

Privacy Policy

Rowheath Pavilion Christian Trust (RPCT) & Rowheath Pavilion Limited (RPL)

This policy replaces the 2023 Privacy Policy and should be read alongside RPCT's related HR policies on safeguarding, finance, governance and operational policies.

1. Purpose

Rowheath Pavilion Christian Trust (RPCT) and Rowheath Pavilion Limited (RPL) are committed to protecting privacy and handling personal information fairly, lawfully, securely and transparently. This policy explains how we collect, use, store, share and protect personal information under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable law.

2. Who We Are

RPCT is a registered charity and charitable company that owns Rowheath Pavilion and provides community, recreational, charitable and faith-based activities. RPL is its wholly owned trading subsidiary and supports the operation and management of the Pavilion and its facilities.

- RPCT: registered charity number 1112847; company number 05433044.
- RPL: company number 01896443.
- Registered office: Rowheath Pavilion, Heath Road, Bournville, Birmingham B30 1HH.

RPCT and RPL may each act as a data controller for the personal information they process. Where they jointly determine why and how information is used, they may act as joint controllers.

3. Whose Information We Process

- Visitors, service users and activity participants.
- Customers, hirers, tenants and event organisers.
- Donors, supporters and Gift Aid declarants.
- Employees, workers, applicants, trustees and volunteers.
- Contractors, suppliers, advisers and partner representatives.
- People who contact us with enquiries, complaints or safeguarding concerns.
- Individuals captured by CCTV.

4. Information We Collect

- Names and contact details.
- Emergency contacts and access or support information.
- Booking, hire, tenancy, attendance, payment information and bank details where needed to return security deposits.
- Donation, fundraising and Gift Aid records.
- Employment, recruitment, trustee and volunteer administration records.
- Safeguarding information where necessary and lawful.
- CCTV images and incident records.
- Enquiries, correspondence, complaints and requests.
- Information required for legal, regulatory, contractual, insurance, health and safety or safeguarding purposes.

5. How We Collect Information

- Directly through forms, bookings, applications, registrations, donations, correspondence or conversations.
- From authorised representatives, employees, trustees or contractors.
- From statutory bodies, safeguarding agencies, emergency services, insurers or advisers where lawful and necessary.
- Automatically through CCTV systems.

6. How We Use Information

- Manage bookings, hires, tenancies, events and facilities.
- Deliver charitable, community, recreational and faith-based activities.
- Respond to enquiries, feedback, complaints and requests.
- Communicate about services and events where permitted.
- Process payments, donations and Gift Aid.
- Administer employment, recruitment, trusteeship and volunteer involvement.
- Maintain safeguarding records and respond to concerns.
- Protect people, buildings, equipment and assets.
- Investigate incidents and support insurance, legal or regulatory matters.
- Meet legal, financial, contractual and governance obligations.
- Review and improve services and operations.

7. Lawful Bases

Depending on the purpose, we rely on one or more of the following:

- Consent.
- Contract.
- Legal obligation.
- Legitimate interests, balanced against individual rights.
- Vital interests.

Where special category data or criminal offence information is processed, we will identify an additional legal condition and apply suitable safeguards.

8. Sharing Personal Information

We share information only where necessary, proportionate and lawful. It may be shared with:

- Employees who need it to perform their duties.
- Trustees for governance, safeguarding, legal or oversight purposes.
- Contractors and service providers acting on our instructions.
- Professional advisers, auditors and insurers.
- HM Revenue & Customs.
- Regulators, local authorities, courts and statutory agencies.
- Safeguarding agencies, emergency services or law enforcement bodies.

We do not sell personal information. Volunteers are not included as routine recipients of other people's personal information.

9. Safeguarding Information

RPCT and RPL may process information relating to safeguarding concerns involving children, young people or adults at risk. It will be handled sensitively, access will be restricted, and it will be shared only where necessary and lawful to protect an individual or meet safeguarding and legal responsibilities.

Safeguarding information will be handled in accordance with RPCT's Safeguarding Policy and safeguarding procedures, with access restricted to those who need the information to carry out their role or legal responsibilities.

