



G-Cloud Service Definition Document – PACER

This document provides key information about the Planning Application Carbon Evaluation and Reduction (PACER) software service, as required under the terms of the G-Cloud 15 framework.

For further details about Preoptima or PACER, please see preoptima.com/pacer or contact us at pacer@preoptima.com.

PACER has been developed in collaboration with the



City of Westminster

and funded by



**Funded by
UK Government**



**Innovate
UK**



Department for
Energy Security
& Net Zero



Department
for Environment
Food & Rural Affairs

Service overview

PACER (Planning Application Carbon Evaluation and Reduction) is a web-based Software as a Service (SaaS) platform that supports Local Planning Authorities (LPAs) to manage and review Whole Life Carbon Assessment (WLCA) submissions within planning workflows.

PACER provides structured data capture, configurable checks and review outputs, officer feedback workflows, and exportable records to support consistent review and audit.

PACER is delivered as a multi-tenant service hosted on Amazon Web Services (AWS).

Introduction to PACER and Preoptima

PACER is developed and maintained by [Preoptima](#), a science-driven software provider focused on reducing the whole life carbon impact of the built environment. PACER's Minimum Viable Product (MVP) was developed in collaboration with [Westminster City Council](#) and **36 other local authorities and public sector organisations**, informed by input from over **40 industry organisations**.

PACER has been funded through [Innovate UK](#), with support from the [Department for Energy Security and Net Zero \(DESNZ\)](#) and the [Department for Environment, Food and Rural Affairs \(Defra\)](#), to strengthen whole life carbon compliance in planning.

PACER is designed specifically for local government teams that need a practical, repeatable process for handling WLCA submissions alongside existing development management systems. It is designed to facilitate case officer reviews, providing a dedicated workspace for WLCA information, review outputs, and communications with applicants.

Why PACER is needed

Whole life carbon requirements add a new layer of technical complexity to planning. LPAs are expected to review evidence, challenge submissions where needed, and maintain a clear audit trail — often with limited specialist capacity and inconsistent submission formats.

Common pressures include:

- Time and workload pressure on planning and sustainability teams
- Inconsistent formats and variable quality of submitted WLCAs and supporting evidence
- Inability to understand or challenge technical assessments
- Difficulty providing clear, timely feedback to applicants and tracking responses
- Need for transparency and auditability (including internal assurance and information requests)
- Need for programme-level visibility to inform reporting and policy refinement

What PACER does

PACER provides a structured workflow from case set-up through submission, review, feedback (iterative), and export. It enables LPAs to:

- Create and manage WLCA review cases and maintain version history
- Invite applicants/agents to submit (where the Applicant Portal is enabled)
- Collect key WLCA inputs in a structured form and validate completeness against configured requirements
- Run configurable compliance checks and generate clear review outputs (for example pass/warn/flag indicators, where applicable)
- Record check-specific comments and requests for clarification, and track applicant responses
- Export case summaries and programme-level datasets to support decision records, reporting, and audit

Typical workflow

A typical PACER workflow is:

1. A case officer creates a case/project record in the LPA Portal and (where enabled) invites an applicant/agent to submit. Invitations are sent by email.
2. The applicant completes the submission via the Applicant Portal, providing required information and uploading supporting documents where applicable.
3. PACER validates required fields and highlights missing or invalid information according to the buyer's configured requirements.
4. Officers review configured outputs alongside evidence and record comments/requests for clarification within the case record.
5. Officers send comments back to the applicant and can request a resubmission, if needed.
6. The applicant responds and resubmits (where requested), with PACER retaining version history and an audit trail of actions and outcomes.
7. Officers export a case summary/report and/or tabular outputs to support decision records, reporting, and audit. Applicants export an application summary for planning records.

Technical requirements

PACER is a web-based service accessed through a browser (HTML5 web application). No installation is required.

A modern web browser is required. Supported browsers are:

- Chrome
- Safari
- Edge
- Firefox

PACER uses a responsive design and can be accessed on desktop and tablet devices. A desktop or laptop is recommended for the best user experience.

Hosting and resilience

PACER is hosted on AWS. Operation and maintenance of the service is handled by Preoptima; customers do not need to perform installation or maintenance activities.

