App Privacy Policy – CJ Workplace

Last updated: 30th April 2026

1. Introduction

CJ Workplace ("we", "us", "our") is a mobile application operated and managed by **CJ Workplace Limited**.

The App is developed, owned, and maintained by **Get Smart Rewards Limited** ("GSR"), which acts solely as the technology and intellectual property provider. CJ Workplace Limited is responsible for the operation of the App and all user data.

Payment services within the App are facilitated by **GS Rewards and Benefits Limited** ("GSRB"), which operates as a Special Purpose Vehicle (SPV) to act as the nominated payment processing entity. This entity utilises third-party payment processors, who specialise in the secure online capture and processing of credit/debit card transactions for all secure payment processing activities, including compliance with PCI DSS standards. CJ Workplace Limited, GSR and GSRB do not store full payment card details.

For the purposes of data protection law, **CJ Workplace Limited is the data controller**. GSR and GSRB act as **data processors** on our behalf.

Registered office:
23 Market Street, Chorley, Lancashire, PR7 2SY, England
Company number: 13779545

CJ Workplace Limited aggregates and facilitates access to financial services and workplace benefits. CJ Workplace Limited is an **Appointed Representative of Cheetham Jackson Ltd**, which is authorised and regulated by the Financial Conduct Authority (FRN: 969033).

This Privacy Policy explains how we collect, use, share, and protect your personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Information We Collect

The information we collect from you or receive about you might include:

2.1 Personal Identity Information

- Full name and display name
- Full postal address (including postcode)
- Email address
- Telephone number
- Date of birth
- Gender
- Profile picture / avatar
- Data provided by forms or surveys

2.2 Employment Information

- Employer name
- Job title, department, employee ID
- Employment start date
- Client account association
- Registration source

2.3 Compensation and Benefits Data

- Salary, bonus, and commission
- Pension contributions and allowances
- Healthcare, dental, and life assurance benefits
- Company-provided benefits (e.g. car, gym membership, training budgets)

This data is used solely to provide personalised workplace insights and benefits.

2.4 Financial and Transaction Data

- Gift card purchase history and savings
- Voucher codes and redemption data
- Points balances and rewards earned
- Balance credits and usage
- Payment references such as payment service provider customer ID, payment-intent ID, and order identifiers.

Payment card details are never stored by us.

2.5 Booking and Appointment Data

- Service type and booking details
- Appointment date and status
- Notes and interaction timestamps

2.6 Support and Communications

- Support messages and attachments you send to us (including any images or files you choose to attach to a support ticket).
- Customer service interactions, including the content of your enquiries, our responses, and ticket status history.
- AI chat conversations and associated metadata (message content, timestamps, conversation identifiers, and token-usage counts).

The in-app AI assistant is powered by a third-party artificial intelligence service provider. When you send a message to the assistant, your message and the recent conversation history are transmitted to this provider solely for the purpose of generating a response. Content submitted through the API is **not** used to train its models. The provider may retain such content for a limited period (currently up to 30 days) solely for abuse and misuse monitoring, after which it is deleted from the providers systems.

We separately store your conversation history within our own environment so that you can resume previous chats. Please avoid sharing special-category personal data (such as health information) or other people's personal data in messages to the AI assistant.

2.7 Requests and Feedback

- Benefit and reward requests
- Feedback and inquiries
- Administrative responses

2.8 Preferences and Personalisation

- Favourite brands and content
- App settings and preferences
- Onboarding status

2.9 Analytics and Usage Data

- Session activity (session start time, session end time, session duration, app version, platform).
- Feature usage events (which in-app features you interact with, action names, and timestamps).
- Screen-view events (which screens you visit and the order in which you visit them).

- Navigation behaviour and engagement metrics derived from the above events.

Analytics events are linked to your account via your user ID and are stored in our systems and those of our third-party database infrastructure providers. We use this data to understand how the App is used, diagnose issues, and prioritise improvements. We do not sell analytics data, and we do not share it with third-party advertising networks. You can request deletion of your analytics history at any time by deleting your account or by contacting us.

2.10 Device and Technical Data

- Device model and platform (iOS or Android)
- Operating system version and app version / build number
- Push notification tokens (Apple APNs and Firebase Cloud Messaging) used to deliver in-app notifications
- Secure on-device storage identifiers used to keep you signed in (stored in the iOS Keychain or Android Keystore)
- Crash diagnostics, stack traces, and performance breadcrumbs captured by our error-monitoring provider
- IP address, as seen transiently by our hosting and payment infrastructure providers in request logs for security, fraud prevention, and debugging purposes
- A record of in-app and push notifications we have sent to your account, including the notification type, send timestamp, delivery status, and read/dismissed state.

