

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

1. Privacy Policy

Privacy Policy

The Corner Bakery

1. Introduction and Data Controller

This Privacy Policy explains how The Corner Bakery collects, uses, stores, and protects your personal data. We are committed to handling your information responsibly and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025, the provisions of which came into effect in February 2026.

The data controller for The Corner Bakery is Sarah Johnson, trading as The Corner Bakery, 12 High Street, Manchester, M1 2AB. If you have any questions about how we use your personal data, please contact us at the address above or by visiting us in person at our premises.

This policy is effective from 31 May 2026 and applies to customers, website visitors, suppliers, and employees.

2. What Personal Data We Collect

Depending on how you interact with us, we may collect and process the following categories of personal data:

- Contact details: your name, email address, and phone number, which you may provide when placing an order, signing up for updates, or making an enquiry through our website or in person.
- Payment information: when you pay by card, your payment is processed securely by our card payment provider. We do not store your full card details on our own systems.
- CCTV footage: our premises at 12 High Street are monitored by closed-circuit television (CCTV) for the purposes of security and crime prevention. Images of individuals on or near our premises may be captured.
- Website usage data: if you visit our website, we may collect technical data such as your IP address, browser type, and pages visited, typically via cookies or similar technologies.
- Employee records: for our members of staff, we collect information necessary for employment purposes, including contact details, bank account information, National Insurance numbers, emergency contacts, and records of hours worked.

3. How and Why We Use Your Personal Data

We use your personal data only for legitimate purposes and where we have a lawful basis to do so under UK GDPR. Our purposes and corresponding legal bases are as follows:

- Processing orders and taking payment: this is necessary for the performance of a contract with you (Article 6(1)(b) UK GDPR).
- Contacting you about your order or enquiry: where you have provided your email address or phone number, we will use these to communicate with you regarding your order. This is based on contract performance or our legitimate interests.
- Marketing communications: if you have given us your email address or phone number and opted in to receive updates, we may send you information about new products, promotions, or seasonal offers. This is based on your consent, which you may withdraw at any time.
- CCTV monitoring: operated on the basis of our legitimate interests in protecting the safety and security of our staff, customers, and premises, and for the prevention and detection of crime.
- Employing and managing staff: processing employee personal data is necessary for compliance with our legal obligations as an employer and for the performance of employment contracts.
- Improving our website: we use technical data to understand how visitors use our website and to maintain its functionality, based on our legitimate interests.

4. CCTV and Surveillance

The Corner Bakery operates CCTV cameras at our premises at 12 High Street, Manchester. Signage is displayed at the entrance to the premises to notify individuals that CCTV is in operation.

CCTV recordings are retained for a maximum of 30 days, after which they are securely overwritten unless required for an ongoing incident, complaint, or legal matter. Access to CCTV footage is restricted to Sarah Johnson and, where necessary, authorised third parties such as the police or relevant authorities. We will only share footage with third parties where we are legally required to do so or where it is necessary to protect the vital interests of individuals.

5. Card Payments and Financial Data

When you pay for goods or services using a debit or credit card, your payment details are processed by our third-party card payment provider. This processing is carried out in accordance with Payment Card Industry Data Security Standards (PCI DSS). The Corner Bakery does not retain, store, or have access to your full card number, expiry date, or CVV code. If you have any concerns about the security of a card transaction, please speak to a member of staff or contact your card provider directly.

6. Use of Personal Devices (BYOD)

Members of staff at The Corner Bakery may, from time to time, use their personal devices such as mobile phones for work-related purposes, including communicating with customers or accessing business systems. Where personal devices are used for work purposes, staff are required to handle any customer or business data in line with this Privacy Policy and our internal data handling guidance. Personal data accessed or processed on personal devices must not be stored beyond what is necessary and must be protected by appropriate security measures such as screen locks and up-to-date software. Staff are reminded that they must not share customer or employee data through personal applications or unofficial channels.

7. Data Sharing and Third Parties

We do not sell your personal data to any third party. We may share your data in the following limited circumstances:

- Card payment processors: to securely process your transactions.
- Website hosting and analytics providers: to support the operation of our website.
- Accounting or payroll software providers: for the management of employee and financial records.
- Legal and regulatory authorities: where we are required by law to disclose information, for example to HMRC or the police.

Where we engage third-party processors, we ensure appropriate data processing agreements are in place to protect your information. We do not transfer your personal data outside the United Kingdom unless adequate safeguards are in place in accordance with UK GDPR requirements.

8. How Long We Keep Your Data

We retain personal data only for as long as is necessary for the purpose for which it was collected, or as required by law. Our general retention periods are as follows:

- Customer contact details and order information: up to 2 years from the date of your last interaction with us, unless you request earlier deletion.
- Marketing contact lists: until you withdraw your consent or request removal.
- CCTV footage: up to 30 days, unless retained for a specific ongoing matter.
- Card payment records: as required by our payment provider and applicable financial regulations, typically 6 years.
- Employee records: for the duration of employment and for up to 6 years thereafter, in line with legal and HMRC requirements.

When data is no longer required, it is securely deleted or anonymised.

9. Your Rights

Under UK GDPR and the Data (Use and Access) Act 2025, you have the following rights regarding your personal data:

- Right of access: you may request a copy of the personal data we hold about you.
- Right to rectification: you may ask us to correct inaccurate or incomplete data.
- Right to erasure: in certain circumstances, you may request that we delete your personal data.
- Right to restrict processing: you may ask us to limit how we use your data in specific situations.
- Right to data portability: where processing is based on consent or contract, you may request your data in a structured, commonly used format.
- Right to object: you may object to processing based on our legitimate interests, including direct marketing.
- Rights related to automated decision-making: we do not make solely automated decisions that significantly affect you.

To exercise any of these rights, please contact Sarah Johnson at 12 High Street, Manchester, M1 2AB. We will respond to your request within one calendar month. There is no charge for making a request in most circumstances.

10. Data Security

We take the security of your personal data seriously and have implemented appropriate technical and organisational measures to protect it against unauthorised access, loss, or disclosure. These measures include restricting access to personal data to those staff members who need it to carry out their role, using secure and up-to-date devices and software, ensuring card payments are handled through PCI DSS-compliant systems, and providing staff guidance on data handling, including where personal devices are used for work purposes.

In the event of a data breach that is likely to result in a risk to your rights and freedoms, we will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, and we will inform affected individuals without undue delay where required.

11. Complaints and the ICO

If you are unhappy with how we have handled your personal data, we encourage you to contact Sarah Johnson in the first instance so that we can try to resolve the matter for you. You also have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK's independent supervisory authority for data protection matters.

ICO contact details:

Website: www.ico.org.uk

Helpline: 0303 123 1113

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

This Privacy Policy was last reviewed and updated on 31 May 2026. We may update it from time to time to reflect changes in our practices or legal requirements. The current version will always be available on our website and displayed in our premises upon request.

Generated by Comply Sorted | complysorted.co.uk

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

- 1. Data Protection Policy

Data Protection Policy

The Corner Bakery

1. Introduction and Purpose

This Data Protection Policy sets out how The Corner Bakery, located at 12 High Street, Manchester, M1 2AB, collects, uses, stores, and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025, the provisions of which came into effect in February 2026. Sarah Johnson is the owner and Data Controller for The Corner Bakery and is responsible for ensuring this business meets its legal obligations. This policy applies to all staff members, whether full-time, part-time, or casual, and covers all personal data processed in connection with our bakery, café, and takeaway operations. We are committed to handling personal data fairly, lawfully, and transparently, and to protecting the privacy of our customers, employees, and suppliers.

2. What Personal Data We Collect

As a restaurant, takeaway, and café business, The Corner Bakery collects and processes the following categories of personal data. Customer data: names, email addresses, and telephone numbers collected when customers place orders, sign up for our mailing list, make enquiries via our website, or participate in any loyalty or promotional activities. Payment data: card payment information processed through our card payment terminal; we do not store full card details ourselves, as these are handled securely by our payment processor. CCTV footage: images captured by our closed-circuit television system on the premises at 12 High Street, which records individuals entering and within the business for the purposes of security and crime prevention. Employee records: names, addresses, contact details, National Insurance numbers, bank account details for payroll, emergency contact information, employment contracts, and records of hours worked, holidays, and any disciplinary matters. Website data: basic usage data and any personal details submitted through contact or ordering forms on our website.

3. Lawful Basis for Processing

The Corner Bakery relies on the following lawful bases to process personal data, as required under UK GDPR Article 6. Contract: processing employee records and customer order information is necessary to fulfil our contractual obligations. Legitimate interests: operating our CCTV system is based on our legitimate interest in maintaining the security of our premises, staff, and customers; we have assessed that this interest is not overridden by the rights of those recorded. Consent: where customers voluntarily

provide their email address or phone number to receive marketing communications, promotional offers, or updates about The Corner Bakery, we rely on freely given, informed consent. Legal obligation: we process certain employee and financial data to comply with HMRC requirements, employment law, and other statutory obligations. We do not process any special category data as part of our normal business operations. If this changes, this policy will be updated accordingly.

4. How We Use Personal Data

Customer email addresses and telephone numbers are used to confirm orders, respond to enquiries, send promotional communications where consent has been given, and manage customer relationships. Customers may withdraw consent to marketing communications at any time by contacting Sarah Johnson at the address above or by using the unsubscribe option in any email we send. Card payment data is used solely to process transactions at our till point; our payment provider is responsible for secure card data handling and we do not retain sensitive card details. CCTV footage is reviewed only when there is a specific security concern, such as suspected theft or an incident on the premises, and is not used for any other purpose. Employee records are used to manage payroll, holidays, and employment matters, and to meet our obligations as an employer under UK law. Our website may collect basic contact and order information, which is used only to respond to enquiries and fulfil requests.

5. Data Storage, Security, and BYOD

The Corner Bakery takes appropriate technical and organisational measures to keep personal data secure. Physical records, such as paper employee files and printed order records, are kept in a locked filing cabinet on the premises and accessed only by Sarah Johnson or authorised staff. Digital data, including customer contact details and employee records, is stored on password-protected devices and, where applicable, in secure cloud-based services. As our staff use personal devices (Bring Your Own Device — BYOD) for work-related tasks, all staff are required to use strong, unique passwords on any device used for work purposes, enable screen locks, avoid storing business data on personal apps or unsecured platforms, and report any lost or stolen device to Sarah Johnson immediately. Staff must not share customer or employee data through personal messaging applications unless absolutely necessary and only via secure, encrypted means. CCTV footage is stored securely on a dedicated recorder with restricted access and is retained for no longer than 31 days unless required for an ongoing investigation. Card payment processing is conducted through a reputable, PCI DSS-compliant payment provider.

6. Data Retention

We retain personal data only for as long as is necessary for the purposes for which it was collected, or as required by law. Customer contact details used for marketing are retained until consent is withdrawn, after which they are securely deleted. Customer

order records are retained for up to 12 months for operational and accounting purposes. CCTV footage is retained for a maximum of 31 days and then automatically overwritten unless preserved for a specific incident. Employee records are retained for the duration of employment and for six years following the end of employment, in line with HMRC and employment law requirements. Payroll and financial records are retained for a minimum of six years as required by HMRC. At the end of the relevant retention period, personal data is securely deleted from digital systems and paper records are shredded.

7. Sharing Personal Data with Third Parties

The Corner Bakery does not sell or share personal data with third parties for their own marketing purposes. We may share data with the following trusted third parties where necessary: our card payment processor, to handle card transactions securely; our payroll provider or accountant, to manage employee wages and tax obligations; our website hosting provider, for the secure operation of our website; and law enforcement or regulatory authorities, if required by law. Any third parties with whom we share data are required to handle it securely and in accordance with UK GDPR. Where we engage a third party to process data on our behalf, we ensure an appropriate data processing agreement is in place.

8. Your Rights as a Data Subject

Under UK GDPR and the Data (Use and Access) Act 2025, individuals whose data we process have the following rights: the right to be informed about how their data is used; the right of access to a copy of their personal data (subject access request); the right to rectification of inaccurate or incomplete data; the right to erasure ('right to be forgotten') where data is no longer necessary; the right to restrict processing in certain circumstances; the right to data portability where processing is based on consent or contract; the right to object to processing based on legitimate interests or for direct marketing; and rights in relation to automated decision-making and profiling. To exercise any of these rights, individuals should contact Sarah Johnson in writing at The Corner Bakery, 12 High Street, Manchester, M1 2AB, or by email where a business email address has been provided. We will respond to all valid requests within one calendar month. There is no charge for exercising these rights in most circumstances.

9. CCTV and Privacy Notice

The Corner Bakery operates a CCTV system on the premises at 12 High Street, Manchester, for the purpose of security, crime prevention, and the safety of staff and customers. Signage is displayed at the entrance to the premises to inform individuals that CCTV is in operation, in accordance with the Information Commissioner's Office (ICO) CCTV Code of Practice. The CCTV system is operated and managed by Sarah Johnson. Footage is retained for a maximum of 31 days. Access to recorded footage is strictly limited to Sarah Johnson and, where required, authorised law enforcement

agencies. Individuals recorded on CCTV may request access to footage in which they appear by contacting Sarah Johnson directly.