The service is designed for resilience, including:

- Redundant deployment across multiple Availability Zones
- Monitoring and alerting for availability and performance
- Controlled deployments and rollback procedures

Backups, restore and disaster recovery

Production data is backed up automatically. Backups are retained for a defined period and can be restored to support recovery from data loss or service incidents.

Restore procedures are documented and restore testing is performed to validate recovery processes.

Planned maintenance is managed to minimise disruption. Where downtime is required, customers are notified in advance and work is typically scheduled outside normal working hours where practicable.

Security

PACER is designed for Local Authorities and other public bodies. Security is a core design principle, informed by UK best practice and the National Cyber Security Centre's Cloud Security Principles.

Key security measures include:

- All user access requires authentication and role-based permissions
- Tenant separation to ensure customer data is logically segregated
- Encryption in transit (TLS 1.2 or above)
- Encryption at rest using AWS-managed encryption
- Least-privilege access controls for administrative functions and operational support
- Logging and monitoring, including audit trails for key actions and privileged operations
- Vulnerability management and patching as part of ongoing service operation

Further information on security controls and assurance evidence can be provided to buyers under a Non-Disclosure Agreement (NDA) where required.

Service scope

PACER includes:

- Secure web application access over HTTPS
- LPA Portal for managing and reviewing cases
- Applicant Portal for submissions, responses and resubmission (where enabled)
- Configurable checks and review outputs
- In-platform commenting and feedback workflow
- Reporting and exports for case and programme data
- Tenant administration (user management and configuration options)
- REST API (where enabled for the buyer)
- Support via email/helpdesk and agreed escalation routes
- Online training /workshops

PACER does not include:

- Authoring or assurance of third-party documents submitted by applicants (for example PDFs or spreadsheets), including their accessibility
- Dedicated private connectivity (for example PSN/VPN) unless separately agreed
- Buyer-specific security documentation or audits beyond what is provided as standard
- On-site training/workshops unless explicitly included in the order
- Bespoke integrations, custom reporting, or non-standard feature development
- Data migration/cleanup beyond standard onboarding support

Service constraints

There are no special constraints beyond those described in this document.
Key constraints are:

- A modern web browser is required (Chrome, Safari, Edge, Firefox)
- File upload and export sizes are subject to configured limits
- PACER does not remediate accessibility issues in third-party documents uploaded by users

Service levels and support

Availability and support are defined in the contract.

The standard monthly availability target for the production service is **99.0%**, measured over each calendar month (excluding pre-notified planned maintenance, emergency maintenance, and events outside the supplier's reasonable control).

Support is provided via **email/helpdesk during Mon–Fri UK business hours 09:00–17:30**, with an agreed escalation route for high-severity incidents.

Support includes:

- Access and user administration support for buyer administrators
- Guidance on the use of the platform and exports
- Incident handling and communications during outages or degradation
- Provision of incident reports on request (impact, root cause, corrective actions)

Outage and maintenance management

Outages and service degradation are communicated to buyer contacts by email (incident acknowledgement, impact and updates). In-service notifications may be used where appropriate.

A status page and/or status endpoint can be provided where agreed/required. Post-incident reports are available on request.

Onboarding and offboarding

PACER is delivered as a web-based service with no installation required. Onboarding focuses on enabling teams to use the service effectively.

Onboarding typically includes:

- Tenant set-up and initial configuration (as applicable)
- Administrator enablement and user provisioning guidance
- Support with agreed workflows (case set-up, review stages, reporting/export routines)
- Remote familiarisation and platform training session(s) as included in the order

Offboarding and exit support includes:

- Support for exporting buyer data in standard formats (for example CSV/JSON and report exports where available)
- Guidance on exporting evidence and case records (subject to user permissions)
- Data deletion from production systems on termination or upon request, subject to contractual retention requirements

Access to data (upon exit)

At the end of the contract, the buyer may request a transfer of their data held within PACER in a usable format, at no additional cost (subject to contract terms).

Once transfer has been completed (or after any applicable retention period), customer data is securely deleted. Backups and snapshots expire in line with configured retention periods.

Contact

For service enquiries, onboarding, or support, contact:

pacer@preoptima.com.