2.11 Account and System Metadata

- User ID and role
- Account timestamps and activity logs
- System identifiers

3. How We Use Your Information

We may process your personal data under the following lawful bases:

Contractual Necessity

- To provide and operate the App
- To manage your account, purchases, and bookings

Legitimate Interests

- To improve the App and user experience
- To analyse usage and engagement
- To prevent fraud and misuse
- To detect, diagnose and resolve technical errors, crashes, and security incidents

Legal Obligations

- To comply with financial and regulatory requirements

Consent

- To collect analytics data where required
- To send push notifications

We do **not use your personal data for advertising or cross-app tracking**.

4. Sharing of Your Information

We may share your personal data with trusted third-party providers where necessary to operate the App.

These include:

- Technology platform providers
- Payment processing providers (including payment processing and related infrastructure)
- Infrastructure, hosting, and communications services
- Reward fulfilment providers

All providers:

- Act as **data processors**
- Process data only on our instructions
- Are contractually required to implement appropriate security measures

We do **not sell your personal data**.

5. Our Sub-Processors

To deliver the App, CJ Workplace Limited engages a limited number of third-party service providers ("sub-processors") who process personal data on our behalf. Where required, written data-processing terms are in place that meet the requirements of UK GDPR Article 28 and, where applicable, Articles 44–49 for international transfers.

5.1 Group / Internal Processors

Processor	Role	Data processed
Get Smart Rewards Limited (GSR)	Technology and intellectual property provider; develops and maintains the App	All categories of personal data necessary to operate and support the App
GS Rewards and Benefits Limited (GSRB)	Nominated payment Special Purpose Vehicle	Transaction metadata associated with gift-card and benefit purchases

5.2 External Sub-Processors

We use third-party providers in the following categories:

- **Cloud infrastructure and database providers** – to host application data, manage authentication, and support core platform functionality
- **Payment processing providers** – to process payments and manage transaction-related data (we do not store full card details)
- **Digital fulfilment providers** – to enable the delivery and redemption of digital products and services
- **Communications providers** – to send transactional emails and service-related notifications
- **Application monitoring providers** – to identify errors, crashes, and performance issues
- **Push notification services** – to deliver notifications to your device via platform providers such as Apple and Google
- **Artificial intelligence service providers** – to support specific features such as the in-app assistant, where applicable

These providers process personal data only on our instructions and in accordance with contractual safeguards.

5.3 What We Do Not Use

We do not use third-party advertising networks, behavioural advertising technologies, or external analytics platforms for user tracking. Usage analytics are handled within our own controlled environment.

5.4 International Transfers

Where personal data is transferred outside the United Kingdom, we ensure that appropriate safeguards are in place in accordance with applicable data protection laws.

Further information about how we handle international data transfers, including the safeguards we rely on, is set out in Section 10 of this Policy.

6. Tracking and Analytics

We request your permission where required before collecting analytics data.

If enabled:

- We collect anonymised or pseudonymised usage data

If disabled:

- No analytics tracking occurs

We do not use data for third-party advertising.

6A. Cookies and Tracking Technologies

The CJ Workplace mobile application does not use traditional browser cookies.

Instead, the App uses secure on-device storage and similar technologies to enable functionality such as authentication, preferences, performance optimisation, and analytics.

Further information about how these technologies are used, including how analytics tracking operates on iOS devices, is set out in our Cookies and Tracking Policy.

Specifically, we use secure storage mechanisms provided by your device's operating system, such as the iOS Keychain and Android Keystore, to retain authentication tokens, and local application storage to retain user preferences.

7. Financial Services

CJ Workplace Limited provides access to financial products, services, and workplace benefits.

All financial service offerings are aggregated and presented by CJ Workplace Limited.

CJ Workplace Limited acts as an **Appointed Representative of Cheetham Jackson Ltd**, authorised and regulated by the Financial Conduct Authority (FRN: 969033).

8. Data Security

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss, misuse, or alteration. These measures include:

- Encryption of data in transit using industry-standard protocols, and encryption of data at rest within our systems and those of our service providers
- Secure authentication mechanisms, including the use of hashed and salted passwords and controlled session management
- Use of secure, platform-provided storage mechanisms on your device (such as the iOS Keychain and Android Keystore) to protect authentication credentials
- Access controls and data segregation to ensure users can only access their own information, with administrative access restricted and monitored
- Use of trusted third-party providers for payment processing, where sensitive financial information is handled securely and not stored on our systems

- Secure delivery of service communications, including push notifications, using platform-supported mechanisms
- Monitoring and logging to detect, investigate, and respond to errors, security events, and potential vulnerabilities
- Regular maintenance, updates, and patching of systems and dependencies to address security risks

While we take appropriate steps to protect your personal data, no system can be guaranteed to be completely secure.