10. Data Breaches

A personal data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All staff must report any suspected or actual data breach to Sarah Johnson immediately. Sarah Johnson will assess the breach and, where it is likely to result in a risk to the rights and freedoms of individuals, will report it to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it, in accordance with UK GDPR Article 33. Where a breach is likely to result in a high risk to individuals, affected persons will also be notified without undue delay. A record of all data breaches, whether reported to the ICO or not, will be maintained by Sarah Johnson. This includes breaches involving personal devices used for work purposes under our BYOD arrangement.

11. Staff Responsibilities and Training

All staff at The Corner Bakery are responsible for handling personal data in accordance with this policy. Sarah Johnson, as Data Controller, is responsible for ensuring this policy is implemented, reviewed, and updated as required. Staff must keep customer and employee data confidential, use strong passwords on any personal device used for work, report any data breach or security concern immediately, and not share personal data with unauthorised individuals. New staff will receive data protection guidance as part of their induction. This policy will be reviewed at least annually, or sooner if there are changes to our business operations, the law, or guidance from the ICO. The Data (Use and Access) Act 2025 changes, effective February 2026, have been incorporated into this policy and will continue to be monitored for further regulatory developments.

12. Policy Review and Contact Details

This Data Protection Policy was last reviewed and adopted on 31 May 2026. It will be reviewed annually or whenever significant changes to the law, ICO guidance, or our business operations require an update. If you have any questions about this policy, wish to exercise your data rights, or wish to raise a data protection concern, please contact: Sarah Johnson, Data Controller, The Corner Bakery, 12 High Street, Manchester, M1 2AB. If you are not satisfied with our response, you have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK's independent data protection authority, at www.ico.org.uk or by telephone on 0303 123 1113.

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

1. Data Retention Policy

Data Retention Policy

The Corner Bakery

1. Introduction and Purpose

This Data Retention Policy applies to The Corner Bakery, located at 12 High Street, Manchester, M1 2AB. The data controller is Sarah Johnson, the owner of the business. This policy sets out how long we keep personal data, why we keep it, and how we securely dispose of it when it is no longer needed. It applies to all personal data held by the business, whether stored digitally on personal devices, in cloud-based systems, or in paper format. This policy has been written in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025, the provisions of which became effective in February 2026. All staff members at The Corner Bakery are required to follow this policy.

2. Scope

This policy covers all personal data processed by The Corner Bakery in the course of running our restaurant, takeaway, and café business. This includes personal data relating to customers, employees, suppliers, and website visitors. Data may be held in a variety of formats including email inboxes, paper records, card payment systems, CCTV footage, and business applications accessed on personal devices used by staff. As The Corner Bakery operates a Bring Your Own Device (BYOD) arrangement, this policy also applies to any personal data relating to the business that is stored or accessed on staff members' personal phones, tablets, or computers. Sarah Johnson, as data controller, is responsible for ensuring this policy is implemented and reviewed regularly.

3. Principles of Data Retention

The Corner Bakery is committed to retaining personal data only for as long as is necessary to fulfil the purpose for which it was collected. We will not keep data longer than is required by law or legitimate business need. Where data is no longer required, it will be securely deleted or destroyed. These principles are consistent with the UK GDPR storage limitation principle, which requires that personal data is kept in a form that permits identification of individuals for no longer than is necessary. The Data (Use and Access) Act 2025 further reinforces the importance of responsible data management, and we have reviewed our retention schedules accordingly to ensure ongoing compliance from February 2026.

4. Customer Data

The Corner Bakery collects customer email addresses and phone numbers for purposes such as order confirmations, marketing communications, and loyalty or promotional activity. Where a customer has provided consent to receive marketing emails or messages, their contact details will be retained for as long as they remain an active subscriber or until they withdraw consent, whichever comes first. If a customer unsubscribes or requests removal, their data will be deleted within 30 days. General customer contact data collected in connection with orders or enquiries will be retained for a period of 2 years from the date of last contact, after which it will be securely deleted. Customer data collected through our website, including any enquiry forms or online ordering data, will follow the same retention period unless a shorter period is appropriate.

5. Card Payment Data

The Corner Bakery takes card payments from customers. We do not store full card details ourselves; card payments are processed through a third-party payment provider. Transaction records, including the amount, date, and a reference number, are retained for 7 years in line with HM Revenue and Customs (HMRC) requirements for financial and accounting records. Any payment data held by our card payment provider is subject to their own data retention and Payment Card Industry Data Security Standard (PCI DSS) obligations. Staff should never write down or store customer card details on paper or on personal devices.

6. CCTV Data

The Corner Bakery operates a CCTV system at our premises at 12 High Street, Manchester. CCTV footage is recorded for the purposes of crime prevention, staff and customer safety, and the protection of business property. In standard circumstances, CCTV footage will be retained for a maximum of 31 days, after which it will be automatically overwritten or manually deleted. Where footage is required in connection with a specific incident, such as a theft, accident, or formal complaint, relevant footage will be preserved for as long as necessary to resolve the matter, which may include the duration of any insurance claim, police investigation, or legal proceedings. Access to CCTV footage is restricted to Sarah Johnson and, where necessary, authorised third parties such as the police. A CCTV notice is displayed at our premises to inform individuals that recording is taking place.

7. Employee Records

The Corner Bakery retains personnel records for all current and former employees. During employment, we keep records including contact details, right to work documentation, contracts of employment, payroll information, absence records, and any disciplinary or performance records. Following the end of employment, records will

be retained for the following periods: payroll and tax records for 7 years (as required by HMRC); right to work documents for 2 years after the end of employment; and general HR records, including contracts and correspondence, for 6 years after termination to cover any potential employment tribunal claims under the Limitation Act 1980. Disciplinary records will be held for no longer than 6 years unless there are exceptional circumstances. Records will be securely deleted or shredded at the end of the relevant retention period.

8. Website and Digital Data

The Corner Bakery's website may collect personal data through contact forms, newsletter sign-ups, or online ordering functions. Any personal data submitted via the website will be processed in accordance with our Privacy Notice, which is published on the website. Website analytics data, where collected, will be anonymised or pseudonymised wherever possible and retained for no longer than 26 months. If the website uses cookies that process personal data, retention periods for cookie data are set out in the website's Cookie Policy. As staff may access website administration on personal devices under our BYOD arrangement, Sarah Johnson will ensure that appropriate access controls and security measures are in place.

9. Personal Devices (BYOD)

Where staff at The Corner Bakery use personal devices to access or process business data, including customer emails, order information, or staff communications, they are required to follow this policy and our associated BYOD guidelines. Business-related personal data must not be stored locally on personal devices beyond what is necessary for immediate operational use. Staff must ensure that any business data on personal devices is deleted promptly when no longer needed, and immediately upon leaving employment. In the event of a data breach involving a personal device, the member of staff must notify Sarah Johnson without undue delay. Sarah Johnson, as data controller, retains the right to request confirmation that business data has been removed from personal devices upon the end of employment.

10. Retention Schedule Summary

For ease of reference, the following summary sets out the key retention periods applied by The Corner Bakery: Customer contact details (with consent for marketing) — until consent is withdrawn or 2 years from last contact; Online order and enquiry records — 2 years; Financial and card payment transaction records — 7 years; CCTV footage — 31 days (or longer if required for an incident); Employee HR records and contracts — 6 years post-employment; Payroll and tax records — 7 years; Right to work documents — 2 years post-employment; Website enquiry data — 2 years; Website analytics — 26 months. These periods will be reviewed annually by Sarah Johnson to ensure they remain appropriate and compliant with current legislation.

11. Secure Disposal

When personal data has reached the end of its retention period, The Corner Bakery will dispose of it securely. Paper records containing personal data will be cross-cut shredded or disposed of using a confidential waste service. Digital data will be permanently deleted from devices, email accounts, and cloud services. Where personal data is held on personal devices under our BYOD arrangement, staff are responsible for ensuring it is permanently deleted when instructed to do so. Sarah Johnson will maintain a record of data disposal activities where appropriate. The secure disposal of data applies equally to data held by any third-party processor acting on behalf of The Corner Bakery.

12. Review and Responsibility

This Data Retention Policy is effective from 31 May 2026 and will be reviewed at least annually, or sooner if there are significant changes to the business, applicable legislation, or the types of data we process. Sarah Johnson, as data controller, is responsible for maintaining and enforcing this policy and for ensuring all staff understand their obligations. Any questions about this policy or about how The Corner Bakery handles personal data should be directed to Sarah Johnson at the business address above. Individuals whose data we hold have rights under the UK GDPR, including the right to request erasure of their data in certain circumstances. Details of how to exercise these rights are set out in our Privacy Notice.

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

1. Health & Safety Policy

Health & Safety Policy

The Corner Bakery

1. Policy Statement

The Corner Bakery, located at 12 High Street, Manchester, M1 2AB, is committed to providing a safe and healthy working environment for all staff and a safe experience for every customer who visits our premises. This policy has been prepared by Sarah Johnson, owner of The Corner Bakery, and applies to all employees, whether full-time, part-time, or casual. As a small bakery, restaurant, and café business with between two and five members of staff, we recognise that our size does not reduce our legal obligations. We are committed to complying fully with the Health and Safety at Work etc. Act 1974, the Management of Health and Safety at Work Regulations 1999, and all other relevant UK health and safety legislation. This policy is effective from 31 May 2026 and will be reviewed annually or whenever significant changes occur to our operations or staffing.

2. Responsibilities

Sarah Johnson, as owner and manager of The Corner Bakery, holds overall responsibility for health and safety across the business. This includes ensuring that risk assessments are completed and kept up to date, that staff receive appropriate training, that safe working procedures are communicated clearly, and that any incidents or hazards are properly recorded and addressed. All members of staff, regardless of their role, are expected to take reasonable care of their own health and safety and that of others who may be affected by their actions. Staff must follow all health and safety instructions given by Sarah Johnson, report any hazards or accidents promptly, and use any equipment or protective gear provided to them correctly. No member of staff should undertake any task they have not been trained to perform safely.

3. Risk Assessment

The Corner Bakery will carry out and regularly review written risk assessments covering all key areas of our bakery, café, and takeaway operations. Given the nature of our business, this includes risks associated with hot ovens, hobs, fryers, and other cooking equipment; the handling of sharp implements such as knives and slicers; manual handling of heavy trays, sacks of flour, and delivery stock; wet or slippery floors in the kitchen and service areas; hot liquids served to customers; and food preparation surfaces and equipment that require thorough cleaning. Risk assessments will be reviewed at least annually, following any accident or near miss, or whenever new equipment or working practices are introduced. All staff will be made aware of the findings of relevant risk assessments.

4. Food Safety and Hygiene

As a food business, The Corner Bakery places particular importance on food safety and hygiene as a core part of our health and safety commitment. We comply with the Food Safety Act 1990, the Food Hygiene (England) Regulations 2006, and Regulation (EC) No 853/2004 on the hygiene of foodstuffs. All staff involved in food preparation or handling must hold an appropriate food hygiene qualification and must follow our documented food safety management system based on HACCP (Hazard Analysis and Critical Control Points) principles. Handwashing procedures must be followed diligently, and staff must not handle food if they are experiencing symptoms of illness, particularly sickness, diarrhoea, or skin infections. Personal protective equipment, including aprons and hair coverings, must be worn at all times during food preparation. Temperature controls for food storage, cooking, and service will be monitored and recorded daily.

5. Fire Safety

The Corner Bakery will maintain a current fire risk assessment for our premises at 12 High Street in compliance with the Regulatory Reform (Fire Safety) Order 2005. Appropriate fire detection equipment, including smoke alarms, will be installed, tested, and maintained in good working order. A fire extinguisher suitable for kitchen environments will be kept on the premises and inspected annually. All staff will be informed of the fire evacuation procedure for the building, including the location of all fire exits, the designated assembly point, and their individual responsibilities in the event of a fire. Fire exits must be kept clear and unobstructed at all times. Fire safety checks will be recorded, and any concerns will be reported to Sarah Johnson immediately.

6. Equipment Safety and Maintenance

All equipment used at The Corner Bakery, including commercial ovens, coffee machines, display fridges, food processors, and any handheld tools, must be used only by staff who have been properly trained in its safe operation. Equipment must be inspected regularly for signs of wear, damage, or malfunction, and any defective equipment must be taken out of use and reported to Sarah Johnson without delay. Electrical equipment will be subject to regular Portable Appliance Testing (PAT) in line with HSE guidance. Gas appliances, including ovens or hobs, will be serviced annually by a Gas Safe registered engineer. Cleaning and maintenance procedures for all kitchen equipment will be documented and followed consistently to minimise risk.

