OPIA

Vouchers & Prepaid Cards, Digital Prepaid Cards, Reward Platforms

Service Definition

Contents

Service Overview

What Opia Offers

Opia provides a fully managed payout solution to distribute Vouchers and PrePaid Cards to citizens and end users.

» Digitally led requisition process, with human support

» Validation and Fraud process embedded as standard.

» Direct to Digital Wallet to allow for rapid provision of funds

» Opia offer a platform to disburse:

- Prepaid Cards to Digital Wallet
- Vouchers and Prepaid card via email
- BACS transfers to verified end users.

What Opia Offers

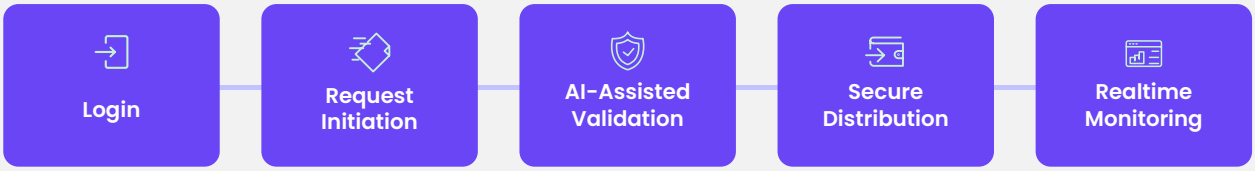
Opia provides a secure, end-to-end managed service for the distribution of financial support, vouchers, and prepaid cards to citizens and businesses. We combine robust financial infrastructure with a user-centric digital platform to manage the entire lifecycle of disbursement programmes. Our solution is designed for government departments and local authorities requiring the efficient distribution of funds (e.g., Household Support Funds, welfare vouchers, and grant schemes) while ensuring rigorous compliance and financial control

We offer a flexible solution capable of issuing cash directly to bank accounts, digital e-vouchers, utility vouchers, and physical prepaid cards. This service embeds market-leading AI fraud prevention to protect public funds while delivering an intuitive, accessible user journey that supports digital inclusion.

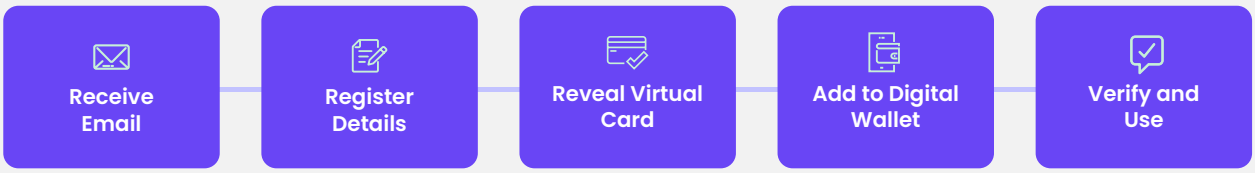
The solution enables direct provision of vouchers direct to Digital Wallet to allow for rapid fund availability to any user that requires urgent support.

The Digital Journey

Distributing funds



Receiving funds



Key Features

We offer a fully managed service to enable our clients distribute Prepaid Cards, Vouchers and Cash (BACS Transfer) accurately and to policy.

Our solution offers:

- **Multi-Channel Disbursement:** Flexible issuance of support via automated BACS transfers (Direct to Bank), digital e-vouchers (email/SMS), and physical prepaid cards or vouchers for offline redemption.
- **Embedded AI Fraud Prevention:** Integrated bank-grade fraud detection (ThreatMetrix®) using AI and behavioural biometrics to analyse digital identities, device fingerprints, and geolocation to generate risk scores and prevent synthetic ID fraud.
- **Secure Financial Management:** Management of ring-fenced client accounts with automated payment processing. We process payment files within one working day of validation, ensuring a typical 3-day payment cycle.
- **User-Centric Digital Portals:** Configurable, WCAG 2.1 AA compliant portals allowing citizens to register, claim, and track vouchers via mobile, tablet, or desktop.
- **Digital Inclusion Support:** Processes to support digitally excluded residents, including printable PDF vouchers and telephone-assisted application routes supported by UK-based agents.
- **Real-Time Budget Control:** Interactive dashboards providing live management information on spend, voucher redemption rates, and remaining budget allocation per department or scheme.
- **Comprehensive Validation:** Hybrid workflows combining automated checks (bank verification, address look-up) with manual review by expert teams to verify eligibility before funds are released.

