where I have two shifts each less than 4 hours, I am entitled to take two optional 10-minute breaks during my shift.

Break Usage: I understand that these break periods are provided for my convenience, allowing time for a drink, meal, mobile phone usage, or a cigarette break.

Unpaid Time: I acknowledge that these breaks are unpaid and are considered my personal time, not compensated by The Warren.

Clocking Procedures: If I choose to take a break during a shift, I must clock out and then back in when I resume work.

Between-Shift Breaks: I also understand that any breaks between my shifts are unpaid.

3. Clothing Policy

General Guidelines:

All employees are required to dress in a manner that is work-appropriate and reflects professionalism at all times.

Clothing Restrictions: 2. Workout attire and clothing typically worn for outdoor activities are not permitted within the workplace.

4. Clothing that is excessively revealing or inappropriate is not allowed. This includes items such as low-cut tops, short shorts, and attire with offensive graphics or slogans.
5. All clothing must be clean and in good condition. Clothing with discernible rips, tears, or holes is not acceptable.
6. Employees are expected to avoid wearing clothing with offensive or inappropriate prints, patterns, or messages.

7. Footwear
    - All employees are required to wear closed-toe, non-slip, and non-skid shoes while on duty.
    - The footwear should provide adequate support and protection for the specific job duties of each role.
    - For kitchen staff, shoes must be heat-resistant, non-slip and designed for kitchen work.
    - For front-of-house staff, footwear should be clean, presentable, and suitable for the restaurant's atmosphere.

Uniform Compliance:

- Footwear must be in good condition and compliant with the restaurant's uniform policy.
- Any non-compliant footwear may result in corrective action.

Hygiene and Safety:

- Footwear must be clean and well-maintained to ensure food safety and a professional appearance.
- Non-slip and non-skid soles are essential to prevent accidents, especially in kitchen areas.

Comfort and Fit:

- Employees should ensure that their footwear is comfortable and fits properly to prevent discomfort or accidents during shifts.
- It is the responsibility of employees to replace worn-out or damaged footwear promptly.

Responsibility:

- Supervisors and managers will periodically inspect employees' footwear to ensure compliance with this policy.
- Employees are encouraged to report any issues with their footwear to their supervisor promptly.

4 Discounts

Discount Entitlement:

Staff members are entitled to a discount of 20% on purchases made both during and outside of their shifts.

Authorization Requirement: 2. To avail of the staff discount, employees must obtain authorization from management.

Payment Procedure: 3. All items purchased by staff members must be paid for immediately at the time of purchase and should not be added to a tab or deferred for later payment.

Compliance: 4. Failure to comply with this staff discounts policy may result in the revocation of staff discount privileges, in accordance with company policies.

5. Mobile Phone Policy - The Warren

General Guidelines:

1. Employees must not have their phones on their person while working in the kitchen or on the restaurant floor during their scheduled working hours.

Storage Requirement: 2. Phones should be securely stored with personal belongings in the designated lockers.

Phone Use: 3. Mobile phones may only be used during unpaid break periods.

Emergency Contact: 4. In the event of an emergency, employees are responsible for asking family and friends to contact the restaurant directly.

Exceptions: 5. This policy does not apply to management or the head chef (chef in charge), General Manager, Front of House Manager or manager on shift. They may use their phones for work purposes as necessary. Any use of mobile phones during working hours by other staff members must be approved by the General Manager or Front of House Manager.

6. Safe Policy

Access to the Safe:

Access to the safe located in the office is limited to the Front of House Manager, General Manager, or the designated shift supervisor in charge.

Security Protocol: 2. After use, the safe must be securely locked.

Key Handling: 3. The safe key must be promptly returned and securely stored in the till after use.

7. Vouchers

Usage Procedure: 2. When a voucher is redeemed, it must be checked against the voucher book, marked off as used, and placed into the till. These records will be verified during the cashing up process.

8. Staff Food & Drink Policy

Staff Meals:

> Staff members on a shift are entitled to a complimentary basic meal, such as soup and bread or any available kitchen offering.

Complimentary Beverage: 2. One complimentary coffee or tea per shift is available to staff. This does not include alcoholic beverages or soft drinks (excluding squash or lemonade).

Timing for Staff Coffees: 3. Staff coffees should not be consumed during service hours.

Discounted Purchases on Shift: 4. While on duty, staff may purchase food and beverages at a 20% discount. Payment must be made when ordering, not afterwards or on tabs.

Off-Shift Discounts: 5. Off-duty staff members are eligible for a 20% discount on all food and drink purchases for their personal consumption only.