7. Manual Handling

The Corner Bakery acknowledges that manual handling tasks form a regular part of our daily operations, including lifting and carrying sacks of flour, sugar, and other ingredients, as well as moving deliveries, trays, and catering equipment. We will comply with the Manual Handling Operations Regulations 1992. Where possible,

mechanical aids such as trolleys will be used to reduce the need for heavy lifting. All staff will receive guidance on safe manual handling techniques, including how to assess a load before lifting, correct posture, and when to seek assistance. Staff should never attempt to lift loads that are beyond their capability and should report any pain or discomfort arising from manual handling tasks without hesitation.

8. Personal Protective Equipment (PPE)

Where risk assessments identify a need for personal protective equipment, The Corner Bakery will provide appropriate PPE to all relevant staff free of charge, in accordance with the Personal Protective Equipment at Work Regulations 1992 (as amended in 2022). In our bakery and café environment this may include oven gloves and heat-resistant PPE for handling hot trays and equipment, cut-resistant gloves when using sharp tools, aprons, and non-slip footwear. Staff are required to wear and maintain any PPE provided to them and to report damage or loss to Sarah Johnson so that replacements can be arranged promptly. The provision of PPE does not replace the need to eliminate or reduce risks at source wherever reasonably practicable.

9. Accident Reporting and First Aid

The Corner Bakery maintains an accident book on the premises to record details of all accidents, injuries, near misses, and dangerous occurrences involving staff or customers. All incidents must be recorded promptly and reported to Sarah Johnson. Where an incident meets the criteria set out under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR), it will be reported to the Health and Safety Executive without delay. A fully stocked first aid kit is kept on the premises and checked regularly to ensure contents are within their use-by dates. At least one member of staff on duty at any time will hold a current emergency first aid at work (EFAW) certificate. The location of the first aid kit will be clearly communicated to all staff.

10. Staff Training and Induction

All new members of staff at The Corner Bakery will receive a health and safety induction before beginning work. This induction will cover the location of emergency exits and fire assembly point, the location of the first aid kit and accident book, food hygiene requirements, safe use of kitchen equipment, manual handling guidance, and how to report hazards or accidents. Ongoing training will be provided as required, particularly when new equipment is introduced, when working practices change, or following an accident or near miss. Sarah Johnson will keep a record of all training completed by each member of staff. We are committed to ensuring that every team member has the knowledge and skills they need to work safely and confidently.

11. Policy Review

This Health and Safety Policy for The Corner Bakery has been approved by Sarah Johnson and is effective from 31 May 2026. It will be reviewed at least once per year or sooner in the event of significant changes to the business, its premises, staffing, or applicable legislation. All staff will be informed of any updates to this policy, and the most current version will be kept on the premises and made available to any member of staff on request. Sarah Johnson retains overall responsibility for ensuring this policy remains current, fit for purpose, and properly implemented across all areas of the business.

Generated by Comply Sorted | complysorted.co.uk

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

1. Risk Assessment

Risk Assessment

The Corner Bakery

1. Document Information

Business Name: The Corner Bakery
Owner / Data Controller: Sarah Johnson
Address: 12 High Street, Manchester, M1 2AB
Business Type: Restaurant, Takeaway and Café
Date of Assessment: 31 May 2026
Review Date: 31 May 2027
Prepared By: Sarah Johnson

This Risk Assessment has been prepared in accordance with UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025, which introduced updated provisions effective February 2026. It identifies the key data protection and operational risks facing The Corner Bakery and sets out the measures in place to mitigate those risks.

2. Purpose and Scope

The purpose of this document is to identify, evaluate and manage the risks associated with the processing of personal data and the day-to-day operations of The Corner Bakery. This assessment covers all personal data processed by the business, including customer contact details (email addresses and phone numbers), employee records, card payment data, and footage captured by the CCTV system installed on the premises at 12 High Street, Manchester.

This assessment applies to all staff (between 2 and 5 individuals) and extends to the use of personal devices (BYOD — Bring Your Own Device) where these are used for business purposes. It does not cover third-party processors beyond the references made within individual risk entries.

3. Risk Scoring Methodology

Each risk is assessed using a simple likelihood and impact matrix:

- Likelihood: Low (1), Medium (2), High (3)
- Impact: Low (1), Medium (2), High (3)
- Risk Score = Likelihood × Impact

Scores of 1-2 are classified as LOW risk.

Scores of 3–4 are classified as MEDIUM risk.

Scores of 6–9 are classified as HIGH risk.

All high and medium risks require documented mitigating controls. This methodology aligns with the accountability principle under UK GDPR Article 5(2) and the updated accountability framework introduced by the Data (Use and Access) Act 2025.

4. Identified Risks — Customer Personal Data

Risk 1: Unauthorised access to customer email addresses and phone numbers

The Corner Bakery collects customer emails and phone numbers, likely for order confirmations, marketing or loyalty purposes. If this data is stored insecurely (e.g., on a personal device, in an unprotected spreadsheet, or via an unsecured website contact form), it may be accessed by unauthorised parties.

Likelihood: Medium | Impact: High | Score: 6 — HIGH

Controls: Customer data must be stored in a password-protected system. The business website must use HTTPS encryption. Customers must be informed of how their data is used via a clear Privacy Notice published on the website. Consent for marketing communications must be obtained and recorded in line with UK GDPR Article 6 and PECR.

Risk 2: Excessive retention of customer contact data

Retaining customer data longer than necessary increases exposure in the event of a breach.

Likelihood: Medium | Impact: Medium | Score: 4 — MEDIUM

Controls: Sarah Johnson should define a retention period for customer contact data (recommended: 12 months from last interaction) and delete records when no longer required. This aligns with the storage limitation principle under UK GDPR Article 5(1)(e).

5. Identified Risks — CCTV

Risk 3: Non-compliant use of CCTV on premises

The Corner Bakery operates a CCTV system at 12 High Street. CCTV footage constitutes personal data under UK GDPR. Failure to display adequate signage, retain footage beyond a reasonable period, or respond to subject access requests (SARs) could result in a regulatory breach.

Likelihood: Medium | Impact: High | Score: 6 — HIGH

Controls: Clear CCTV warning signs must be displayed at the entrance to the premises, stating the purpose of recording, the identity of the data controller (Sarah Johnson / The Corner Bakery), and contact details. Footage should be retained for no longer than 31 days unless required for an ongoing investigation. Access to footage must be restricted to Sarah Johnson and authorised staff. A process must be in place to respond to SARs within one calendar month, as required by UK GDPR Article 12. Under the Data (Use

and Access) Act 2025, data subjects have strengthened rights of access, and timely responses are essential.

6. Identified Risks — Card Payments

Risk 4: Payment card data breach

The Corner Bakery accepts card payments, which introduces obligations under the Payment Card Industry Data Security Standard (PCI DSS) as well as UK GDPR where cardholder data may be linked to personal identifiers.

Likelihood: Low | Impact: High | Score: 3 — MEDIUM

Controls: The business must use a PCI DSS-compliant card payment provider and must not store card details manually or digitally. Staff should be trained not to write down card details under any circumstances. The business should ensure its payment terminal provider supplies annual PCI DSS compliance confirmation. Card transaction receipts containing partial card numbers must be disposed of securely by shredding.

7. Identified Risks — Employee Records

Risk 5: Insecure storage of employee personal data

The Corner Bakery holds employee records which may include names, addresses, National Insurance numbers, bank details, employment contracts and payroll information. Insecure storage of this data presents a significant risk of harm to staff.

Likelihood: Medium | Impact: High | Score: 6 — HIGH

Controls: Employee records must be stored securely, whether in a locked physical filing cabinet or an encrypted digital system. Access must be limited to Sarah Johnson only. Records should be retained in line with HMRC guidance (minimum 3 years for payroll; recommended 6 years for contracts). Former employees' records must be securely deleted or destroyed after the applicable retention period.

Risk 6: Unauthorised disclosure of employee data

Sharing employee information with third parties without a lawful basis could constitute a breach under UK GDPR Article 6.

Likelihood: Low | Impact: High | Score: 3 — MEDIUM

Controls: Employee data must only be shared where legally required (e.g., HMRC) or with explicit consent. Staff must be informed of how their data is used via an Employee Privacy Notice.

8. Identified Risks — Personal Devices (BYOD)

Risk 7: Data breach via personal devices used for business purposes

Staff at The Corner Bakery use personal devices for work-related tasks. This creates a risk that business data (including customer contact details, order information or staff communications) may be stored on unmanaged, potentially insecure devices.

Likelihood: High | Impact: High | Score: 9 — HIGH

Controls: Sarah Johnson must implement a BYOD Policy setting minimum security

requirements for personal devices used for work. Requirements should include: screen lock and PIN or biometric authentication; up-to-date operating system and security patches; prohibition on storing customer or employee personal data in personal apps or unencrypted storage. Staff must be informed of these requirements. Business communications should use a dedicated channel (e.g., a separate work email or messaging application) rather than personal accounts. If a device is lost or stolen, Sarah Johnson must be notified immediately so the risk of a personal data breach can be assessed and, if necessary, reported to the ICO within 72 hours under UK GDPR Article 33.

9. Identified Risks – Website

Risk 8: Non-compliant website data collection

The Corner Bakery's website collects personal data (customer emails and phone numbers) and likely uses cookies. Non-compliance with UK GDPR and PECR could result in regulatory action by the ICO.

Likelihood: Medium | Impact: Medium | Score: 4 — MEDIUM

Controls: The website must display a clear and accessible Privacy Policy. If cookies are used beyond strictly necessary functionality, a cookie consent banner must be implemented. Contact forms must include a clear statement of purpose. Under the Data (Use and Access) Act 2025, the legitimate interests basis has been clarified, but explicit consent remains required for direct marketing communications. The website should be reviewed annually for compliance.

10. Data Breach Response

In the event of a suspected or confirmed personal data breach (including loss of a personal device containing customer or employee data, unauthorised access to the website, or inappropriate disclosure of CCTV footage), Sarah Johnson must:

1. Contain the breach as quickly as possible.
2. Assess the likely risk to individuals.
3. If the breach is likely to result in a risk to the rights and freedoms of individuals, report it to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it (UK GDPR Article 33).
4. If the breach is likely to result in a high risk to individuals, notify those affected without undue delay (UK GDPR Article 34).
5. Document all breaches, including those not reported to the ICO, in a breach log.

Given the small size of the business, a proportionate but prompt response process is sufficient. The ICO can be contacted at ico.org.uk or 0303 123 1113.

11. Risk Summary Table

Risk	Likelihood	Impact	Score	Rating
Unauthorised access to customer emails/phone numbers	Medium	High	6	HIGH
Excessive retention of customer contact data	Medium	Medium	4	MEDIUM
Non-compliant CCTV use	Medium	High	6	HIGH
Payment card data breach	Low	High	3	MEDIUM
Insecure storage of employee records	Medium	High	6	HIGH
Unauthorised disclosure of employee data	Low	High	3	MEDIUM
BYOD data breach via personal devices	High	High	9	HIGH
Non-compliant website data collection	Medium	Medium	4	MEDIUM

Four risks are rated HIGH and require priority attention. Sarah Johnson should address these controls as a matter of urgency.

12. Review and Sign-Off

This Risk Assessment must be reviewed at least annually or following any significant change to the business, such as:

- Introduction of new systems or technology
- Changes to the website or payment processing arrangements
- A personal data breach or near-miss incident
- Changes in the number or roles of staff
- Updates to UK data protection legislation or ICO guidance

By maintaining and acting upon this Risk Assessment, The Corner Bakery demonstrates its commitment to the accountability principle under UK GDPR Article 5(2) and the enhanced accountability obligations introduced by the Data (Use and Access) Act 2025.

Signed: Sarah Johnson

Role: Owner and Data Controller

Date: 31 May 2026

Next Review Due: 31 May 2027

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

- 1. Employee Privacy Notice

Employee Privacy Notice

The Corner Bakery

1. Introduction and Data Controller

This Employee Privacy Notice explains how The Corner Bakery collects, uses, stores, and protects personal information about its employees and workers. The Corner Bakery is located at 12 High Street, Manchester, M1 2AB. The data controller responsible for your personal information is Sarah Johnson, owner of The Corner Bakery. This notice applies to all staff, whether employed on a full-time, part-time, casual, or zero-hours basis. We are committed to handling your personal data responsibly and in full compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025, which came into force in February 2026. If you have any questions about how your data is used, please speak directly with Sarah Johnson.

2. What Personal Information We Collect

As a small café and bakery employing between two and five members of staff, we collect and hold only the personal information necessary to manage our employment relationship with you. This includes: your full name, home address, date of birth, and contact details including personal telephone number and email address; your National Insurance number, bank account details for payroll purposes, and tax information provided to HMRC; emergency contact details for a nominated person of your choosing; details of your right to work in the United Kingdom, including copies of identification documents such as your passport or visa; records of your working hours, shift patterns, holiday entitlement, and any absences including sickness absence; any relevant medical information you have chosen to share with us that may affect your ability to work safely in a food preparation and customer-facing environment; and records of any disciplinary or grievance matters, training completed, and performance reviews. We keep these records because they are essential to running a compliant and safe workplace at The Corner Bakery.