Our Platform includes:

- Intuitive Web Interfaces
- Omnichannel Citizen and User Accessibility
- Global Support Capabilities
- Claim Workflow Digitisation
- Automated Decision Making
- AI Driven Fraud Detection
- Digital & Physical Goods Payment Solutions
- Returns and Dispute Management
- Fully Managed Service
- 24/7 platform access
- Website design to client guidelines
- Website development and build and hosting
- SSL (Secure Sockets Layer)
- SFTP Server and payment fulfilment file integration
- User acceptance and vulnerability testing
- Legal compliance
- Telephone line set up and Email set up
- Qualifying Documents and Help videos on site

Key Benefits

Our solution is designed to support government departments, local authorities, and public bodies in distributing funds efficiently to citizens and businesses.

Rapid Provision of Funds: We understand that fund provision can require urgent attention.

Fraud Reduction: Protecting Public Funds is a critical part of our objective when working with our clients. We maintain fraud rates of less than 1%, which is well below industry standard.

Significant Cost Savings: Our automation-first approach delivers substantial efficiencies. Our solutions enable a **+70% automation rate** for claims and requests, which leads to a **40% cost saving compared to traditional people-based processes.**

Operational Agility: We offer rapid mobilisation, capable of deploying complex schemes within 4 to 10 weeks, reducing "time to serve" from weeks to days.

Enhanced User Experience: We deliver intuitive, personalised journeys that foster satisfaction, evidenced by a 96% end-user satisfaction rate on government contracts.

High Scalability: Our infrastructure and resourcing models are designed to manage over 100,000 claims monthly, with the ability to scale rapidly to meet policy announcements or seasonal demand.

The Right Level of AI for You: As part of our onboarding process, we discuss your objectives to find you the right product which blends the best levels of automation, human involvement and AI to best meet your citizen and users' needs.