9. Data Retention

We retain personal data only for as long as necessary for the purposes set out in this Policy, to comply with our legal and regulatory obligations, and to resolve disputes. Typical retention periods are as follows:

- **Account and profile data:** retained while your account is active. Deleted (or anonymised where deletion is not technically possible) within a 30 day period following account closure, unless longer retention is required by law.
- **Financial and transaction records** (including purchase history, redemption data, and payment references): retained for up to 6 years from the date of the transaction, in line with UK financial record-keeping and tax requirements.
- **Compensation and benefits data:** retained while your account is active and deleted within a 30 day period following account closure.
- **AI chat interactions:** retained within our systems until you delete the conversation or your account. Content processed by third-party AI service providers may be retained for a limited period for security and abuse monitoring purposes and is not used to train models on our behalf.
- **Support tickets and customer service correspondence:** retained for up to 24 months after the matter is closed to support follow-up enquiries and dispute resolution.
- **Notification history** (including in-app and push notifications): retained for up to 12 months.
- **Analytics and usage data:** retained while your account is active and deleted upon account deletion or on request. Aggregated, non-identifying

analytics may be retained for longer periods for product improvement purposes.
- **System logs and diagnostics data** (including authentication and session logs): retained for a limited period (typically up to 90 days) for security, fraud prevention, and system integrity purposes.
- **Marketing and consent records:** retained for as long as necessary to demonstrate compliance with applicable laws and for a reasonable period thereafter.

Where we are required to retain data for longer to comply with legal, regulatory, accounting, or reporting obligations, we will do so for the minimum period necessary.

10. International Data Transfers

Most of your personal data is stored within the United Kingdom or the European Economic Area (EEA).

In some cases, we use carefully selected third-party service providers who may process personal data outside the UK or EEA, including in countries such as the United States. Where this occurs, we ensure that only the minimum necessary data is transferred for the relevant purpose.

Where personal data is transferred internationally, we implement appropriate safeguards in accordance with UK GDPR requirements. These may include:

- the UK International Data Transfer Agreement (IDTA); or
- the EU Standard Contractual Clauses together with the UK Addendum

These safeguards are supported by appropriate technical and organisational measures, such as encryption in transit and at rest.

Where applicable, additional contractual commitments may be in place with service providers to further protect personal data, including restrictions on data use and retention.

Further information about the categories of service providers we use is set out in Section 5 of this Policy.

11. Your Rights

Under UK data protection law, you have the following rights in relation to your personal data:

- **Right of access** – to request access to the personal data we hold about you and obtain a copy
- **Right to rectification** – to request that inaccurate or incomplete personal data is corrected
- **Right to erasure** – to request the deletion of your personal data where there is no overriding legal basis for us to retain it
- **Right to restrict processing** – to request that we limit how we use your personal data
- **Right to object** – to object to our processing of your personal data in certain circumstances
- **Right to withdraw consent** – where processing is based on consent (for example, for analytics or notifications), you may withdraw that consent at any time without affecting the lawfulness of prior processing
- **Right to data portability** – to request that your personal data is provided in a structured, commonly used, machine-readable format, where applicable

You can exercise any of these rights by contacting us at **support@email.cjworkplace.com** or via the in-app support feature.

We will respond to valid requests within one month of receipt, as required by UK GDPR. In certain circumstances, such as where requests are complex or numerous, this period may be extended by up to a further two months. We will notify you within the initial one-month period if an extension is required and explain the reasons.

We may need to verify your identity before processing your request in order to protect your personal data from unauthorised access.

If you are not satisfied with how we have handled your personal 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**. We would, however, appreciate the opportunity to address your concerns directly in the first instance.

12. Age Restrictions

The App is not intended for use by individuals under the age of 18, and we do not knowingly collect or process personal data relating to children.

If we become aware that we have collected personal data from a person under the age of 18 without appropriate authorisation, we will take steps to delete that information as soon as reasonably practicable.

If you believe that a child has provided personal data to us, please contact us using the details set out in this Policy.

13. External Links

We are not responsible for third-party services linked within the App.

14. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, our sub-processors, or applicable law. The "Last updated" date at the top of this Policy will always show when the most recent changes were made.

Where changes are material — for example, a change to the categories of personal data we collect, the lawful bases on which we rely, our retention periods, or the addition of a new sub-processor that involves an international transfer — we will notify you in advance through the App, by in-app notification, or by email to the address associated with your account, before the changes take effect.

We encourage you to review this Policy periodically so that you are aware of how we are protecting your personal data. Continued use of the App after an updated Policy takes effect constitutes acceptance of the updated terms, to the extent permitted by applicable law.

15. Contact Us

Email: support@email.cjworkplace.com
Or via the in-app support feature.