3. How and Why We Use Your Information

We use your personal information for the following purposes: to fulfil our legal obligations as your employer, including paying your wages, deducting tax and National Insurance, and meeting our duties under employment law and food safety regulations; to manage day-to-day bakery and café operations, including scheduling shifts and maintaining adequate staffing levels; to maintain accurate records as required by HMRC and other regulatory bodies; to respond appropriately to sickness, absence, or workplace incidents; to process and retain training records relevant to food hygiene,

health and safety, and allergen awareness, which are particularly important given the nature of our business; and to contact your nominated emergency contact if required in an urgent situation. We do not use your personal data for automated decision-making or profiling.

4. Legal Basis for Processing

We rely on the following lawful bases under UK GDPR to process your personal information. The majority of processing is carried out because it is necessary to perform your contract of employment, or to take steps before entering into that contract. We also process data to comply with our legal obligations, for example, payroll reporting to HMRC and maintaining right-to-work records. Where we process special category data, such as health information relevant to food safety or workplace adjustments, we rely on the legal obligation and employment law basis under Article 9(2)(b) UK GDPR. In limited circumstances, for example where you have volunteered information about a health condition to help us support you, we may rely on your explicit consent, which you are always free to withdraw. Under the Data (Use and Access) Act 2025, we are committed to transparency about our data practices and your right to understand how decisions about your data are made.

5. CCTV at The Corner Bakery

The Corner Bakery operates a CCTV system at our premises at 12 High Street, Manchester. CCTV is used to protect the safety and security of our staff, customers, and premises, and to help prevent and detect crime. As a staff member, you may appear in CCTV footage during your working hours. CCTV recordings are retained for a limited period, typically no longer than 31 days, unless footage is required in connection with an incident, investigation, or legal matter. Access to CCTV footage is restricted to Sarah Johnson and, where necessary, relevant authorities such as the police. We have appropriate signage in place to notify customers and visitors that CCTV is in operation. Our lawful basis for CCTV processing is our legitimate interests in maintaining a secure working environment, balanced against your right to privacy.

6. Use of Personal Devices (BYOD)

At The Corner Bakery, staff may use their own personal devices, such as mobile phones, to carry out certain work-related tasks, for example accessing rotas, messaging regarding shift changes, or using work-related applications. Where you use your personal device for work purposes, please be aware that any business-related data accessed or stored on your device, including customer or colleague information, must be handled securely. You must not store customer or staff personal data on personal devices beyond what is necessary, and you must ensure your device is protected with a PIN, password, or biometric lock. If your personal device is lost, stolen, or compromised, you must inform Sarah Johnson immediately. We will not access your

personal device without your consent, and we only request access to business-related data in exceptional circumstances.

7. Card Payments and Financial Data

The Corner Bakery takes card payments from customers using a card payment terminal. Staff involved in processing card transactions may handle payment devices and customer payment information in the course of their duties. We do not retain customer card details ourselves; all card transactions are processed securely by our payment provider in accordance with Payment Card Industry Data Security Standards (PCI DSS). Staff should never record, photograph, or retain any customer payment card information and must report any suspected data breach or security concern to Sarah Johnson without delay.

8. Sharing Your Personal Information

We share your personal information only where necessary and with appropriate safeguards in place. Recipients may include: HMRC and other government bodies for tax, National Insurance, and statutory reporting purposes; our payroll provider, who acts as a data processor on our behalf under a written agreement; our bank, for the purpose of paying your wages; our employers' liability insurer, where required; and legal or regulatory authorities if we are required to disclose information by law. We do not sell your personal data and we do not share it with third parties for marketing purposes. Any third parties with whom we share your data are required to handle it securely and in accordance with UK data protection law.

9. How Long We Keep Your Records

We retain employee records for as long as necessary to fulfil the purposes set out in this notice and to comply with our legal obligations. As a general guide, we keep payroll and tax records for a minimum of six years following the end of the tax year to which they relate, in line with HMRC requirements. Right-to-work documents are retained for two years after the end of employment. Health and safety records and accident reports are kept for a minimum of three years. Disciplinary and grievance records are typically retained for one to two years after the matter is resolved, depending on the outcome. CCTV footage is retained for up to 31 days unless required for longer in connection with an investigation. Once retention periods expire, records are securely deleted or destroyed.

10. Your Rights

Under UK GDPR and the Data (Use and Access) Act 2025, you have the following rights regarding your personal data: the right to access a copy of the personal information we hold about you (a Subject Access Request); the right to request correction of inaccurate or incomplete data; the right to request erasure of your data in certain circumstances;

the right to object to processing based on legitimate interests; the right to restrict processing in certain situations; and the right to data portability where processing is based on consent or contract. To exercise any of these rights, please contact Sarah Johnson at The Corner Bakery, 12 High Street, Manchester, M1 2AB. We will respond within one calendar month. If you are unhappy with how we have handled your data, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk or by calling 0303 123 1113.

11. Data Security

We take the security of your personal information seriously. Physical employee records are stored securely and accessible only to Sarah Johnson. Digital records are password-protected, and access is restricted to authorised individuals. Staff are expected to follow good data security practices, including keeping work-related information confidential, not sharing login credentials, and promptly reporting any suspected data breaches or security incidents. In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the ICO within 72 hours and inform affected individuals without undue delay, in accordance with our obligations under UK GDPR.

12. Updates to This Notice

This Employee Privacy Notice was last reviewed and updated on 31 May 2026. We may update this notice from time to time to reflect changes in our business practices or in data protection law. Where we make significant changes, we will bring these to your attention directly. The current version of this notice will always be made available to you on request from Sarah Johnson. We encourage you to read this notice carefully and to raise any questions or concerns with Sarah Johnson at any time.

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

- 1. Cookie Policy

Cookie Policy

The Corner Bakery

1. Purpose and Who This Policy Applies To

This Cookie Policy explains how The Corner Bakery, owned and operated by Sarah Johnson of 12 High Street, Manchester, M1 2AB, uses cookies and similar tracking technologies on our website. Sarah Johnson is the Data Controller responsible for your personal data. This policy applies to all visitors to our website and is intended to help you understand what cookies we use, why we use them, and how you can control them. This policy should be read alongside our Privacy Notice. It has been prepared in accordance with the Privacy and Electronic Communications Regulations 2003 (PECR), UK GDPR Article 6, the Data Protection Act 2018, and the Data (Use and Access) Act 2025, the provisions of which came into effect in February 2026. This policy is effective from 31 May 2026.

2. What Are Cookies?

Cookies are small text files that are placed on your device — such as your computer, tablet, or smartphone — when you visit a website. They are widely used to make websites work properly, function more efficiently, and to provide information to the website owner. Cookies do not contain viruses or harmful software. Some cookies are deleted when you close your browser (known as session cookies), while others remain on your device for a set period of time or until you delete them manually (known as persistent cookies). Cookies may be set by the website you are visiting (first-party cookies) or by third-party services that the website uses, such as analytics providers or payment processors.

3. Types of Cookies We Use

We use the following categories of cookies on The Corner Bakery website:

Strictly Necessary Cookies: These cookies are essential for our website to function correctly and cannot be switched off. They include cookies that manage your session as you navigate the site, maintain security through CSRF (Cross-Site Request Forgery) tokens, and remember items if we operate an online ordering function. These cookies do not collect any personally identifiable information and do not require your consent under PECR.

Analytics Cookies: We use Google Analytics to help us understand how visitors interact with our website, including which pages are visited most often and how users navigate through the site. Google Analytics sets cookies including `_ga`, `_gid`, and `_gat`. This data

is aggregated and anonymised wherever possible. These cookies help us improve the experience for our customers. Your consent is required before these cookies are placed on your device.

Functional Cookies: These cookies allow our website to remember choices you make, such as your preferred language or region, and to provide enhanced, more personalised features. For example, they may remember whether you have previously dismissed a notice or set a display preference. These cookies require your consent.

Marketing and Advertising Cookies: We may use the Meta Pixel (Facebook) and Google Ads conversion tracking to measure the effectiveness of any promotional activity we run online to promote The Corner Bakery. These cookies track your activity across websites and may be used to show you relevant adverts on social media platforms or search engines. These cookies require your explicit consent before being activated and are only placed if you opt in via our cookie banner.

4. Legal Basis for Using Cookies

Under the Privacy and Electronic Communications Regulations 2003 (PECR), we are required to obtain your prior informed consent before placing any non-essential cookies on your device. Strictly necessary cookies are exempt from this requirement as they are essential to delivering the service you have requested. For all other cookies — including analytics, functional, and marketing cookies — we rely on your freely given, specific, informed, and unambiguous consent as the legal basis under UK GDPR Article 6(1)(a). Where cookies process personal data, this processing is carried out in compliance with UK GDPR and the Data Protection Act 2018. You have the right to withdraw your consent at any time. The Data (Use and Access) Act 2025, effective February 2026, reinforces transparent and accountable data practices, and we are committed to meeting those standards.

5. How to Manage and Reject Cookies

When you first visit our website, you will be presented with a cookie consent banner that allows you to accept or decline non-essential cookies. You can update your preferences at any time by clicking the 'Cookie Settings' link in the footer of our website.

You can also control and delete cookies through your browser settings:

Google Chrome: Go to Settings > Privacy and Security > Cookies and other site data.

Mozilla Firefox: Go to Options > Privacy and Security > Cookies and Site Data.

Safari: Go to Preferences > Privacy > Manage Website Data.

Microsoft Edge: Go to Settings > Cookies and site permissions > Manage and delete cookies.

Please be aware that if you disable or reject certain cookies, some parts of our website may not function as intended. Withdrawing your consent will not affect the lawfulness of any processing carried out before you withdrew it.

6. Third-Party Cookies

Some cookies on our website are set by third-party services that we use. These third parties have their own privacy policies, which we encourage you to review. The relevant third parties and their policies are as follows:

Google Analytics (Alphabet Inc.): Used to collect anonymised usage statistics about how visitors use our website. Privacy policy: <https://policies.google.com/privacy>

Meta Pixel (Meta Platforms, Inc.): Used to measure the effectiveness of our advertising on Facebook and Instagram. Privacy policy: <https://www.facebook.com/policy.php>

Google Ads (Alphabet Inc.): Used for conversion tracking linked to any paid advertising campaigns we run. Privacy policy: <https://policies.google.com/privacy>

Payment Processor: If you make payments through our website, our card payment provider may set cookies to ensure secure transaction processing. Please refer to your payment provider's documentation for further details.

We do not control the cookies set by these third parties and are not responsible for their content or privacy practices.

7. Cookie Retention Periods

The table below sets out the specific cookies we use, along with their provider, purpose, and how long they remain on your device:

Cookie Name: `_ga` | Provider: Google Analytics | Purpose: Distinguishes unique users and sessions for website analytics | Duration: 2 years

Cookie Name: `_gid` | Provider: Google Analytics | Purpose: Distinguishes users across sessions | Duration: 24 hours

Cookie Name: `_gat` | Provider: Google Analytics | Purpose: Throttles request rate to Google Analytics | Duration: 1 minute

Cookie Name: `_fbp` | Provider: Meta (Facebook Pixel) | Purpose: Tracks visits and conversions from Facebook/Instagram ads | Duration: 3 months

Cookie Name: _gcl_au | Provider: Google Ads | Purpose: Conversion tracking for Google Ads campaigns | Duration: 3 months

Cookie Name: CSRF_token | Provider: The Corner Bakery (first-party) | Purpose: Security token to prevent cross-site request forgery | Duration: Session

Cookie Name: session_id | Provider: The Corner Bakery (first-party) | Purpose: Maintains your session as you navigate the website | Duration: Session

Cookie Name: cookie_consent | Provider: The Corner Bakery (first-party) | Purpose: Records your cookie consent preferences | Duration: 12 months

8. Changes to This Policy

We may update this Cookie Policy from time to time to reflect changes in the cookies we use, changes in applicable law, or updates to ICO guidance on cookies and similar technologies. When we make significant changes to this policy, we will update the effective date shown at the top of this document and, where appropriate, notify you via a prominent notice on our website or by email if you have provided us with your email address. We encourage you to review this policy periodically. Continued use of our website following notification of changes will constitute acceptance of those changes, subject to any consent requirements under PECR.

9. Contact Us and Review Date

If you have any questions about how The Corner Bakery uses cookies, or if you wish to exercise any of your rights under UK GDPR, please contact our Data Controller:

Sarah Johnson
The Corner Bakery
12 High Street, Manchester, M1 2AB

If you are not satisfied with our response, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk or by calling 0303 123 1113.

This policy was last reviewed and updated on 31 May 2026. It will next be reviewed no later than 31 May 2027.

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

1. CCTV Policy

CCTV Policy

The Corner Bakery

1. Introduction and Purpose

The Corner Bakery, located at 12 High Street, Manchester, M1 2AB, operates a closed-circuit television (CCTV) system on its premises. This policy explains how and why CCTV is used, how footage is managed, and the rights of individuals whose images may be captured.

CCTV is operated for the following specific and proportionate purposes:

- Prevention and detection of crime, including theft, vandalism, and unauthorised access to the premises.
- Protection of property, including stock, equipment, and cash held on site.
- Health and safety of staff and customers within the café and kitchen environment.
- Staff safety, particularly during opening and closing of the premises.