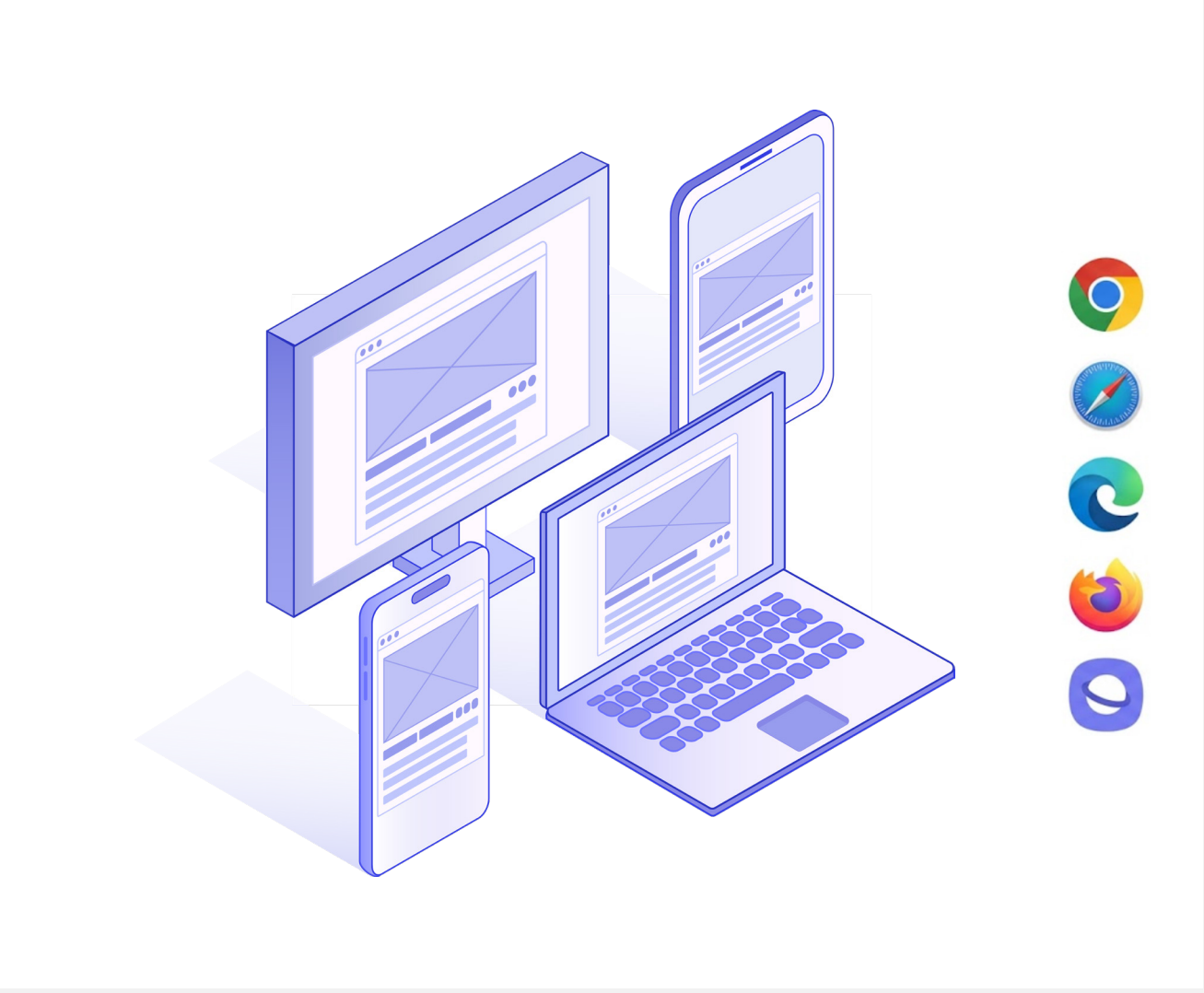
Technical Capability

Browser Compatibility

Opia's web portal solution is engineered to operate seamlessly across all modern web browsers, including Google Chrome, Microsoft Edge, and Safari, ensuring broad accessibility for all users.

Designed with a responsive interface, the platform functions effectively across all standard device types, adapting to PCs, laptops, mobiles, and tablets to maintain consistent usability regardless of screen resolution.

To uphold these standards, Opia conducts rigorous cross-browser and device compatibility testing, validating performance across supported operating systems and hardware to guarantee a robust and user-friendly experience.



How We Work With You

Onboarding

Opia utilises a structured, agile implementation methodology to enable rapid service mobilisation, typically achieving deployment within 4-to-10-weeks depending on scheme complexity. Our approach minimises risk and ensures operational readiness from Day One, underpinned by our ISO 9001 (Quality Management) and ISO 27001 (Information Security Management Systems) accredited processes.

Opia's fully managed solutions begin before contract launch date and starts with understanding your team and company objectives. We will mutually agree and guide your team through the following key milestones to ensure a reliable onboarding:

- Implementation and Transition Plan
- Communications Plan
- Continuous Improvement Plan
- Risk Management Plan (Risk Register)
- Fraud-Specific Risk Assessment
- Test Plan
- Opia Compliance Table
- Quality control
- Opia Implementation and Service Delivery Team Profiles

Onboarding

Mobilisation & Discovery

Upon contract award, we appoint a dedicated cross-functional team including a Project Manager, Technical Lead, and Account Director. We conduct discovery workshops to define requirements, eligibility criteria, and reporting needs, producing a detailed Solution Design and Project Initiation Document (PID)

Configuration & Build

We configure the Opia Cloud platform to your specific requirements, including the setup of Multi-Factor Authentication (MFA), AI fraud rules, and data integration protocols. For our clients who are migrating existing schemes, we offer our “Adopt and Innovate” strategy to migrate services with zero disruption

Testing & Assurance

We apply a rigorous testing strategy including User Acceptance Testing (UAT), regression testing, and security penetration testing by CREST-certified partners. We ensure all digital portals meet WCAG 2.2 AA accessibility standards prior to launch

Training & Go-Live

We provide comprehensive training materials and webinars for your staff. We operate a “hyper-care” period post-launch to ensure stability and rapid resolution of early-life queries

Account Management

Governance Structure

We view our relationship with buyers as a long-term strategic partnership. Each client is assigned a dedicated Senior Account Director as the primary point of contact, supported by an Executive Sponsor who provides senior-level oversight, escalation support and accountability. A dedicated Service Delivery Manager is responsible for day-to-day performance, ensuring services operate in line with agreed service levels, policies and controls. This role focuses on operational stability, issue resolution and continuous service quality. We operate a tiered governance model including weekly operational calls, Monthly Performance Reviews to track SLAs/KPIs, and Quarterly Business Reviews (QBRs) to discuss strategic roadmap and innovation.

Real-Time Reporting

Clients are provided with 24/7 access to interactive Microsoft Power BI dashboards, offering live insights into claim volumes, spend, fraud prevention rates, and customer satisfaction scores. In addition to operational metrics, we provide insight to the key benefits and outcomes, supporting evidence-based reporting on value for money and service impact.

Continuous Improvement and Innovation

We maintain a live Continuous Improvement Plan, actively soliciting feedback to implement enhancements such as process automation or new self-service features. We hold regular workshops internally and with our clients to share new ideas, services and process. These are designed to offer you the latest improvements to maintain our commitment to push boundaries and exceed your expectations.

Risk, Compliance and Audit Oversight

We provide named leads for risk management, data protection and compliance, ensuring adherence to statutory, contractual and security requirements. Regular audits, control testing and risk reviews support transparency and assurance.

User Support

For Citizens and End Users:

Account and User Support: Opia delivers a multi-channel, human-centric support service designed to handle fluctuations in demand while ensuring accessibility for all users of all abilities. Our support services are Cyber Essentials Plus certified and staffed by highly trained experienced UK-based teams.

For the Buyer (Account Support)

We are an agile company and understand the benefits of having a responsive dedicated team at all levels assigned to support you. Your Account Director and operational team are available for on-demand support, rapid issue resolution, and strategic consultation. We operate an agile escalation route up to Director level to resolve critical issues within the agreed service levels.