Authorization Requirement: 6. The provision of these discounts is subject to authorization by management.

9. Smoking Policy - The Warren

Smoking During Breaks:

- Employees who smoke have the option to do so during their unpaid breaks.

Designated Smoking Area: 2. Smoking must take place exclusively in the designated smoking area, located near the bins and out of sight from the public.

Additional Smoking Arrangements: 3. If an employee requires more frequent smoking breaks than scheduled breaks permit, they must obtain approval from their Manager or Head Chef.

10. Sickness Policy

1. Reporting Illness: Employees who are feeling unwell or experiencing symptoms of illness, such as fever, vomiting, diarrhea, or other contagious conditions, must notify their head chef or front of house manager immediately and should not report to work.
2. Medical Certification: Employees who are absent due to illness for more than seven consecutive days, including weekends and bank holidays, must provide a fit note from their doctor (also known as a Statement of Fitness for Work) as required by the Statutory Sick Pay (SSP) regulations.

3. Sick Pay: Eligible employees will be entitled to Statutory Sick Pay (SSP) as per the applicable laws and regulations.
4. Return to Work: Employees who have been absent I undue to illness must check in with their manager before restarting work.
5. Confidentiality: All information related to an employee's illness, including medical documentation, will be treated as confidential and will only be shared with appropriate personnel on a need-to-know basis. Disclosing an employee's medical condition to others without proper authorization is strictly prohibited and may be a breach of data protection laws.
6. Preventive Measures: The company will take appropriate preventive measures, such as regular cleaning and sanitization, providing personal protective equipment (PPE) to employees, and promoting good hygiene practices, to reduce the risk of illness transmission among employees and customers, in accordance with relevant health and safety guidelines.
7. Training and Education: The company will provide necessary training and education to employees on the importance of reporting illnesses, good hygiene practices, and the company's sickness policy to ensure a safe and healthy work environment.

11. DISCIPLINARY PROCEDURES

Introduction

We have developed our disciplinary procedures in order to provide clear and transparent structures for dealing with difficulties which may arise as part of the working relationship and to ensure that such difficulties are dealt with in a fair and equitable manner in compliance with the acas code of practice.

We would hope to informally resolve potential disciplinary issues. However, where an issue cannot be resolved informally, then there is often no option other than to follow a formal process. This policy sets out the basic requirements of fairness that will be applicable in most cases.

We regard disciplinary action as a corrective measure to foster an improvement in the conduct or attitude of the employee concerned and not as a punishment. Disciplinary procedures are necessary to let all of our employees know what is expected of them in terms of standards of performance or conduct (and the likely consequences of continued failure to meet these standards) and to enable management and employees to determine suitable goals and timescales for improvement in an individual's performance or conduct. The following procedures do not form part of your contract of employment.

The process

There will normally be a full investigation of the facts before a decision to take any disciplinary action is invoked. Dependent upon the circumstances, we may hold an independent investigation meeting to determine if a formal disciplinary hearing is necessary. At all stages of the process, we will ensure that matters are kept confidential and expect you to do the same.

If we feel that it is necessary to take disciplinary action, we will notify you in writing of our concerns. where relevant, we will supply you with details of any evidence we will be using in the disciplinary hearing. You will be given a reasonable amount of notice to attend the meeting and to arrange for another member of staff or a trade union official to accompany you.

If we regard an offence as potential gross misconduct, we may suspend you on your normal contractual pay for the duration of the process. This period will be kept as short as is reasonably practical to investigate the matter, hold any necessary disciplinary hearing and consider the outcome.

At the meeting, we will outline our concerns and you will be given ample opportunity to explain your version of the situation and also to bring any supporting evidence to our attention. you may also ask witnesses to deliver their version of events to support you if you so wish. We will listen to what you say and will consider all points you put forward before reaching a decision on whether any disciplinary sanction is to be imposed. no decision will be made regarding any disciplinary action before we have had time to consider the discussion and any evidence produced at the meeting.

Outcome of the meeting/s

After the meeting has concluded we will take time to consider all the evidence and we will take one of the options listed below:

1. no action

   if we feel that there is no case to answer, or there is insufficient evidence to support any action or if we feel that you were genuinely unclear about what was expected from you and you agree to take remedial action, we may decide it is appropriate to take no further action.

2. warning

   if we feel that you have not presented a valid reason or supporting evidence for the misconduct, we will issue you with a formal warning. dependent upon the circumstances, this could either be a formal verbal warning, a written warning, or a final written warning.

   except for cases of gross misconduct or a short period of service, we will not normally proceed to dismissal for a first offence.