CCTV is not used for any purpose beyond those listed above. The system is not used to monitor staff performance or to carry out covert surveillance.

2. Legal Basis for Processing

The Corner Bakery processes personal data captured via CCTV under Article 6(1)(f) of the UK General Data Protection Regulation (UK GDPR) — legitimate interests. The legitimate interests pursued are crime prevention, property protection, and the safety of staff and customers.

A Legitimate Interests Assessment (LIA) has been completed by Sarah Johnson, owner and Data Controller, to confirm that the use of CCTV is necessary, proportionate, and that the privacy interests of individuals do not override the legitimate interests of the business. A copy of the LIA is available on request by contacting Sarah Johnson directly.

The Corner Bakery is registered with the Information Commissioner's Office (ICO) as a data controller in accordance with the Data Protection Act 2018. This policy has been prepared with reference to the UK GDPR, the Data Protection Act 2018, the ICO CCTV Code of Practice, the Surveillance Camera Code of Practice 2021, and the Data (Use and Access) Act 2025, the provisions of which take effect from February 2026.

3. Camera Locations and Scope

CCTV cameras are positioned to cover areas relevant to the stated purposes of this policy. At The Corner Bakery, cameras are located at or near the following areas:

- The main entrance and exit of the premises on High Street.
- The customer-facing counter and sales area.
- The kitchen and food preparation area, for health, safety, and security purposes.
- The rear entrance and any external storage or delivery areas.

All camera positions have been carefully considered to ensure they are proportionate and necessary. Cameras are positioned to minimise capture of areas outside the business's own premises where possible.

Cameras are NOT installed in, and footage is NOT captured from, any area where individuals have a reasonable expectation of privacy. This includes staff toilet facilities and any private changing or welfare areas. No camera is directed into a neighbouring property or public highway beyond what is incidental and unavoidable.

4. Signage

Clearly visible CCTV warning signs are displayed at all entry points to The Corner Bakery and at the location of each camera. In accordance with ICO guidance, each sign states:

- That CCTV is in operation on the premises.
- The identity of the operator: The Corner Bakery, 12 High Street, Manchester, M1 2AB.
- The purpose for which CCTV is used: crime prevention, health and safety, and property protection.
- Contact details for data subject enquiries or requests: Sarah Johnson, sarah@thecornerbakery.co.uk (or the business contact details displayed on site).

Signage is reviewed annually to ensure it remains legible, accurate, and compliant with ICO requirements. Any member of the public or staff member who is unsure about the CCTV system is encouraged to speak with Sarah Johnson directly.

5. Recording and Retention of Footage

The CCTV system at The Corner Bakery operates on a continuous recording basis during business hours and, where security requires it, outside of business hours. Footage is stored on a dedicated recording device held securely on the premises.

Footage is retained for a maximum of 30 days from the date of recording. At the end of this period, footage is automatically overwritten unless it has been specifically retained for a legitimate reason (see below).

Footage may be retained beyond 30 days only where there is a documented justification, for example:

- An incident has occurred or been reported and the footage is required as evidence.
- A subject access request has been received in relation to specific footage.
- Law enforcement or legal proceedings require the footage to be preserved.

In such cases, the reason for extended retention must be noted in writing by Sarah Johnson and the footage stored securely until no longer required. Footage will not be retained indefinitely without ongoing justification.

6. Access to CCTV Footage

Access to CCTV footage recorded at The Corner Bakery is strictly limited to:

- Sarah Johnson (owner and Data Controller).
- Any member of staff expressly authorised by Sarah Johnson in writing for a specific and documented purpose.

Given the small size of the business (2-5 staff), access is tightly controlled. A written log is maintained of every occasion on which footage is accessed, recording the date, the name of the person accessing the footage, the reason for access, and the time period of footage reviewed.

No member of staff or other individual is permitted to copy, download, share, or distribute footage without the express written authorisation of Sarah Johnson. Footage must not be shared via personal devices, social media, messaging applications, or any other informal channel.

Third-party access to footage is only permitted through the formal process described in Section 8 of this policy.

7. Subject Access Requests

Any individual who believes they have been captured on CCTV footage at The Corner Bakery has the right to request access to that footage under Article 15 of the UK GDPR.

To submit a subject access request:

1. Submit the request in writing (by letter or email) to Sarah Johnson at the business address or email address displayed on site and on the business website.
2. Provide sufficient proof of identity (for example, a copy of a driving licence or passport).

3. Provide details to assist in locating the relevant footage, including the approximate date, time, and location of the recording.

The Corner Bakery will respond to subject access requests within 30 calendar days of receipt. Where a request relates to footage that also captures other individuals, those individuals' images will be redacted or obscured prior to disclosure in order to protect their privacy rights. In some cases, it may not be possible to provide footage without disclosing third-party images, in which case the request will be considered carefully and a written explanation provided where footage cannot be shared in full.

8. Disclosure to Third Parties

CCTV footage recorded at The Corner Bakery will only be disclosed to third parties in the following circumstances:

- Law enforcement agencies (such as Greater Manchester Police), where they present a valid legal authority, formal request, or court order requiring disclosure.
- Insurance companies, where an incident has occurred on the premises and footage is relevant to an insurance claim made by or against The Corner Bakery.
- Legal advisers or courts, where footage is required in connection with legal proceedings.

In all cases, disclosure will be documented in the access log, noting the recipient, the legal basis for disclosure, the date, and the footage provided.

CCTV footage will never be sold, shared commercially, or disclosed for marketing or entertainment purposes. Footage will not be shared on social media or in any public forum under any circumstances.

9. Data Security

The Corner Bakery takes the security of CCTV footage seriously and has implemented the following measures:

- All recording equipment is protected by a strong, unique password. Login credentials are held only by Sarah Johnson and are not shared with unauthorised individuals.
- Recording hardware is stored in a secure, locked location on the premises and is not accessible to customers or unauthorised personnel.
- Where footage is copied for a legitimate purpose (for example, to provide to the police), copies are transferred securely and not retained beyond their purpose.
- Recording equipment, including any networked components, is reviewed at least annually to identify and address security vulnerabilities, including software updates and firmware patches.
- As staff may use personal devices (BYOD) for some business tasks, it is confirmed

that CCTV footage is not stored on, accessed from, or transferred via personal devices unless in an emergency and with Sarah Johnson's express approval, in which case the footage is deleted from the personal device immediately once transferred securely.

Any suspected breach involving CCTV footage will be assessed promptly and, where required under UK GDPR, reported to the ICO within 72 hours.

10. Complaints Procedure

If any individual has a concern about the way in which CCTV is operated at The Corner Bakery, or about how their personal data has been handled in connection with this policy, they should in the first instance raise the matter with Sarah Johnson:

- In writing at: The Corner Bakery, 12 High Street, Manchester, M1 2AB.
- By email using the contact details displayed on the business website and on-site signage.

Sarah Johnson will acknowledge the complaint within five working days and aim to provide a full response within 30 calendar days.

If an individual is not satisfied with the response received, or wishes to escalate the matter independently, they have the right to lodge a complaint with the Information Commissioner's Office (ICO):

- Website: ico.org.uk
- Telephone: 0303 123 1113
- Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

11. Policy Review

This policy will be reviewed by Sarah Johnson at least annually to ensure it remains accurate, proportionate, and compliant with current legislation and regulatory guidance. The policy will also be reviewed and updated promptly following any significant change, including:

- Installation of additional cameras or relocation of existing cameras.
- A change in the purposes for which CCTV is operated.
- A relevant change in law, ICO guidance, or regulatory requirements.
- A significant incident involving the CCTV system or recorded footage.

The current version of this policy is available to staff and to members of the public on request. The business website may also carry a summary of this policy.

Policy Title: CCTV Policy

Data Controller: Sarah Johnson, The Corner Bakery

Business Address: 12 High Street, Manchester, M1 2AB

Effective Date: 31 May 2026

Next Review Date: 31 May 2027

Generated by Comply Sorted | complysorted.co.uk

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

- 1. Data Breach Response Procedure

Data Breach Response Procedure

The Corner Bakery

1. Purpose and Scope

This Data Breach Response Procedure sets out how The Corner Bakery identifies, manages, and reports personal data breaches in compliance with UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (effective February 2026). It applies to all staff, volunteers, and contractors at our premises at 12 High Street, Manchester, M1 2AB, and covers all systems and processes used to handle personal data. This includes our website, card payment systems, CCTV, customer contact records (emails and phone numbers), and employee records. Because staff use personal devices (BYOD) to carry out work-related tasks, this procedure also applies to any personal device on which business data is accessed or stored. The Data Controller is Sarah Johnson, who acts as the Data Protection Lead for The Corner Bakery.

2. What Is a Personal Data Breach?

A personal data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data. Breaches are not limited to external attacks. Examples relevant to The Corner Bakery include: a member of staff losing a personal mobile phone containing customer contact details or employee records; a customer email list being sent to the wrong recipient; our website or payment system being hacked or subjected to a ransomware attack; card payment data being compromised through our point-of-sale system; CCTV footage being accessed by an unauthorised person or being accidentally deleted; a paper staff rota or job application form being left where customers or unauthorised individuals can see it; a member of staff accessing colleague or customer records without a legitimate reason; and accidental deletion of customer booking or contact information without a backup.

3. Detecting and Reporting a Breach Internally

Any member of staff at The Corner Bakery who discovers or suspects a personal data breach must report it immediately to Sarah Johnson (Data Protection Lead). An internal report must be submitted within 24 hours of discovery and should include: a description of what happened; the date and time the breach was discovered; the type of personal data affected (for example, customer emails, card data, employee payroll records, or CCTV footage); an estimate of how many individuals may be affected; and any steps already taken to limit the damage. Staff must not attempt to investigate a breach independently, take unilateral action to cover it up, or delay reporting in the hope the problem resolves itself. Because staff use personal devices, any suspected

breach involving a personal phone, tablet, or laptop used for work must also be reported to Sarah Johnson without delay, even if the staff member is uncertain whether business data was involved.

4. Assessing Severity

Once a breach is reported, Sarah Johnson will assess the likely risk to affected individuals. The following factors will be considered: the sensitivity of the data involved (financial data such as card payment details, health information, or data relating to children carries higher risk); the volume of records affected; whether any data was encrypted or otherwise protected at the time of the breach; the nature of the breach (deliberate attack versus accidental loss); and whether the breach is reversible. Breaches will be placed into one of three categories. No or Low Risk: the breach is unlikely to result in any risk to individuals' rights and freedoms, for example, encrypted data lost where the decryption key remains secure. No ICO notification is required, but the breach must still be recorded in the breach log. Risk: the breach is likely to result in some risk to individuals' rights and freedoms. Notification to the ICO is required within 72 hours. High Risk: the breach is likely to result in significant harm, such as identity theft, financial loss, or reputational damage. Both ICO notification and direct notification to affected individuals are required.

5. Notifying the ICO (UK GDPR Article 33)

Where Sarah Johnson determines that a breach presents a risk to individuals' rights and freedoms, the ICO must be notified within 72 hours of The Corner Bakery becoming aware of the breach. Notification is made via: ico.org.uk/make-a-complaint/data-security-concerns/. If full information is not yet available within the 72-hour window, a partial report may be submitted. This is expressly permitted under UK GDPR — the report should clearly state that further information will follow, and updates must be provided promptly. The notification must include: the nature of the breach; the categories and approximate volume of personal data affected; the estimated number of individuals concerned; the contact details of Sarah Johnson as Data Controller; the likely consequences of the breach; and the measures taken or proposed to address the breach and mitigate its effects. Notification is not required where the breach is unlikely to result in any risk to individuals, for example, where a device containing encrypted data is lost and the encryption key has not been compromised.

6. Notifying Affected Individuals (UK GDPR Article 34)

Where a breach is assessed as high risk to individuals' rights and freedoms, Sarah Johnson must notify the affected individuals directly without undue delay. This includes, for example, a situation where customer payment card details, customer email addresses, or employee personal records are exposed to an unauthorised party. Notifications must be written in clear, plain English and must include: a description of the nature of the breach; the name and contact details of Sarah Johnson as Data

Controller (12 High Street, Manchester, M1 2AB); the likely consequences of the breach for the individual; the steps The Corner Bakery has taken or proposes to take to address the breach; and information about the individual's data protection rights and how they can exercise them, including the right to complain to the ICO. Notifications should be sent by the most effective means available, such as direct email or telephone, using the contact details held for each affected individual.

7. Containment Actions

Immediate steps must be taken to limit the impact of any breach. Relevant containment actions for The Corner Bakery include: remotely wiping or locking a lost or stolen personal device on which business data was stored; changing passwords or access credentials for any compromised account, including website admin, email, or payment system accounts; suspending access for any staff account believed to be compromised; contacting our payment card processor if card payment data may have been affected; retrieving any misdirected emails or documents where possible; securing any physical records that have been left accessible; applying security patches or updates to our website or any affected system; and reviewing CCTV system access logs if footage may have been viewed without authorisation. Sarah Johnson is responsible for coordinating all containment activity and for keeping a record of actions taken and the times at which they were taken.