For the End User (Citizen Support):

- **Multi-Channel Access:** Support is available via Telephone, Email, Web Chat, and Post. We offer extended hours (e.g. 9:00 am – 7:00 pm) to suit citizen needs.
- **Digital Inclusion:** We support digitally excluded users through paper-based applications, offline voucher distribution, and proxy support for vulnerable citizens.
- **Accessibility & Language:** Our support includes translation services for non-English speakers (including Welsh language schemes) and is optimised for users with accessibility needs.
- **Service Levels:** We adhere to strict SLAs, defined and agreed with each of our Clients, targeting 80% of calls answered within 45 seconds and 98% of emails processed within 2 working days. Our ethos is to deliver a service to achieve your desired outcomes, we can be flexible and deliver to meet your goals.

Termination Process

Termination and Contract Exit Process

Opia's termination process is fully aligned with the Call-Off Contract and associated Framework Agreement terms, ensuring transparency, fairness and consistency for the contracting authority. Termination rights, notice periods and obligations are applied strictly in accordance with the contract.

Notice and Formal Notification

Upon receipt or issue of a termination notice (whether for convenience, expiry or cause), we formally acknowledge the notice and confirm the effective termination date, notice period and exit obligations. All actions are documented to ensure clarity and auditability.

Exit Plan Activation

The agreed Exit Management Plan is immediately activated following notice of termination. This plan has been maintained throughout the contract lifecycle and is designed to support an orderly, controlled transition with no avoidable disruption to service users.

Governance and Oversight

A Joint Exit Board is established, comprising senior representatives from Opia and the contracting authority. The Exit Board provides oversight of the exit process, agrees priorities, manages risks and ensures contractual and statutory obligations are met.

Below the Exit Board, an operational exit team manages day-to-day delivery, reporting progress, issues and dependencies.

Service Continuity During Run-Off Period

During the run-off period, Opia continues to deliver services in line with agreed service levels, security controls and data protection requirements. No changes are made that could adversely impact service performance, data integrity or user experience without client approval.

Knowledge, Data and Asset Handover

We support the structured handover of service knowledge, documentation, data and assets to the contracting authority or incoming supplier. This includes:

» Transfer of data in agreed open formats
» Provision of operational documentation and process materials
» Knowledge transfer sessions to ensure continuity of delivery

All handover activities are conducted securely and in line with UK GDPR and information security requirements.

People and Resource Transition (Where Applicable)

Where relevant, Opia cooperates fully with any applicable staff transfer or workforce transition arrangements, supporting continuity of expertise and compliance with contractual and statutory requirements.

Information Security and Data Protection

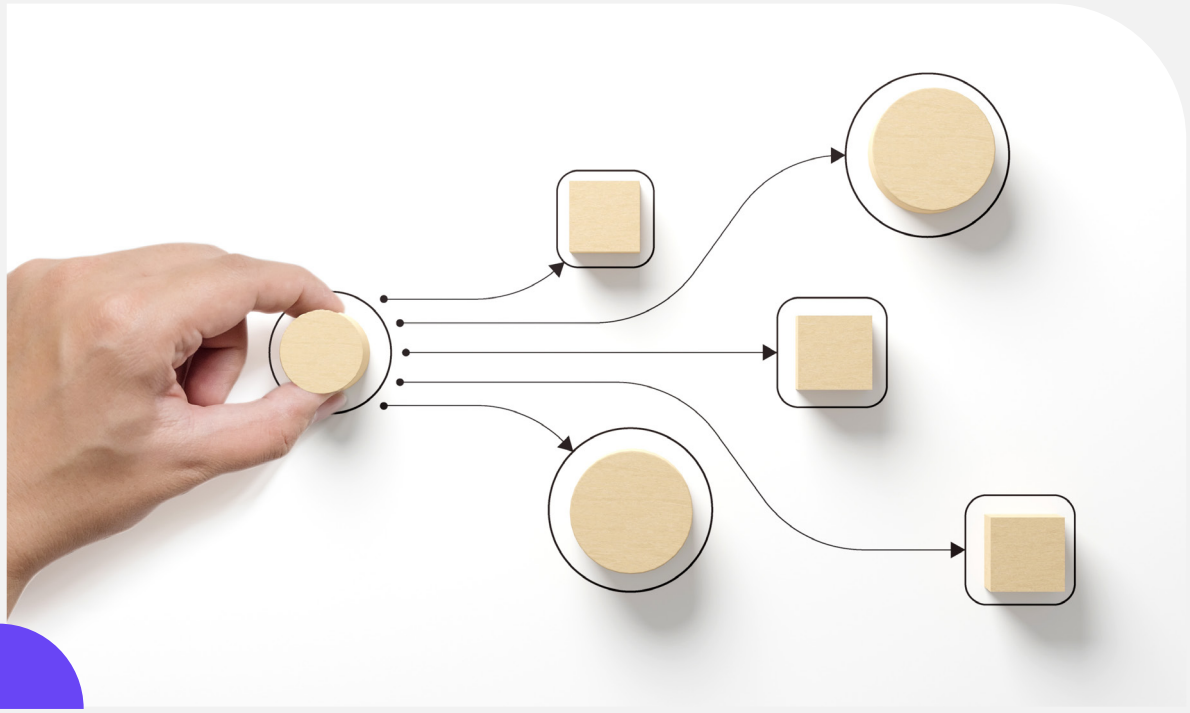
Throughout the termination and exit period, Opia continues to apply full information security controls in line with ISO 27001, the Security Policy Framework and UK GDPR. Access controls remain in place until final handover is completed.