3. dismissal
   if you are in receipt of prior warnings, we may decide to terminate your employment with us, giving you your contractual notice. if your misconduct is determined to be gross misconduct, then you will be summarily dismissed, (without any notice or pay in lieu of notice), irrelevant of whether or not you have had any previous warnings.

4. demotion

   if you are in a supervisory or managerial position, we may decide to demote you, except in the case of gross misconduct.

5. suspension without pay
   we may decide to suspend you without pay for a period up to 5 working days, except in the case of gross misconduct.

Notification of outcome of the disciplinary meeting

We will notify you, in writing, as soon as we have considered the evidence and have reached a decision. the timescale will depend upon the complexity of the situation however, this will normally be no more than 7 calendar days after the meeting has taken place, unless there is good reason why this cannot be so. The letter will outline our reasons for the decision made and, where disciplinary action is taken, the level or nature of the sanction imposed. It will also name the person to whom you should address an appeal to should you wish to do so.

Right to be accompanied

You have the right to be accompanied by a fellow employee of your choice, or by a trade union official at all stages of the formal disciplinary procedures and at any subsequent appeal meetings.

It is your responsibility to arrange for the appropriate person of your choice to be informed of the matter and the dates of the hearing/s. If you wish a member of staff to accompany you, then either yourself or the person concerned, should notify us as early as possible, so that we can ensure that they can be released from their duties at the appropriate times.

We wholeheartedly support the right to be accompanied and any person who agrees to support a member of staff at any disciplinary or appeal hearing, will not be subject to any form of detriment as a result of doing so.

Record-keeping

We will take notes of all meetings held and these, along with any supporting evidence used in the investigation and meetings will be held on your personnel file. details of any disciplinary action taken will also be kept.

Administration of disciplinary warnings

Warnings will normally be issued in line with the following guidelines, however this is not prescriptive. When deciding the level of action to be taken, we will take account of any mitigating factors, including your length of service and may vary the process or the administration of warnings accordingly. Dependent upon your length of service, you may be dismissed without any previous warnings.

Other than in cases of gross misconduct, we may choose to demote you or suspend you for up to five working days without pay as an alternative to dismissal.

offence	1st occasion	2nd occasion	3rd occasion	4th occasion

unsatisfactory conduct	formal verbal warning	written warning	final written warning	dismissal
misconduct	written warning	final written warning	dismissal	
serious misconduct	final written warning	dismissal		
gross misconduct	dismissal			

examples of unsatisfactory conduct and misconduct

- failure to comply with our health and safety rules.
- gambling.
- smoking outside of designated areas and/or outside of your authorised break times.
- unacceptable levels of absenteeism or lateness.
- failure to follow our absence reporting procedures.
- unsatisfactory work performance.
- failure to carry out reasonable management instructions.
- failure to comply with business rules, procedures and guidelines.
- use of objectionable or insulting language or behaviour.
- failure to report any damage to our property or premises caused by you or witnessed by you.
- breach of our email and internet policy, including excessive personal use.
- deliberate misuse or neglect of business property or vandalism.
- excessive use of the business's telephone for personal calls.
- negligence in the performance of your duties.
- leaving your place of work without prior authorisation.
- unauthorised use of our vehicles.
- allowing unauthorised people to use our vehicles.

serious misconduct

Dependent upon the circumstances, any of the above examples could be deemed to be serious misconduct and as such, if a disciplinary sanction is imposed this could be a final written warning even though no other warnings have been given.

examples of gross misconduct

- theft or fraud.
- physical violence or bullying.
- threatening behaviour or language.
- being under the influence of alcohol.
- attending work under the influence of illegal drugs, or being in possession or supplying illegal drugs whilst at work or during working hours.
- any action, or breach of health and safety rules which does, or could be expected to, endanger the health or safety of yourself or any other person.
- acceptance or administration of gifts or hospitality etc. without prior permission from the business.
- bribing or attempting to bribe another individual, or personally taking or knowingly allowing another person to take a bribe.
- any act or omission which could cause the reputation or integrity of the business to be compromised or bring the business into disrepute.
- discriminatory behaviour.
- deliberate fraudulent or false claims of bullying, harassment or victimisation.
- accessing internet sites or downloading information from such sites, which contains offensive, illegal, obscene or pornographic material.
- knowingly perpetrating or taking part in acts of discrimination or harassment.
- providing false information re your right to work in the uk.
- deliberate and serious damage to property.
- causing loss, damage or injury through serious negligence.
- unauthorised use or disclosure of confidential information or failure to ensure that confidential information in your possession is kept secure.
- serious misuse of the business's information technology systems (including misuse of developed or licensed software, use of unauthorised software).

nb: The above lists are neither exhaustive nor prescriptive in the level of disciplinary sanction which may be imposed. You may be disciplined for any other reason which is considered misconduct or unsatisfactory conduct.