8. Record-Keeping

All personal data breaches must be recorded in The Corner Bakery's Breach Log, regardless of whether notification to the ICO or to individuals is required. This is a mandatory requirement under UK GDPR. The Breach Log will be maintained by Sarah Johnson and will include for each incident: the date and time of discovery; a description of the nature of the breach; the categories of personal data involved (for example, customer contact details, employee payroll data, CCTV footage, or payment card data); the estimated number of individuals affected; the likely consequences of the breach; the remedial actions taken; and the notification decision, including the reasons if a decision was made not to notify the ICO or affected individuals. The Breach Log must be made available to the ICO on request.

9. Post-Breach Review

Within two weeks of resolving any breach, Sarah Johnson will conduct a root cause analysis to understand how the breach occurred and what can be done to prevent recurrence. This review will consider whether existing policies, procedures, or technical controls need to be updated; whether any staff training is required, particularly in relation to the use of personal devices for work purposes; whether the website, payment systems, or CCTV configuration requires improvement; and whether contractual arrangements with any third-party suppliers need to be reviewed. The findings and any recommended actions will be documented and communicated to all

relevant staff. Any updates to this procedure or related policies will be implemented promptly following the review.

10. Roles and Responsibilities

Data Protection Lead — Sarah Johnson: responsible for receiving all breach reports, conducting severity assessments, making notification decisions, coordinating containment, maintaining the Breach Log, and overseeing post-breach reviews. All Staff: responsible for identifying and immediately reporting any suspected breach to Sarah Johnson, following containment instructions, and not attempting to manage or conceal a breach independently. Staff using personal devices must report any suspected compromise of those devices without delay. IT and Systems: Sarah Johnson, with the assistance of any relevant third-party service providers (such as the website host or payment processor), is responsible for technical containment and recovery. Management Sign-Off: Sarah Johnson, as owner and Data Controller, holds final sign-off authority on all ICO notification and individual notification decisions.

11. Legislative References and Review

This procedure is issued under and should be read alongside: UK GDPR Articles 33 and 34; the Data Protection Act 2018; the Data (Use and Access) Act 2025 (provisions effective February 2026); and ICO guidance on personal data breach reporting. This procedure will be reviewed annually or following any data breach, whichever is sooner. Effective date: 31 May 2026. Data Controller: Sarah Johnson, The Corner Bakery, 12 High Street, Manchester, M1 2AB.

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

- 1. Subject Access Request Procedure

Subject Access Request Procedure

The Corner Bakery

1. Purpose and Scope

This procedure sets out how The Corner Bakery, 12 High Street, Manchester, M1 2AB, handles Subject Access Requests (SARs) in compliance with Article 15 of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Data (Use and Access) Act 2025 as effective from February 2026. Sarah Johnson, owner and Data Controller, is responsible for overseeing this procedure. The Corner Bakery processes personal data relating to customers, employees, website visitors, and suppliers. This procedure applies to all staff, whether using personal devices under our bring-your-own-device (BYOD) arrangement or any other means of handling business data.

2. What is a Subject Access Request?

A Subject Access Request is a request by an individual (a data subject) to find out what personal data The Corner Bakery holds about them and how it is used. Under Article 15 of the UK GDPR, any individual has the right to: (a) confirmation of whether we are processing their personal data; (b) a copy of that personal data; and (c) supplementary information about how and why the data is processed. This right applies to all categories of data subject whose information we hold, including customers whose email addresses and phone numbers we collect, employees (current and former), website visitors, and any suppliers or other individuals whose data we retain. Personal data held across all formats is in scope, including card payment records, CCTV footage, employee records, and any data stored on personal devices used for business purposes.

3. How Requests Can Be Made

A SAR can be submitted by any means — in person at our premises, by telephone, by email, by letter, via our website, or through social media. There is no requirement for the requester to use a specific form or to use the words 'Subject Access Request'. Any communication in which a customer, employee, or other individual asks to see 'their data', 'what information we hold on them', or 'their records' must be treated as a potential SAR. All staff at The Corner Bakery must be trained to recognise such requests regardless of the channel through which they arrive. On receipt of a suspected SAR, the member of staff who receives it must forward it to Sarah Johnson within 24 hours without delay. SARs received via personal devices used for business purposes must be treated with the same urgency as those received on any other channel.

4. Identity Verification

Before releasing any personal data, Sarah Johnson must take reasonable steps to verify the identity of the requester. This is to protect individuals from their data being disclosed to unauthorised third parties. Verification must be proportionate to the circumstances — for example, confirming a customer's name alongside their email address or phone number already held on our system, or asking an employee to confirm their date of birth or staff start date. We will not request excessive documentation, and we will not use the verification process as a tactic to delay our response. Importantly, the one-month response clock begins from the date the request is received, not from the date identity is confirmed. If verification cannot be completed promptly, we will still work towards the response deadline.

5. Response Timeline

The Corner Bakery must respond to every SAR within one calendar month of the date the request is received. For example, a request received on 15 March must be responded to by 15 April. Where a request is complex or we receive multiple requests from the same individual at the same time, we may extend the response period by a further two months. If we apply an extension, we must notify the requester in writing within the first calendar month, explaining clearly why the extension is needed. We may not simply allow the deadline to pass without communication. Sarah Johnson is responsible for calculating and monitoring all SAR deadlines and must log each request on receipt.

6. What We Must Provide

In response to a valid SAR, The Corner Bakery must provide: (a) a copy of all personal data held about the requester, provided in a commonly used electronic format (such as a PDF or spreadsheet) unless the requester asks for another format; (b) the purposes for which the data is processed, for example, to fulfil orders, manage staff payroll, or operate CCTV for security; (c) the legal basis for each processing activity; (d) how long the data will be retained or the criteria used to determine retention periods; (e) details of any third parties with whom the data has been shared, such as card payment processors; (f) a summary of the data subject's rights, including the right to rectification, erasure, restriction of processing, and the right to object; (g) the right to lodge a complaint with the Information Commissioner's Office (ICO); (h) if data was not collected directly from the individual, information about its source; and (i) whether any automated decision-making, including profiling, is applied to their data. If CCTV footage captures an identifiable individual, they are entitled to request a copy, subject to the redaction of other individuals who also appear in the footage.

7. Exemptions

Certain categories of information may be withheld or redacted under DPA 2018 Schedule 2 exemptions. These include: data relating to identifiable third parties who have not consented to disclosure (for example, information about another employee or customer that appears within the requested data); legally privileged documents; information relating to the prevention or detection of crime; management forecasts and confidential business negotiations; and information that would prejudice ongoing legal proceedings. Exemptions must be applied narrowly and only where clearly justified. Sarah Johnson must document the reasoning for any exemption applied, recording which data was withheld and on what legal basis. Partial disclosure is preferable to withholding an entire document where only part of it is exempt — in such cases, the exempt portions should be redacted.

8. Fees and Manifestly Unfounded or Excessive Requests

Subject Access Requests are normally provided free of charge. A reasonable fee may be charged if a request is manifestly unfounded or excessive, particularly where it is repetitive in nature. Alternatively, we may refuse to act on such a request. If a fee is to be charged, Sarah Johnson must inform the requester of this before proceeding, giving them the opportunity to withdraw or narrow their request. We must be able to demonstrate why we consider a request to be manifestly unfounded or excessive and must not use this provision to avoid responding to legitimate requests.

9. Refusing a Request

If The Corner Bakery decides to refuse a SAR — whether on grounds that it is manifestly unfounded, excessive, or falls within a recognised exemption — Sarah Johnson must inform the requester in writing within the one-month deadline. The written response must: state clearly that we are refusing the request; explain the reasons for refusal; advise the requester of their right to complain to the ICO; and advise them of their right to seek judicial remedy. We must never simply ignore a SAR. A refusal must always be communicated and properly recorded.

10. Record-Keeping

Sarah Johnson must maintain a SAR log recording: the date the request was received; the identity of the requester; the nature of the request; the deadline for response; the data provided and any data withheld (with reasons); whether an extension was applied and why; any fee charged; and the date the response was sent. This log must be kept securely and reviewed periodically. Given that staff use personal devices for business purposes, Sarah Johnson must ensure that data searched in response to SARs covers all locations where personal data may be stored, including messaging apps, email accounts, and any cloud-based tools used on BYOD devices.

11. ICO Complaints and Enforcement

If a requester is dissatisfied with our response, or if we fail to respond within the required timeframe, they have the right to complain to the Information Commissioner's Office (ICO) at ico.org.uk. The ICO has the authority to investigate complaints, request information from The Corner Bakery, and issue enforcement notices or monetary penalties where breaches are found. Sarah Johnson should treat any notification of an ICO complaint seriously and cooperate fully with any investigation. Relevant legislative references for this procedure are: UK GDPR Articles 12 and 15; DPA 2018 Schedule 2; ICO Right of Access Guidance; and the Data (Use and Access) Act 2025.

12. Review

This procedure was adopted on 31 May 2026 and will be reviewed annually or sooner if there are changes to data protection law, ICO guidance, or the nature of The Corner Bakery's data processing activities. Sarah Johnson is responsible for ensuring this procedure remains current and that all staff are aware of and trained on its contents.

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

- 1. Acceptable Use Policy

Acceptable Use Policy

The Corner Bakery

1. Purpose and Scope

This Acceptable Use Policy ('Policy') sets out the rules governing the use of IT systems, devices, and data at The Corner Bakery, 12 High Street, Manchester, M1 2AB. It applies to all employees, workers, contractors, and volunteers who use business IT systems or handle business data in any capacity. This Policy covers all systems and devices used in connection with The Corner Bakery's operations, including computers, mobile phones, tablets, email accounts, internet access, cloud services, point-of-sale systems, card payment terminals, and any software used to manage customer orders, bookings, or communications. Given that The Corner Bakery collects customer email addresses and phone numbers, operates a website, processes card payments, records CCTV footage, and maintains employee records, it is essential that all staff handle data and technology responsibly. This Policy is effective from 31 May 2026 and supports compliance with UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

2. Acceptable Use of Email

Email must be used professionally and primarily for business purposes relevant to The Corner Bakery's operations, such as communicating with suppliers, responding to customer enquiries, and coordinating staff matters. A courteous and professional tone must be maintained at all times. Staff must take particular care when handling personal data via email. Customer email addresses, phone numbers, order histories, or employee records must never be sent via unencrypted or plain email. Do not forward customer contact lists or bulk personal data to personal email addresses. Staff must remain vigilant against phishing and social engineering attacks. If you receive an unexpected email requesting urgent action, a payment change, login credentials, or access to systems, do not act on it immediately. Verify the request by contacting the sender through a separate, trusted channel before responding or clicking any links.

3. Acceptable Use of the Internet and Business Systems

Business systems and internet access are provided primarily to support the work of The Corner Bakery, including managing orders, processing payments, updating the website, and communicating with customers and suppliers. Limited personal use is permitted during breaks, provided it does not interfere with your work duties, consume excessive bandwidth, or create any legal or reputational risk to the business. The following are not permitted on business systems at any time: streaming media or music for personal entertainment, online gaming, accessing adult or otherwise inappropriate content, or

using social media in a way unrelated to business operations. Card payment systems and any device connected to the payment network must be used exclusively for business purposes and must not be used to browse the internet or access unrelated applications.

4. Password and Security Requirements

All accounts used in connection with The Corner Bakery's systems must be protected by a strong password of at least ten characters, containing a mixture of upper and lower case letters, numbers, and symbols. Passwords must not be shared with anyone under any circumstances, including colleagues, managers, or family members. Do not reuse passwords across different systems or accounts. Where a password manager is available, staff are encouraged to use it to generate and store unique passwords securely. Multi-factor authentication (MFA) must be enabled on all systems that support it, including email accounts, cloud services, and the business website's administration panel. When leaving a device unattended, even briefly, lock your screen immediately using Windows+L on Windows devices or Ctrl+Command+Q on Apple devices.

5. Prohibited Activities

The following activities are strictly prohibited when using any device or system in connection with The Corner Bakery: (a) accessing, downloading, storing, or distributing illegal, discriminatory, offensive, defamatory, or obscene content; (b) installing unauthorised software, browser extensions, or applications on any device used for business purposes; (c) sharing login credentials with any person, including colleagues or the business owner; (d) using business systems or data to operate a personal business or for personal financial gain; (e) downloading or distributing copyrighted material without an appropriate licence; (f) transferring bulk personal data, such as customer contact details, without authorisation or via unsecured channels; (g) attempting to access systems, files, or data that you are not authorised to view, including accessing customer payment data beyond your role; (h) circumventing or attempting to bypass security controls, firewalls, or monitoring systems; and (i) connecting unknown or unverified USB drives or external storage devices to any business system.