Exit Completion and Assurance

On completion of the exit process, we provide formal confirmation that all contractual exit obligations have been met. Any remaining client data is securely deleted in accordance with agreed retention schedules, with certificates of destruction provided as assurance.

Dispute Resolution and Contractual Compliance

Any issues arising during termination are managed in accordance with the dispute resolution and escalation provisions set out in the Call-Off Contract, ensuring a fair and controlled approach.



Offboarding

Opia maintains a comprehensive Exit Management Plan throughout the contract lifecycle to ensure that, should the service end, the transition to a new supplier or in-house team is seamless, secure, and compliant with ISO 27001 (Information Security) and UK GDPR requirements standards.

Exit Governance and Oversight

At the agreed date before Contract expiry (or at termination of agreement), the Exit Management Plan is activated and an Exit Manager is appointed as the single point of coordination.
Clear governance arrangements are established, including regular progress reporting, risk management and escalation routes, ensuring transparency and control throughout the exit period.

Service Continuity During Exit

During the exit and run-off period, Opia continues to deliver services in line with agreed service levels, security controls and data protection requirements. No material changes are made to systems, processes or resourcing without client agreement, ensuring stability until transition is complete.

Risk, Compliance and Assurance

Exit activities are managed in line with Opia's information security, data protection and risk management frameworks. Regular checks are undertaken to ensure ongoing compliance with contractual, statutory and security obligations throughout the exit process.

- Data Migration: We securely extract and transfer all service data, transaction history, and user accounts in agreed open formats (e.g., CSV, SQL) using secure protocols (SFTP/AWS S3). We ensure data integrity is validated with you before final handover.
- Knowledge Transfer and Documentation: We provide full operational handbooks, asset registers, and knowledge transfer sessions to the incoming provider to ensure business continuity.This includes service handbooks, process maps, asset registers and configuration details. Structured knowledge transfer sessions are delivered to the incoming provider or internal team to ensure a smooth handover and minimise service disruption.
- Secure Data Destruction: Upon completion of the exit period, all client data remaining on our systems is securely deleted in accordance with UK GDPR and our Data Retention Policy, with certificates of destruction provided.
- People and Capability Transfer (Where Applicable)

Where services involve dedicated resources, we support an orderly transition of knowledge and capability, including cooperation with any applicable staff transfer arrangements. This ensures continuity of expertise and maintains service quality for users.

Pricing

Initiation

To explore our offerings or to commission Opia for your upcoming projects, please contact our team at tender@opia.com.

Our engagement model begins with a collaborative discovery session. Rather than simply taking an order, we arrange a consultation to fully understand your specific landscape and requirements.

Following this, if needed, Opia will generate a comprehensive proposal outlining our suggested methodology, key deliverables, and projected timelines.

Contracting and Frameworks

Once we are ready to formalise the partnership, we will proceed to the order stage using the standard call-off contract. To ensure absolute clarity, Opia provides a detailed Statement of Work (SoW) alongside the contract. This document serves as a blueprint for the project, aligning both parties on the exact approach and expected outcomes before work commences.

Contract Duration

Our standard engagement typically runs for a minimum term of 12 months, effective from the initiation of the work, subject to final agreement.

Commercial Structure & Pricing

We understand that modern projects require agility. Therefore, Opia's commercial model is designed to be flexible yet secure. While our pricing adapts to the specific nuances of your requirements, it remains anchored within a fixed commercial framework.

We typically operate an activity-based costing approach, which can be banded or variable. Fixed Fee options are also available given the specific requirements of your work.

This ensures you have the flexibility to adjust scope where necessary without losing sight of budget certainty and cost control.

We typically structure our costs in one of two ways:

- Variable Costs (per unit): Ideal for projects where scope and volume may change through the contract. We provide a breakdown of transaction rates for transparency.
- Fixed Price: For projects with a strictly defined scope, we can provide a fixed quote to guarantee a set cost for specific deliverables. This will fall within one of our standard packages based off complexity.