When considering the level of disciplinary action to be taken against individuals, we will take into account both the severity of the offence, the impact on the business or other individuals and any mitigating circumstances.

Therefore, the above categories are guidelines only and a higher or lower level of disciplinary action may be imposed, dependent upon the circumstances.

Validity period of warnings

We will keep a record of warnings issued and appeal details in your personnel file. Whilst such information will normally be kept in your personnel file permanently, it will normally be disregarded for further disciplinary purposes in line with the following:

verbal warning – after a period of 3 months
written warning – after a period of 6 months
final warning – after a period of 12 months

Authority to take disciplinary action

The following persons are authorised to take disciplinary action. this does not prevent another member of staff, or other appropriate nominated person to take such action.

	person/s authorised to take disciplinary action in the case of all staff
Formal verbal warning	Manager
Written warning	Manager
Final written warning	Manager
Dismissal	Manager
Demotion	Manager
Suspension without pay	Manager

Appeal process

If you feel you have been treated unfairly in the disciplinary process, or that the sanction imposed was too heavy or unfairly administered, you have the right of appeal.

You should write to the person detailed in the outcome letter, within 7 calendar days of the date of the letter, outlining the grounds for your appeal. We will then arrange to hear your appeal, normally no more than 14 calendar days after receipt of your letter of appeal.

In interests of fairness, your appeal will normally be held by a different person than the one who held the disciplinary hearing.

We will notify you in writing of the decision, normally within 14 calendar days of the hearing.

12 Privacy Notice

We are committed to protecting the privacy of our employees and ensuring the security of their personal information. This privacy notice explains how we collect, use, and safeguard employee data in the course of employment. We are dedicated to complying with the General Data Protection Regulation (GDPR) and all relevant UK data protection laws.

1. Data Controller: Deri Reed

2. Information We Collect: As part of your employment, we may collect and process the following types of personal information:

- Personal Details: Your name, address, contact details, date of birth, and national insurance number.
- Employment Information: Details related to your employment, including job title, department, salary, and work schedule.
- Payment Details: Bank account information for salary payments.
- Emergency Contact: Information about your emergency contact person.
- Health Information: Health-related data for statutory and safety purposes.
- CCTV: We have CCTV cameras on our premises for security purposes, and you are recorded while on our premises.

3. How We Use Your Information: We use your personal information for the following employment-related purposes:

- To manage your employment, including payroll processing.
- To meet legal obligations, such as tax and employment law requirements.
- To ensure the safety and security of our premises through CCTV.
- To communicate with you regarding employment matters.
- To administer benefits, if applicable.
- To facilitate emergency contacts in case of emergencies.

4. Legal Basis for Processing: We process your data based on the following legal grounds:

- The necessity of processing for the performance of an employment contract.
- Compliance with legal obligations (e.g., employment and tax laws).
- Our legitimate interests (e.g., security and safety).
- Consent, when applicable (e.g., emergency contact information).

5. Data Sharing: We may share your data with third parties only when necessary for employment-related purposes, such as payroll processing, tax authorities, and benefits providers.

6. Data Security: We have implemented measures to protect your data from unauthorized access, disclosure, alteration, or destruction. Our staff is trained on data protection and privacy matters.

7. Your Rights: As an employee, you have rights under data protection laws, including:

- The right to access your data.
- The right to rectify inaccurate data.
- The right to erasure (in certain circumstances).
- The right to restrict processing (in certain circumstances).
- The right to data portability.
- The right to object to processing.
- The right to withdraw consent (if applicable).

8. Data Retention: We will retain your employment-related data for as long as necessary to fulfill the purposes for which it was collected, including legal and regulatory requirements.

9. Contact Us: For any questions, requests, or concerns regarding your employment-related data and privacy.

13. IT, Social Media, and Communications Systems Policy

1. We value the importance of information technology (IT), social media, and communications systems in enhancing our operations and maintaining our reputation. This policy sets forth the guidelines and best practices for the responsible and secure use of these systems by employees, contractors, and authorized users.