Safeguarding records and sensitive incident records must be stored securely in RPCT/RPL's approved digital filing system, with access restricted to authorised personnel on a need-to-know basis. Access will normally be limited to the relevant safeguarding leads, safeguarding trustee, Operations Manager or other authorised senior staff. Such records must not be stored on personal devices, personal email accounts, USB sticks, messaging apps, private cloud storage or any unauthorised system. File names should be clear but should not include unnecessary sensitive personal details. Records must only be shared where necessary for safeguarding, legal obligations, statutory referrals or authorised internal governance. Retention, review and secure deletion must be carried out in line with RPCT's retention schedule, UK GDPR, the Data Protection Act 2018 and this Privacy Policy.

10. CCTV

CCTV operates in certain areas to help protect safety and security, prevent and detect crime or anti-social behaviour, protect RPCT and RPL property and assets, and assist with investigations of incidents, accidents, safeguarding concerns, complaints, insurance matters or legal issues. CCTV will be used only where necessary, proportionate and lawful.

- 10.1 CCTV operation and purpose: CCTV may be used to monitor public and operational areas of Rowheath Pavilion and its grounds where this supports safety, security, safeguarding, incident management, asset protection or crime prevention. CCTV will not be used in areas where individuals would reasonably expect privacy.
- 10.2 Authorised access and review: Access to live or recorded CCTV is restricted to authorised personnel only, including the Operations Manager, nominated senior staff or site leads, and trustees where access is necessary for governance, safeguarding, legal or oversight purposes. CCTV may only be reviewed for a specific and legitimate reason, such as an incident, accident, safeguarding concern, complaint, suspected crime or anti-social behaviour, insurance matter, health and safety concern or legal request.
- 10.3 Downloading footage: CCTV footage must not be downloaded routinely. Footage may be downloaded only where it is required for a specific incident, safeguarding concern, complaint, insurance claim, legal matter, criminal investigation or other lawful purpose. Downloaded footage should be saved directly to the secure SharePoint incident report file wherever possible. If footage is temporarily downloaded to a personal phone because this is necessary in the circumstances, it must be uploaded to the secure SharePoint incident report file as soon as possible and deleted from the personal device immediately after the upload has been completed. CCTV footage must not be retained on personal phones, personal laptops, personal cloud storage, removable media or informal messaging systems.
- 10.4 Recording downloads and reviews: Any review or download of CCTV footage must be recorded in the relevant incident report. The incident report should include the date and time of the review or download, who accessed the footage, the reason for access, the camera or location involved, the incident or reference details, where the footage has been stored, who it has been shared with and the planned deletion date where applicable.
- 10.5 Secure storage and incident reports: Where CCTV footage is downloaded in relation to an incident or concern, it must be attached to or stored with the relevant incident report file in SharePoint, with access restricted to authorised personnel. Downloaded footage will be retained only for as long as it is needed to investigate, manage or resolve the matter, or for as long as continued retention is lawfully required.
- 10.6 Retention: CCTV footage is normally available for review and download for up to 15 days following the recording date. Downloaded footage will be securely deleted once the matter has been investigated and resolved, unless a further lawful or legitimate reason requires continued retention, such as safeguarding, legal, insurance, regulatory or law enforcement requirements.
- 10.7 Sharing CCTV footage: CCTV footage will only be shared externally where lawful, necessary and proportionate. This may include sharing with the police, emergency services, safeguarding agencies,

insurers, legal advisers, local authorities, regulators or individuals making a valid rights request, subject to legal exemptions and the rights and freedoms of others.

10.8 Safeguarding-related CCTV: CCTV footage linked to a safeguarding concern will be handled in line with section 9 of this policy, RPCT's Safeguarding Policy and relevant safeguarding procedures. Access will be restricted and information will only be shared where necessary and lawful to protect children, young people, adults at risk or others from harm.

10.9 Individual rights and signage: Individuals may request access to CCTV footage containing their personal information, subject to identity checks, legal exemptions and the rights of others. RPCT and RPL may refuse or limit disclosure where necessary, including where disclosure would prejudice an investigation, disclose information about another person or conflict with safeguarding, legal or regulatory duties. Signs will be displayed where appropriate to inform people that CCTV is in operation.

11. Data Security

We use appropriate technical and organisational measures to protect personal information against accidental or unlawful loss, destruction, alteration, disclosure, access or misuse. Access is limited according to role and need.

Staff, trustees and authorised users are expected to follow RPCT and RPL's relevant confidentiality, IT security and data protection procedures, including requirements for secure access, appropriate sharing, password protection, device security, record storage and prompt reporting of any suspected data breach.