6. Personal Devices (BYOD)

As The Corner Bakery permits staff to use personal devices for work purposes, the following rules apply to all personal phones, tablets, or laptops used in connection with the business. All personal devices used for work must be registered with Sarah Johnson before being used to access business data or systems. Devices must meet minimum security requirements: a screen lock using a PIN, password, or biometric authentication must be enabled; the device operating system and apps must be kept up to date; and a reputable antivirus or security application must be installed where applicable. Business data, including customer contact details, order information, and any employee records,

must be stored only in approved apps or cloud services designated by the business. Data must not be saved to personal photo libraries, personal cloud storage accounts, or messaging apps. By using a personal device for work, you consent to the remote deletion of company data held on that device if the device is lost, stolen, or compromised. This remote wipe will be limited to company data only and will not affect your personal files or data. Upon leaving The Corner Bakery, all business data must be permanently removed from your personal device, and access to business accounts must be revoked immediately.

7. Monitoring

The Corner Bakery reserves the right to monitor the use of business systems, accounts, and devices for the purposes of security, legal compliance, and ensuring the effective operation of the business. Monitoring may include review of email content sent from business accounts, internet browsing activity on business systems, application usage, and access logs. The Corner Bakery operates CCTV on its premises; use of CCTV is governed separately by the CCTV Policy and the Data Protection Policy. All monitoring is conducted in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA), UK GDPR, and the Data Protection Act 2018. Staff are reminded that there is no expectation of personal privacy when using business-owned systems or accounts. Where personal devices are used for work under the BYOD arrangement, monitoring is limited to business applications and data only.

8. Data Protection Responsibilities

All staff at The Corner Bakery who handle personal data, including customer email addresses, phone numbers, card payment data, or employee records, must comply with the business's Data Protection Policy. The data controller is Sarah Johnson. Personal data must be processed lawfully, fairly, and securely. Suspected data breaches, including lost devices, unauthorised access to customer data, or accidental disclosure of personal information, must be reported to Sarah Johnson immediately. Under the Data (Use and Access) Act 2025, effective February 2026, obligations around transparency and accountability for data use are strengthened, and all staff must support the business in meeting these duties. Do not transfer personal data to personal email addresses or unapproved storage. When sending sensitive data externally, use a secure and encrypted file transfer method.

9. Social Engineering and Phishing Awareness

Staff at The Corner Bakery should be aware that criminals may attempt to obtain access to business systems, customer data, or financial accounts by impersonating trusted individuals or organisations. Be suspicious of any email, text message, or phone call that creates a sense of urgency, requests payment details, asks you to click an unfamiliar link, or requests your login credentials. This includes messages that appear to come from suppliers, card payment providers, or even from within the business.

Never enter your password or payment details in response to an unsolicited request. Always verify unexpected requests by contacting the relevant person or organisation through a known and trusted contact method, not by replying to the suspicious message. Report any suspicious communications to Sarah Johnson as soon as possible.

10. Consequences of Breach

Any breach of this Policy will be taken seriously. Depending on the nature and severity of the breach, disciplinary action may be taken in accordance with The Corner Bakery's disciplinary procedure. This may include a formal warning, suspension, or dismissal in cases of serious or repeated breaches. Certain breaches may also constitute a criminal offence. Unauthorised access to computer systems or data is an offence under the Computer Misuse Act 1990. Unlawful processing of personal data may constitute an offence under the Data Protection Act 2018. The Corner Bakery reserves the right to refer matters to the police or the Information Commissioner's Office (ICO) where appropriate.

11. Review and Approval

This Policy was adopted by The Corner Bakery on 31 May 2026 and is approved by Sarah Johnson, Data Controller and Owner. It will be reviewed annually or sooner if there are significant changes to the business's systems, devices, or applicable legislation. All staff will be informed of any material updates to this Policy. Questions regarding this Policy should be directed to Sarah Johnson at the business address: 12 High Street, Manchester, M1 2AB. Legislative references: UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025, Computer Misuse Act 1990, Regulation of Investigatory Powers Act 2000 (RIPA).

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

1. Social Media Policy

Social Media Policy

The Corner Bakery

1. Purpose and Introduction

This Social Media Policy has been prepared for The Corner Bakery, 12 High Street, Manchester, M1 2AB. It is effective from 31 May 2026 and applies to all use of social media in connection with the business.

Social media is a valuable tool for promoting The Corner Bakery, engaging with customers, and building our reputation in the local community. However, its misuse can cause serious harm — including damage to our reputation, legal liability, and breaches of data protection law. This policy is designed to protect the business, our employees, and our customers from reputational, legal, and data protection risks arising from social media use, whether on official business accounts or personal accounts where The Corner Bakery could be identified.

2. Scope

This policy applies to all individuals working at or for The Corner Bakery, including full-time staff, part-time staff, casual workers, contractors, and volunteers — regardless of seniority or role.

It covers:

- Use of official The Corner Bakery social media accounts at any time.
- Personal social media use during working hours.
- Personal social media use outside working hours where The Corner Bakery is identified, referenced, or could reasonably be identified from the content.

As The Corner Bakery operates on a bring-your-own-device (BYOD) basis, staff who access social media on personal devices for work-related purposes are equally subject to this policy. All staff are expected to read, understand, and comply with these rules.

3. Official Business Accounts and Representing The Corner Bakery Online

Only staff authorised by Sarah Johnson (Owner and Data Controller) may post content on The Corner Bakery's official social media accounts. Authorised staff must ensure that all content is accurate, professional, and consistent with the bakery's tone and branding.

When managing official accounts, authorised staff must:

- Obtain approval for any significant announcements, promotions, or posts relating to pricing or new products before publishing.
- Not make commitments, quotes, or statements on behalf of The Corner Bakery without prior approval from Sarah Johnson.
- Follow any agreed branding guidelines, including the use of the bakery's name, logo, and imagery.
- Use strong, unique passwords for all business social media accounts and enable two-factor authentication (2FA) on every platform.
- Ensure that Sarah Johnson maintains an up-to-date register of all staff who have access to each account.
- Complete a formal handover of all account access and passwords to Sarah Johnson upon leaving the business. Access must be revoked promptly when a member of staff departs.

Content created for The Corner Bakery's official accounts — including photographs of products, written copy, and promotional material — belongs to the business, not the individual who created it.

4. Personal Social Media Use

Staff are free to use personal social media accounts in their own time. However, where The Corner Bakery is identified or identifiable, the following rules apply at all times:

- Do not post anything that could bring The Corner Bakery into disrepute or damage its reputation with customers, suppliers, or the wider public.
- Do not use The Corner Bakery's name, logo, or branding on personal accounts in a way that could imply official endorsement.
- Adding a disclaimer such as 'views are my own' does not provide legal protection. Staff remain personally liable for defamatory statements, breaches of confidence, or discrimination expressed online, even in a personal capacity.
- Personal social media activity during paid working hours should be kept to a minimum and must not interfere with duties at the bakery.

5. Confidentiality and Data Protection

The Corner Bakery handles personal data in accordance with UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (effective February 2026). Social media use must not result in any breach of these obligations.

Staff must NEVER post on any social media platform — whether on official or personal accounts:

- The names, contact details, email addresses, or telephone numbers of customers. This is particularly important as The Corner Bakery collects customer emails and phone numbers, and this data must remain strictly confidential.

- Images, photographs, or videos of customers taken inside or outside the bakery without their explicit written consent. Images must not be published even if the customer appears incidentally in the background.
- Details of internal business information, including financial data, pricing strategies, supplier arrangements, or unreleased plans (such as new menu items not yet announced).
- Details of any ongoing complaints, disputes, or legal matters involving the business, a customer, or a colleague.
- Information about any colleague's personal circumstances, health, conduct, or performance.
- Images taken inside The Corner Bakery that could inadvertently reveal confidential information — for example, images showing order receipts, staff rotas, or customer details on screen.
- Details of employee records or any information held in staff files.

Any accidental disclosure of personal data via social media must be reported to Sarah Johnson immediately as it may constitute a reportable data breach under UK GDPR.

6. Conduct Towards Colleagues, Customers, and Competitors

The Corner Bakery is committed to maintaining a respectful and inclusive working environment. This extends to behaviour online.

Staff must not post anything on social media — whether directly or by implication — that:

- Could be interpreted as bullying, harassment, or discrimination towards any colleague, customer, or competitor.
- Identifies or targets a recognisable individual, even if no name is used. Anonymised posts that could reasonably identify a person are equally prohibited.
- Involves screenshotting or sharing internal communications, messages, or conversations from workplace messaging groups or apps.
- Makes derogatory comments about customers, competitors, or suppliers in connection with The Corner Bakery.

Breaches of this section may also amount to misconduct under employment law and could result in disciplinary action.

7. Handling Negative Comments and Online Complaints

Negative reviews and comments are an inevitable part of running a customer-facing food business. Staff must handle these situations carefully and professionally.

- Do not delete or hide negative comments without first escalating the matter to Sarah Johnson. Removing comments without consideration can escalate situations and, in

some cases, may have legal implications.

- Do not respond to negative comments in a personal or emotional manner. Do not engage in public arguments on behalf of the business or in a personal capacity.
- Escalate all complaints or negative comments received via social media to Sarah Johnson, who will determine the appropriate professional response.
- Where a comment contains allegations that may have legal implications — for example, a claim of food safety failure or a threat of legal action — do not respond until advice has been sought.
- Where The Corner Bakery becomes aware of posts impersonating the business or using its name without authorisation, this must be reported to Sarah Johnson immediately so that appropriate action can be taken with the relevant platform.

8. Reporting Obligations

All staff have a responsibility to report the following to Sarah Johnson without delay:

- Any social media content — by staff or third parties — that appears to breach this policy.
- Any negative coverage of The Corner Bakery that could affect its reputation or business.
- Any suspected impersonation accounts, fake reviews, or fraudulent use of The Corner Bakery's name or branding.
- Any accidental or suspected sharing of customer or staff personal data via social media.

Prompt reporting allows the business to respond quickly and minimise potential harm. Staff should not attempt to resolve such matters independently.

9. Consequences of Breach

Compliance with this policy is a condition of working at The Corner Bakery. Breaches will be taken seriously.

Depending on the nature and severity of the breach, consequences may include:

- An informal discussion or written warning.
- Formal disciplinary proceedings in accordance with the bakery's disciplinary procedure.
- In serious cases — such as the deliberate sharing of customer data, harassment of a colleague online, or bringing the business into significant disrepute — dismissal without notice may be considered.
- In cases involving data protection breaches, defamation, or intellectual property infringement, the business may also pursue civil legal action.

Staff should be aware that posts shared online may be permanent and traceable, even after deletion.

10. Policy Review

This policy was issued on 31 May 2026 by Sarah Johnson, Owner and Data Controller of The Corner Bakery.

It will be reviewed annually, or sooner if there are significant changes to legislation, social media platforms, or the business's operations. Staff will be informed of any material updates. It is each individual's responsibility to ensure they are familiar with the current version of this policy.

For any questions about this policy, please speak to Sarah Johnson directly.

Generated by Comply Sorted | complysorted.co.uk

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

1. Fire Safety Policy

Fire Safety Policy

The Corner Bakery

1. Policy Statement and Commitment

The Corner Bakery, located at 12 High Street, Manchester, M1 2AB, is fully committed to ensuring the fire safety of all employees, customers, and visitors on its premises. This policy sets out the arrangements in place to prevent fire, respond effectively in an emergency, and comply with all relevant legislation.

This policy is issued in accordance with the Regulatory Reform (Fire Safety) Order 2005, which places a legal duty on the Responsible Person to take general fire precautions to ensure the safety of all relevant persons. The Fire Safety (England) Regulations 2022 impose additional duties, including the requirement to share fire safety information with residents and building managers where applicable.

Sarah Johnson, owner of The Corner Bakery, accepts overall accountability for fire safety at these premises and is committed to ensuring that all reasonable steps are taken to prevent fire and protect life. This policy is effective from 31 May 2026 and will be reviewed annually.

2. Named Responsible Person

The designated Responsible Person for fire safety at The Corner Bakery is:

Name: Sarah Johnson

Role: Owner and Responsible Person

Premises: 12 High Street, Manchester, M1 2AB

As Responsible Person, Sarah Johnson has a legal duty under the Regulatory Reform (Fire Safety) Order 2005 to:

- Carry out or commission a suitable and sufficient fire risk assessment for the premises;
- Implement any findings and remedial actions identified;
- Ensure adequate fire detection, warning, and firefighting equipment is in place;
- Establish and maintain an emergency evacuation procedure;
- Ensure all staff are trained in fire safety;
- Review and update fire safety arrangements regularly;
- Maintain a fire log book recording all tests, drills, maintenance, and incidents.

In the absence of Sarah Johnson, all staff on duty share responsibility for following this policy and ensuring the safe evacuation of the premises.

3. Fire Risk Assessment

A fire risk assessment has been completed for The Corner Bakery premises at 12 High Street, Manchester, M1 2AB. As a working bakery and café serving food and hot beverages, the following key fire hazards have been identified and assessed:

- Commercial cooking and baking equipment, including ovens, grills, and hot plates, which generate significant heat and present an ignition risk;
- Accumulation of grease and food residue on cooking surfaces, extractor hoods, and ducting, which can fuel a fire if not regularly cleaned;
- Gas supply lines serving cooking equipment, which must be regularly inspected and switched off when the premises are unoccupied;
- High-heat areas adjacent to flammable materials such as packaging, paper bags, cardboard boxes, and wooden furniture;
- Electrical equipment including display fridges, till systems, card payment terminals, and kitchen appliances.