2. IT Usage:

2.1. Equipment Use:

- All IT equipment, including computers, tablets, and mobile devices, provided by the company is for business purposes only. Personal use should be limited to break times and should not interfere with work responsibilities.

2.2. Software and Applications:

- Employees are expected to use company-authorized software and applications for their designated purposes. Unauthorized installation or use of software is prohibited.

2.3. Data Security:

- Protect sensitive and confidential data by adhering to our data security policy. Do not share passwords or access credentials.

2.4. Reporting Issues:

- Report any IT equipment malfunctions or security concerns to your Front of House Manager

3. Social Media Usage:

3.1. Professional Conduct:

- When using social media for business-related purposes, maintain a professional tone and uphold the company's values.

3.2. Personal Use:

- Employees are permitted to use social media for personal purposes during non-working hours. However, avoid engaging in activities that may harm the company's reputation.

3.3. Confidentiality:

- Do not share confidential or proprietary company information on social media platforms.

3.4. Respect for Others:

- Show respect and consideration for colleagues, customers, and competitors when using social media. Avoid engaging in offensive or discriminatory behavior.

4. Communications Systems:

4.1. Email Usage:

- Use company-provided email accounts for business communication. Exercise caution when opening emails from unknown sources to prevent malware or phishing attacks.

4.2. Phone and Messaging Systems:

- Use company-provided phone and messaging systems for work-related communication. Keep personal phone use to break times..

4.3. Voicemail and Out-of-Office:

- Ensure that voicemail greetings and out-of-office notifications are professional and provide alternative contacts for urgent matters.

4.4. Communication Records:

- Company communication records, including emails and messages, may be monitored for quality assurance, security, and compliance purposes.

5. Compliance and Consequences:

5.1. Policy Compliance:

- All employees and authorized users are expected to comply with this policy. Violations may result in disciplinary action, up to and including termination of employment.

5.2. Reporting Violations:

- Report any violations of this policy to the Front of House Manager

5.3. Amendments to the Policy:

- The company reserves the right to amend this policy as needed. All employees will be notified of any policy updates.

By adhering to this IT, Social Media, and Communications Systems Policy, we contribute to maintaining a secure and professional environment at The Warren. Your cooperation is essential in upholding our commitment to excellence.

14. Data Security

1. We are committed to safeguarding the security and confidentiality of all data, including customer information, employee records, and business-related data. This policy outlines our approach to data security to protect sensitive information from unauthorized access, disclosure, alteration, or destruction.

2. Data Classification:

2.1. Confidentiality Levels:

- Data will be classified into levels of confidentiality: Public, Internal, Confidential, and Highly Confidential.

2.2. Data Owner:

- Each data category will have a designated data owner responsible for its security and management.

3. Access Control:

3.1. User Access:

- Access to data and information systems will be restricted to authorized personnel only.

3.2. Password Security:

- Passwords must be strong and unique. They should be changed regularly, and password sharing is strictly prohibited.

3.3. User Roles:

- User access privileges will be based on their roles and responsibilities. Employees will only have access to the data required for their job functions.

3.4. Termination Procedures:

- Access to data and information systems will be promptly revoked for employees who leave the company or change roles.

4. Data Handling:

4.1. Encryption:

- Sensitive data, especially customer payment information, will be encrypted during storage and transmission.

4.2. Data Backup:

- Regular data backups will be performed to prevent data loss in case of system failures or security breaches.

4.3. Data Retention:

- Data will be retained only for as long as necessary for legal, regulatory, or business requirements.

4.4. Disposal:

- Data that is no longer needed will be securely destroyed to prevent unauthorized access.

5. Security Measures:

5.1. Antivirus Software:

- All computers and devices will have up-to-date antivirus software installed and regularly updated.

5.2. Firewall:

- A firewall will be in place to protect the network from unauthorized access.

5.3. Security Updates:

- Regular security updates and patches will be applied to software and systems to address vulnerabilities.

6. Incident Response:

6.1. Reporting Incidents:

- All employees are required to report any security incidents or data breaches immediately to the designated authority.

6.2. Investigation and Response:

- The company will promptly investigate and respond to security incidents, taking necessary actions to mitigate and prevent further damage.

7. Compliance:

7.1. Legal and Regulatory Compliance:

- The company will adhere to all applicable data protection laws and regulations, including the General Data Protection Regulation (GDPR).

8. Responsibility:

- All employees, contractors, and authorized users share responsibility for maintaining data security.

Consequences of Non-Compliance: Non-compliance with this policy may result in corrective action, including verbal warnings, written warnings, or, in severe cases, suspension or termination of employment.