RHP Payment App – Privacy Notice

Last updated: 19-02-2026

About RHP

Richmond Housing Partnership Limited ("RHP") is a charitable Community Benefit Society registered with the Financial Conduct Authority under the Co operative and Community Benefit Societies Act 2014 (registration number 30939R). We are also registered with the Regulator of Social Housing (number L4279) and with the Information Commissioner's Office. Our registered office is 8 Waldegrave Road, Teddington, TW11 8GT.

The RHP Payment App is intended for RHP customers -including tenants, shared owners, and leaseholders - because it supports tenancy related payments and account management, which are responsibilities held by adults under UK law. The app is not designed for anyone under 18.

This Privacy Notice explains how RHP collects, uses, stores, and shares your information when you use the RHP Payment App. Please also see our Customer Privacy Notice. This can be viewed at https://www.rhp.org.uk/privacy-notice

RHP uses PayPoint's Multipay service to process payments made to us. Multipay is PayPoint's regulated payment platform and is used across different RHP payment channels, including payments made online, by telephone, and through the RHP Payment App. Multipay supports card payments, Open Banking payments, refunds, settlement, reconciliation and fraud prevention activities. It operates as a single, integrated service delivered by several regulated PayPoint companies.

GDPR Compliance

RHP processes your personal information in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. As the data controller, RHP is responsible for ensuring that your information is handled lawfully, fairly, and transparently.

Lawful bases for processing:

- Contract – to provide the app, process payments, and manage your account
- Legal obligation – to meet financial, audit, fraud prevention, and regulatory requirements
- Consent – for optional features such as biometric login or saving card details
- Legitimate interests – to maintain app security, diagnose issues, and ensure service reliability

1. Information We Collect

Information you provide

Registration and account information

- Name,
- Email address
- Mobile number
- RHP Service Account Number (SAN)

Payment Information

- Card payment details
- Billing address (used for card payment verification and fraud prevention checks)
- Open Banking payment details

Information collected automatically

- Transaction history
- Technical and diagnostic information
- IP address and related network and device information (used for security, fraud prevention, and to protect payment transactions)

Device permissions

- Camera access (optional)
- Biometric login (optional)

Biometric data is never collected or stored by RHP. If you use biometric login, your device processes your fingerprint or facial data locally using its built in secure hardware and software (such as Apple Face ID/Touch ID or Android BiometricPrompt). The app receives only a secure confirmation that authentication was successful — it never receives or has access to your biometric data.

2. How We Use Your Information

We use your information to process payments, support authentication, send receipts, display transactions, maintain security, and enable optional biometric login.

We do not use your information for advertising or profiling.

3. Information We Share

PayPoint has been contracted by RHP to develop and support payment services, and we share your information only with approved contracted providers like PayPoint who help us deliver secure payment and Open Banking services.

PayPoint Group companies “PayPoint” and their roles

PayPoint plc – parent company overseeing PayPoint's UK payment and digital services.

PayPoint Network Limited – operates the PayPoint retail network and supports in store payment services.

PayPoint Digital Limited – a regulated Open Banking provider regulated by Open Banking Directory: https://www.openbanking.org.uk/regulated-providers/paypoint-digital/

PayPoint Payment Services Limited (PPSL) – provides Open Banking connectivity and account information/payment initiation services (AIS/PIS).

All registered at 1 The Boulevard, Shire Park, Welwyn Garden City, Herts AL7 1EL

OBCONNECT Limited – A PayPoint majority invested company - provides Open Banking technology for banks (ASPSPs) and third party providers (TPPs)

Website: https://obconnect.io

Registered office: WG08, West building, Workspace Vox Studios, 1-45 Durham Street, London, SE11 5JH

Open Banking Payment Initiation

Permission to Make an Open Banking Payment

When you choose to pay by bank transfer, the RHP Payment App directs you to PayPoint's regulated Open Banking service.

Open Banking payments require your explicit consent for each transaction. You must review and approve every payment within your own banking app or online banking service before it can be completed. RHP and PayPoint cannot initiate a bank to bank payment without your active authorisation.

Your bank shares your sort code and account number with PayPoint only for the purpose of initiating the payment and issuing a refund. All authentication and payment approval take place within your bank's secure environment. RHP does not receive or store your bank login credentials.

Controller and Processor Roles

RHP is the data controller for the personal information you provide when using the RHP Payment App. This includes your contact details, SAN , app activity, and any preferences you set within the app.

PayPoint act as independent data controllers for Open Banking information they process. This includes bank to bank payments, Open Banking journeys, and any information required to initiate, authenticate, or refund a payment.

Financial Institutions Involved in Card Payments

When you make a card payment, several financial institutions may process your information as independent data controllers.

Including:

- PayPoint using payment process services from Access PaySuite Ltd, Pay and Shop Limited (trading as Global Payments), and Cardstream Limited to process payments.
- Your card issuer
- RHPs Acquiring bank (Elavon, https://www.elavon.co.uk/)
- Card schemes (e.g. Visa, Mastercard)
- Fraud prevention and anti-money laundering (AML) services used by banks and card networks

These organisations process your card information for:

- authorising and settling payments
- preventing fraud and financial crime
- meeting regulatory and audit requirements
- resolving disputes and chargebacks

These organisations act as independent data controllers for the parts of the card payment process they each handle. Although they do not jointly determine how your data is used, they operate together within the same global card payment network to authorise, process, and settle your transaction. Each institution is responsible for the data it processes within its own systems.

3 D Secure 2 (3DS2) and Strong Customer Authentication

Card payments may involve Strong Customer Authentication (SCA) using 3 D Secure 2 (3DS2). This is a security step required by your bank or card issuer to confirm that the payment is genuine. During 3DS2 checks, you may be asked to verify the payment using your banking app, a one time passcode, biometrics, or another method chosen by your bank. These checks are carried out directly between your bank, the card network (such as Visa or Mastercard), and the payment processors involved in the transaction. RHP does not receive or store any authentication codes, passwords, or biometric information used during 3DS2.

Information used during 3DS2 checks

During 3DS2 Strong Customer Authentication, your bank, the card network, and the payment processors involved in the transaction may analyse information such as your IP address, device information, browser or app settings, and transaction patterns to detect fraud and confirm that the payment is genuine. These checks take place within the secure systems of those financial institutions.

RHP does not control how these financial institutions process your card data.

4. International Transfers

Some payment related information may be transferred outside the UK/EEA by your bank, card issuer, acquiring bank, or global card schemes. These transfers are determined and controlled by those financial institutions, not by RHP

5. Security and Storage

Card details are encrypted and stored securely by PayPoint

RHP does not store card details in the app

Hosted payment information is stored in the UK

Biometric data never leaves your device

6. Retention of Your Information

- Information is retained while you actively use the app
- Inactive accounts may be disabled and later deleted
- Payment information may be retained longer where required by law
- Saved card details remain until you delete them

7. Your Rights Under UK GDPR

You have the right to access, correct, delete, restrict, object, request portability, withdraw consent, and complain to the ICO.

8. Your Choices and Controls

You can delete saved cards, disable camera access, choose not to use biometric login, uninstall the app, or contact RHP to exercise your rights.

9. Contact Us

Email: dpo@rhp.org.uk

Post: Data Protection Team, RHP, 8 Waldegrave Road, Teddington, TW11 8GT

Telephone: 0800 032 2433

10. Updates to This Notice

We may update this notice if there are significant changes to how we use your personal information.