Clients who require bespoke customisation of our platform may benefit from a hybrid model of the above, consisting of a Fixed Fee, with ongoing Variable Costs.

Data Security

Data Protection

Data Security

Opia is certified to ISO 27001:2022, the recognised international standard for Information Security Management Systems (ISMS). Our comprehensive security framework ensures that we adhere to the principles of confidentiality, integrity, and availability across all statutory functions.

Our security approach includes:

- Access Control: Robust logical access controls managed by IT and Digital teams, ensuring access is granted only on a need-to-know basis,.
- Vulnerability Management: We perform regular vulnerability scans of applications and networks, alongside annual penetration testing of our platforms and frameworks by independent security agencies.
- Encryption: We utilise encryption at rest for sensitive data (including PII) and encryption in transit (HTTPS/SFTP) for information transfer. Secure Development: Our software development lifecycle incorporates security reviews, peer code reviews, and automated testing within secure development environments.
- Physical Security: Strict access controls, including key fobs and supervised visitors, are enforced at our UK locations.

People Security, Training and Compliance

Pre-Employment and Onboarding Controls:
All staff undergo appropriate pre-employment checks proportionate to their role before accessing systems or data. Security responsibilities are clearly communicated during induction, in line with Cabinet Office people security principles.

Mandatory Security and Data Protection Training:
All staff must complete mandatory information security and data protection training as part of induction. Training covers secure handling of information, recognising security threats, incident reporting and individual responsibilities under UK GDPR and government policy.

Refresher and Ongoing Training:
Refresher training is delivered at least annually, and more frequently where required by changes in policy, risk or service scope. Completion is monitored and enforced.

Role-Based Security Training:
Staff with elevated access or responsibility for sensitive services receive additional role-specific training to ensure appropriate understanding of risks, controls and secure working practices.

Policy Compliance and Assurance:
All staff are required to formally acknowledge Opia's information security, acceptable use and data protection policies. Compliance is monitored through technical controls, access logging, audits and management oversight.

Monitoring, Audit and Incident Management:
Security incidents or suspected breaches are managed through formal incident response procedures, including timely reporting, investigation and corrective action.

Management Accountability and Culture:
Clear accountability for information security is embedded at all management levels. We promote a strong security culture through regular communications, awareness activity and leadership engagement, reinforcing the shared responsibility for protecting government information.

Business Continuity

Opia maintains a Business Continuity and Disaster Recovery Framework designed to ensure the delivery of critical services during disruptive incidents. The plan is owned by the Director of Technology and supported by a **Business Continuity Response Team (BCRT)** comprising senior executives.

Key features of our continuity strategy include:

- Defined Recovery Objectives: Critical systems and services have clearly defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), agreed in line with service criticality and public sector expectations for continuity.
- Scenario-Based Planning: The BCDR Framework covers a wide range of credible scenarios, including:
- Loss of access to physical sites
- Loss or degradation of critical systems
- Cyber security incidents
- Loss of key suppliers or third-party services
- Significant staff unavailability

Each scenario includes defined response actions, escalation routes and recovery steps.

» Resilient Infrastructure: Our production environments are hosted in Amazon Web Services (AWS) Virtual Private Clouds (VPC). Infrastructure spans multiple data centres (Availability Zones), ensuring no single point of failure.
» Redundancy: We utilise load balancers and redundant proxy servers to automatically route traffic away from unhealthy instances.
» Scenario Planning: The framework covers various scenarios including loss of physical site access, loss of critical systems, and loss of key suppliers.
» Remote Working: As a primarily remote/home-working enabled business, staff can
» operate effectively off-site using secure VPNs and cloud-based tools (Office 365) in the
» event of office inaccessibility.
» Testing: We conduct annual testing of disaster scenarios, including database recovery and site failover, to ensure processes remain fit for purpose.

Data Breaches:

In the event a data breach is suspected or confirmed, the Information Security Team will assess the risks associated with the breach, including:

- what type of data is involved?
- how sensitive is the data?
- who is affected by the breach, ie the categories and approximate number of data subjects involved?
- the likely consequences of the breach on affected data subjects, eg what harm can come to those individuals, are there risks to physical safety or reputation, or financial loss?
- where data has been lost or stolen, are there any protections in place such as encryption or pseudonymization?

Notifying Stakeholders:

In the first instance, given a situation that qualifies for notification, we will contact you (the client) as early as practically possible to inform you of the likely impact and immediate containment and remedial actions.

The Information Security Team will also notify the ICO when a personal data breach has occurred which is likely to result in severe harm and/or a risk to the rights and freedoms of data subjects (such as identity fraud or financial loss). Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after we became aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

Post-Incident Activity

Post-incident activity should be completed by the Information Security Forum, and covers the following areas:

- Review of the incident to confirm, if possible, the validity of the analysis and the effectiveness of the actions taken;
- Assessment of any service, process or procedure changes which may be necessary to prevent or discourage a recurrence of the incident including updating all relevant documentation;
- Consideration of any training or awareness initiatives arising from the incident.