Control measures in place include a strict cleaning schedule for all cooking equipment, regular inspection of gas connections, appropriate separation of flammable materials from heat sources, and adequate ventilation throughout the kitchen and customer areas.

The fire risk assessment will be reviewed annually and immediately following any fire incident, near miss, significant change to the premises, equipment, or staffing arrangements.

4. Emergency Evacuation Procedure

In the event of a fire or suspected fire at The Corner Bakery, the following procedure must be followed immediately by all staff:

1. Raise the alarm without delay — shout to alert others, activate the nearest call point or break-glass unit, or sound the alarm.
2. Call 999 immediately and state the address clearly: The Corner Bakery, 12 High Street, Manchester, M1 2AB.
3. Evacuate the premises calmly and swiftly using the nearest available safe escape route. Do NOT use any lift.
4. Do NOT stop to collect personal belongings, coats, bags, or equipment.
5. Assist any customer, colleague, or visitor who requires help to evacuate safely, in line with any Personal Emergency Evacuation Plan (PEEP) in place.
6. Direct all persons to the designated assembly point: [outside at the front of the

premises on the pavement opposite the main entrance — to be confirmed and clearly signposted by the Responsible Person].

7. Do NOT re-enter the building under any circumstances until the fire service has declared it safe to do so.

8. A roll call must be conducted at the assembly point against the staff register and any record of customers present at the time of evacuation.

5. Fire Warden Responsibilities

Given the small size of the team at The Corner Bakery (between two and five members of staff), Sarah Johnson is the designated Fire Warden. A second member of staff will be nominated as deputy Fire Warden and briefed accordingly.

The Fire Warden's responsibilities during an evacuation are:

- Ensure all areas of the premises are evacuated, including customer seating areas, kitchen, store rooms, and staff areas;
- Check toilets and any enclosed or hidden areas to confirm no person remains inside;
- Close all doors on exit to slow the spread of fire and smoke;
- Confirm evacuation status to the fire service on their arrival and provide any relevant information about the premises;
- Conduct and record the roll call at the assembly point;
- Maintain order and calm at the assembly point and prevent anyone from re-entering the building.

6. Fire Detection and Alarm Systems

The Corner Bakery is fitted with smoke and heat detection equipment appropriate to a commercial catering environment. The alarm system provides audible warning throughout the premises to ensure all areas can be alerted simultaneously.

The following testing and maintenance schedule is in place:

- Weekly alarm test: conducted on the same day and at the same time each week. All test results are recorded in the fire log book, including the date, time, person conducting the test, and outcome.
- Annual service: the alarm system is serviced and inspected by a competent, qualified contractor at least once per year. Service records are retained in the fire log book.
- Fire log book: a written fire log book is maintained on the premises at all times and is available for inspection by the fire authorities upon request.

7. Firefighting Equipment

The following firefighting equipment is provided at The Corner Bakery, located in clearly marked and accessible positions:

- Wet chemical extinguisher: located in the kitchen area, suitable for use on cooking oil fires and commercial kitchen hazards including deep fat fryers and oil-based cooking equipment;
- CO2 extinguisher: located near electrical equipment including the till, card payment terminal, and any IT devices, suitable for electrical fires;
- Fire blanket: located in the kitchen area for smothering small pan fires quickly and safely.

Maintenance arrangements:

- Monthly visual inspection by a member of staff to ensure equipment is in position, undamaged, and unobstructed. Results recorded in the fire log book.
- Annual service and inspection by a competent contractor. Service labels to be kept current.

All staff are trained in the correct and safe use of each extinguisher type. This training is refreshed at least annually.

8. Staff Training Requirements

All staff at The Corner Bakery, including any temporary or part-time workers, must receive fire safety training as follows:

- Induction training: all new starters receive fire safety awareness training before or on their first day. This covers the location of fire exits, extinguishers, and the alarm system; the emergency evacuation procedure; and the location of the assembly point.
- Annual refresher training: all staff receive refresher fire safety training at least once per year.
- Evacuation drills: a practical evacuation drill is conducted at least once per year. Given the nature of The Corner Bakery as a food preparation and customer-facing premises, two drills per year are recommended as best practice.
- All training sessions and drills are recorded in the fire log book, including the date, attendees, and any observations or actions arising.

9. Visitors, Customers, and Persons Requiring Assistance

The Corner Bakery welcomes members of the public as customers on a daily basis. Fire exit signage is clearly displayed throughout the premises to guide customers to safe exit routes in an emergency. Staff will verbally direct customers to evacuate calmly and quickly during any fire alarm activation.

Personal Emergency Evacuation Plans (PEEPs): where any member of staff or a regular visitor to the premises has a disability or mobility impairment that may affect their ability to evacuate independently, a personalised PEEP will be prepared in advance,

agreed with the individual, and reviewed at least annually. PEEPs are stored securely and made known to the Fire Warden.

All staff are expected to assist any customer or visitor who requires help evacuating the premises, ensuring no person is left behind.

10. Out-of-Hours Access

The Corner Bakery has confirmed that it does not operate a formal lone working arrangement. However, in circumstances where a single member of staff may be on the premises alone — for example during early morning preparation or closing — the following precautions must be observed:

- The fire alarm system must be active and operational at all times;
- All fire escape routes must be checked to ensure they are unobstructed and accessible;
- The member of staff must have a means of raising the alarm, including a charged mobile phone to call 999 if required;
- The full evacuation procedure set out in Section 4 of this policy must be followed without exception.

Sarah Johnson is responsible for ensuring these arrangements are communicated to all staff.

11. Emergency Services Information and Record-Keeping

The full address of the premises — The Corner Bakery, 12 High Street, Manchester, M1 2AB — is clearly posted near the main entrance to assist emergency services in identifying the location rapidly. A site plan of the premises, indicating the layout, exit routes, location of firefighting equipment, and utility shut-off points, is available on request.

A fire log book is maintained on the premises and contains records of:

- All alarm tests and outcomes;
- Evacuation drills, including dates and attendees;
- Maintenance and servicing of fire detection, alarm, and firefighting equipment;
- Any fire incidents, near misses, or false alarms;
- Staff training records.

The fire log book is available for inspection by the fire authority or enforcing authority at any time.

12. Policy Review

This Fire Safety Policy will be reviewed by Sarah Johnson at least annually. A review will also be triggered immediately following any of the following:

- A fire, near miss, or false alarm on the premises;
- Any significant change to the layout, use, or occupation of the premises;
- The introduction of new equipment, processes, or materials that may affect fire risk;
- A change in staffing levels or key personnel responsible for fire safety;
- Any change in relevant legislation or guidance.

Policy effective date: 31 May 2026

Next scheduled review date: 31 May 2027

Responsible Person: Sarah Johnson, The Corner Bakery, 12 High Street, Manchester, M1 2AB

Legislative references: Regulatory Reform (Fire Safety) Order 2005; Fire Safety (England) Regulations 2022; HSE Fire Safety Guidance.

COMPLY SORTED

Compliance Document Pack

The Corner Bakery

12 High Street, Manchester, M1 2AB

Date Generated: 31 May 2026

Prepared by Comply Sorted (complysorted.co.uk)

Contents

1. Lone Worker Policy

Lone Worker Policy

The Corner Bakery

1. Status Notice — Not Currently Applicable

Business Name: The Corner Bakery

Owner / Data Controller: Sarah Johnson

Address: 12 High Street, Manchester, M1 2AB

Effective Date: 31 May 2026

This Lone Worker Policy has been prepared for The Corner Bakery. Following a review of current working arrangements, The Corner Bakery does not presently employ or engage any lone workers. No staff member is currently required to work without the close or direct supervision of at least one other person present on the premises or in the working environment.

As a result, the detailed operational provisions of this policy — including risk assessments, check-in procedures, and lone worker training requirements — are not currently activated or enforced. This document serves as a formal record that the matter has been considered and assessed as not applicable at this time.

2. Why This Policy Has Been Prepared

Although lone working does not currently apply at The Corner Bakery, Sarah Johnson, as the owner and responsible person, recognises that working arrangements can change. Staff numbers at The Corner Bakery are small (between two and five employees), and operational changes — such as staff absence, rota changes, early morning baking preparation, late-night close-down, deliveries, or emergency cover — could, at short notice, result in a situation where a member of staff is present on the premises or conducting business-related activity without a colleague present.

In a restaurant, takeaway, and café environment such as The Corner Bakery, potential lone working scenarios could include:

- Opening the premises alone in the early morning before other staff arrive.
- Closing and locking up the premises at the end of the evening without a second person present.
- Receiving early morning food or supplies deliveries without a colleague on site.
- A staff member remaining on the premises alone to complete cleaning, cashing up, or administrative tasks after other employees have left.
- Working in isolated areas of the premises, such as the kitchen, storage areas, or

cellar, without a colleague nearby.

Sarah Johnson has considered these scenarios and confirmed that, as of 31 May 2026, none of these situations arise routinely or as a matter of current practice. However, this policy has been documented so that The Corner Bakery is prepared to act quickly and responsibly should circumstances change.

3. Legal Framework

Should lone working arise at The Corner Bakery in the future, the following legal duties will immediately apply and must be addressed before any lone working is permitted:

— Section 2, Health and Safety at Work Act 1974: Sarah Johnson, as employer, has a duty to ensure, so far as is reasonably practicable, the health, safety, and welfare of all employees. This duty applies equally to those working alone.

— Regulation 3, Management of Health and Safety at Work Regulations 1999: A suitable and sufficient risk assessment must be carried out. Where lone working is identified as a working practice, the risk assessment must specifically consider the hazards and risks associated with working without supervision or the immediate assistance of a colleague.

— HSE Guidance INDG73 — 'Working Alone': The Health and Safety Executive's published guidance on lone working provides practical advice on identifying risk and implementing appropriate controls. The Corner Bakery will follow this guidance in full if lone working becomes part of its operations.

Sarah Johnson understands that failure to manage lone working risks appropriately would constitute a breach of these legal duties and could result in enforcement action by the Health and Safety Executive.

4. Commitment to Health, Safety, and Wellbeing

The Corner Bakery is committed to the health, safety, and wellbeing of every member of staff. Sarah Johnson takes her responsibilities as a small business owner seriously and recognises that lone working, even in a familiar environment such as a bakery or café, carries real risks — including the risk of accident or injury without assistance available, medical emergencies with no colleague present, risk of aggression from members of the public or late-night visitors, and communication difficulties.

Should lone working become a feature of working life at The Corner Bakery, it will be managed as an integral part of the overall health and safety management system, not as an afterthought. No member of staff will be required or permitted to work alone

without an appropriate risk assessment having first been completed, reviewed, and communicated to them.

5. Actions Required if Lone Working Arises

If Sarah Johnson determines that lone working will become a regular or foreseeable part of operations at The Corner Bakery — whether planned or as a result of changed circumstances — the following steps must be taken before lone working begins:

1. Conduct a written lone worker risk assessment for each identified lone working scenario (e.g. early morning opening, late-night close-down, lone kitchen work). The assessment must identify hazards, evaluate risks, and specify controls proportionate to those risks.
2. Establish a formal check-in procedure, including agreed intervals, a named check-in contact, and a clear escalation process for missed check-ins — including when to contact emergency services.
3. Ensure the lone worker carries a fully charged mobile phone, that signal coverage at relevant locations has been checked, and that higher-risk situations are supported by appropriate technology (such as a lone worker app with automated escalation).
4. Provide lone worker training to any affected member of staff, covering personal safety awareness, how to raise an alarm, de-escalation techniques where a risk of aggression is identified, emergency procedures, and incident reporting.
5. Obtain pre-authorisation from Sarah Johnson before any out-of-hours lone working takes place.
6. Record all risk assessments, training, and check-in logs. Review risk assessments annually and immediately following any lone working incident or near-miss.
7. Ensure all lone workers know the local emergency services number (999), Sarah Johnson's emergency contact number, and the location of the nearest medical facility.
8. Confirm that no member of staff will be penalised for refusing to carry out lone work they reasonably believe poses an unacceptable risk to their safety.

6. Review and Monitoring

Sarah Johnson will review this policy annually, and in any event before any operational change that could result in a member of staff working alone. The review will consider whether lone working has arisen or is likely to arise, whether this placeholder policy should be activated and expanded into a full operational lone worker policy, and

whether any incidents, near-misses, or staff concerns have been raised that are relevant to lone working safety.

If this policy is activated, a full review will then take place annually and following any lone working incident.

Next scheduled review date: 31 May 2027, or earlier if working arrangements change.

Policy Owner: Sarah Johnson, The Corner Bakery, 12 High Street, Manchester, M1 2AB.

Generated by Comply Sorted | complysorted.co.uk