Safeguarding records and sensitive incident records must also be handled in line with the additional storage, access and sharing requirements set out in section 9 of this policy.

12. Data Retention

Personal information is retained only for as long as necessary for the purpose for which it was collected and to meet legal, financial, contractual, insurance, safeguarding and regulatory requirements. Retention periods vary according to the record and reason it is held. CCTV is handled under section 10. Safeguarding records and sensitive incident records must also be retained, reviewed and securely deleted in line with RPCT's Safeguarding Policy, safeguarding procedures and retention schedule. RPCT and RPL will keep retention arrangements under review and may develop more detailed retention guidance for specific categories of records where needed.

13. International Transfers

Where information is transferred outside the United Kingdom, we will use an appropriate lawful transfer mechanism and safeguards required by data protection law.

14. Your Rights

- To be informed.
- To request access.
- To request correction of inaccurate or incomplete personal information.
- To request erasure where applicable.
- To request restriction in certain circumstances.
- To object in certain circumstances.
- To request data portability where applicable.
- To withdraw consent where processing relies on consent.
- To complain to the Information Commissioner's Office.

Rights may be subject to legal conditions and exemptions. We may verify identity before responding.

Requests to exercise data protection rights should be made to the Operations Manager using the contact details in section 17. RPCT and RPL will respond within the timescales required by data protection law, subject to any legal extensions or exemptions.

15. Children and Young People

We take particular care when processing children’s information, including providing clear information, obtaining consent where required, restricting access and acting in accordance with safeguarding duties, the child’s best interests and RPCT’s Safeguarding Policy. Any safeguarding-related information will be handled in line with section 9 of this policy and our safeguarding procedures.

16. Personal Data Breaches

Actual or suspected loss, unauthorised disclosure, access, alteration or destruction of personal information must be reported promptly to the Operations Manager. RPCT and RPL will respond to personal data breaches using the following process:

- 16.1 Report the breach promptly to the Operations Manager, including what happened, when it happened, what information may be involved and who may be affected.
- 16.2 Take immediate steps to contain the incident where possible, such as recovering information, changing access permissions, securing devices, stopping further disclosure or asking unintended recipients to delete information securely.
- 16.3 Assess the incident, including what personal information is involved, whether sensitive or safeguarding-related information is affected, who may be impacted, the likely risk to individuals and any legal, financial, insurance or reputational implications.
- 16.4 Record the breach internally, whether or not it is reportable to the Information Commissioner’s Office, including the facts of the incident, the assessment made, decisions taken and actions completed.
- 16.5 Escalate serious incidents, safeguarding-related breaches, incidents involving sensitive information, or breaches that may significantly affect individuals or the organisation to the appropriate trustees.
- 16.6 Notify the Information Commissioner’s Office where required by law, without undue delay and, where feasible, within 72 hours of becoming aware of the breach.
- 16.7 Report serious incidents to the Charity Commission where required, in line with trustee responsibilities and Charity Commission guidance.
- 16.8 Inform affected individuals where required by law or where this is necessary to help protect them from harm or further risk.
- 16.9 Review the incident afterwards and take appropriate action to reduce the risk of recurrence, including updating procedures, staff guidance, training or security measures where needed.

17. Governance and Contact

The RPCT Operations Manager coordinates data protection matters for RPCT and RPL. The trustees retain appropriate governance oversight. Questions, rights requests and concerns should be directed to:

RPCT maintains registration with the Information Commissioner’s Office where required. The current registration details should be checked regularly and updated where necessary as part of data protection governance.

Individuals may also complain to the Information Commissioner’s Office. A copy of this policy will be available on our website and may be requested from the Operations Manager.

Operations Manager
Rowheath Pavilion Christian Trust
Rowheath Pavilion, Heath Road
Bournville, Birmingham B30 1HH
Email: info@rowheathpavilion.co.uk
Telephone: 0121 458 1711

18. Policy Review

This policy will be reviewed annually and sooner where legislation, regulatory guidance, organisational activities, systems or data-processing practices change significantly. Material changes will be approved through the appropriate governance process.

19. Trustee Approval

Approved by the Trustees of Rowheath Pavilion Christian Trust on behalf of RPCT and Rowheath Pavilion Limited.

Chair of Trustees	Wendy Sorby
Signature	signed on behalf of WS
Date	3/9/2026
Review Date	1/8/2027