Back Up and Restoration

Opia operates a robust backup and restoration framework designed to protect the integrity, availability and recoverability of data in line with public sector resilience and assurance expectations. Backup arrangements are embedded within our wider Business Continuity and Disaster Recovery framework and are subject to regular review and testing.

- Automated Database Backups: Automated backups for Relational Database Service (RDS) instances are performed nightly. These backups are retained for a minimum of 7 days.
- Server and System backupsServer Snapshots: For domain controllers and critical servers hosted in AWS, native snapshots are taken nightly with a 30-day retention policy.
- High Availability and Failover Capabilities: Database instances are mirrored across multiple Availability Zones. In the event of an instance failure, traffic automatically fails over to the backup instance.
- Recovery Objectives: Clear recovery objectives are defined and aligned to service criticality.In the unlikely event of a non-recoverable outage, our architecture is designed to limit data loss to a maximum of 24 hours.Backup and restoration processes are tested periodically to provide assurance that recovery can be achieved within agreed tolerances.

About Opia

A 20-Year Heritage: Delivering Outcomes vs Outputs

Our ethos is one of mutual value, innovation and partnership. Opia has changed the landscape of sales promotions by putting our clients and their customers at the centre of everything we do.

With unique, imaginative and long-lasting campaigns, we create excitement, loyalty and encourage engagement. Our ingenious, customised promotions can eliminate the need for costly discounting, improving affordability and offering a smart alternative to our clients – we deliver true business outcomes.

Lenovo

A 12-year strategic partnership that has delivered a 30%+ sales uplift, **40% cost savings**, and a **<1% fraud rate**. This is all achieved through a fully managed service model combining people, process, and technology

SAMSUNG

Automated **>80% of claims** and customer journeys, with a projected **40% cost saving** compared to conventional people-based processes.

Carrefour

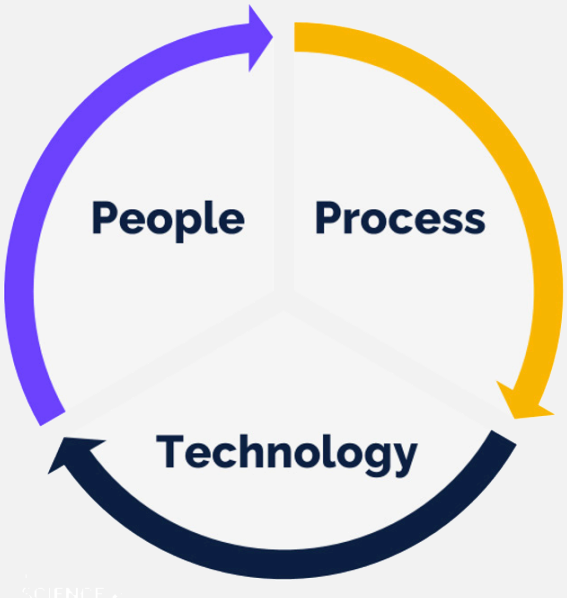
Achieved a **98% influence rate** with **50% of customers** citing their low-friction experience as driving their behaviour

A new 2025 partnership

A new 2025 partnership that has already delivered 'turn the dial' outcomes, including a +25% sales uplift, **£1m in cost savings** (versus discounting), and a **20% market share steal** from direct competitors.

Our Operating Model

Opia's solutions are built on a powerful synergy of human expertise, streamlined processes, and cutting-edge technology. The unique combination is engineered to deliver a seamless and personalised redemption journey for your customers, turning every promotion into a positive brand touchpoint.



People: Our dedicated in-house teams are an extension of your business. This includes specialists in fraud prevention, customer service, development, and insurance, all working together to delivery on your objectives.

Process: We apply intelligent workflow and automation to streamline complex journeys, ensuring a frictionless experience for both customers and your internal teams. Our lean processes are designed for efficiency and accuracy.

Technology: Our digital-first platforms, powered by AI and robust back-end systems, provide the technical foundation for scalable and secure solutions. Real-time tracking and reporting provide full transparency and control.

Some of Our Clients

What Our Customers Say

> They are very flexible and I don't think we are the easiest business to work with, as we are dynamic and fast-paced and we change things at the last minute but they are endlessly flexible and accommodating to us, so that's a real strength.

Samsung
Nationwide Redemption Scheme

SAMSUNG

> OPIA consistently deliver great service. They take the time to understand our business and tailor solutions to suit our needs and those of our members, delivering genuine value. Their responsiveness, transparency, and thoughtful approach make them a trusted and valued partner.

Blue Light Card, Staff Engagement Scheme

BLUE LIGHT CARD

> What sets them apart is their hands-off, full process management, handled with professionalism and expertise. We consider Opia to be a trusted partner and a crucial part of our strategy, consistently adding value to achieve our business objectives. I wouldn't hesitate to recommend them.

Stuart Wright, PC & Smart Device Director, Lenovo

Lenovo

Accreditations

Opia holds comprehensive accreditations that validate its commitment to security and operational quality. The organisation is certified to ISO/IEC 27001 and ISO/IEC 27002, ensuring its Information Security Management System (ISMS) adheres to strict international standards for data protection. Additionally, Opia holds Cyber Essentials Plus certification and operates a Quality Management System accredited to ISO 9001 to underpin its continuous improvement and service delivery. We are committed to achieving our environmental goals and are accredited to ISO14001. We have a published Carbon Reduction Plan (https://www.opia.com/wp-content/uploads/2025/10/Opia_Ltd_Carbon_Reduction_Plan_2025.pdf). This plan is overseen by a nominated individual with the business and supported by Board level backing.

Culture and Values

One Opia: We break down silos and build each other up. Collaborating selflessly across teams, roles and regions to do what's best for the whole business, not just our piece of it.

People Always, Thrive In and Out of Work: We look after each other and ourselves, valuing our diversity, our wellbeing and belonging. We care about the world beyond our walls, doing right by our communities and the planet… And we make it fun! Celebrating the wins, sharing the laughs and enjoying the journey together.

Progress over Perfection. Growth is our Mindset. Compliance and legislation are non-negotiable, but progress means taking responsible steps forward, even as we refine and improve.

Client-obsessed. Exceed Expectations, Every Time. We listen deeply, act boldly and deliver results that exceed expectations, solving real problems and creating lasting impact for our clients and their customers.

Trust first: We earn trust through honesty and respect.

Own Your Impact. Be Accountable, Elevate Opia. We own our choices, keep our commitments, step up when it matters and deliver with pride, knowing our work powers the success of everyone at Opia.

Social Value

Opia aligns its social value strategy with the UK Social Value Model, specifically focusing on creating employment opportunities for those facing barriers (MAC 2.2) and supporting educational attainment to address skills gaps (MAC 2.3).

A. Inclusive Recruitment and Employment Practices

- Accessible Recruitment: Job descriptions are reviewed for neutral language and accessibility. The recruitment process focuses on core competencies and transferable skills rather than just traditional qualifications to encourage diverse applicants.
- Bias Minimisation: The company utilises anonymous screening processes and structured interview scoring to minimise unconscious bias.
- Remote and Hybrid Working: Opia operates a remote working model which aids in attracting staff from diverse geographical areas who might otherwise face barriers to accessing opportunities.
- Fair Pay: Opia is committed to ensuring 100% of its workforce receives the Real Living Wage or above. Currently, 78% of the workforce is in receipt of this rate, with regular pay reviews conducted to bridge the gap.

B. Targeted Community Outreach and Partnerships

Opia positions itself as a community-embedded SME, directing its social impact efforts locally, particularly within North Tyneside and areas identified by the Indices of Multiple Deprivation (IMD).

- STEM Learning Partnership: Opia partners with STEM Learning UK to target schools in deprived areas. Activities include donating laptops (targeting 20 per annum) and delivering AI-focused STEM volunteering sessions to students aged 14–16.
- Local Volunteering: The company aims to invest approximately 50% of its total volunteering hours into local community projects in North Tyneside, such as beach cleanups and supporting local food banks.
- Apprenticeships: Opia works with providers like Gateshead Council and Apprentify to upskill teams, prioritising individuals with limited qualifications.

C. Workforce Wellbeing and Development

Internal social value is driven through staff support structures:

- Wellbeing Support: The HR team is trained as workplace Health Advocates. Resources include an online Wellbeing Centre, an Employee Assistance Programme (EAP), and mental health support.
- Employee Holiday Purchase / Sell Scheme. Opia promoted a healthy Life/work balance and has implemented a holiday exchange scheme since 2024.
- Inclusion Networks: An employee-led inclusion network called “Connect” offers peer support and shapes internal policies.
- Mentorship: Opia provides buddy and mentorship schemes to support the career progression of employees from underrepresented backgrounds.

D. Measurement and Governance

- Leadership: Delivery is overseen by the Head of ESG (Samantha Miller), who is responsible for embedding these initiatives.
- Data Collection: Opia collects data on workforce diversity and socio-economic background (e.g., parental occupation) to benchmark against national statistics and identify barriers.
- KPIs: Specific targets include increasing applications from deprived areas by 10% and achieving a ≥80% satisfaction rate among hires from disadvantaged backgrounds

Environmental Impact

At Opia, we believe that sustainability and corporate social responsibility (CSR) are essential for building a better future. We are dedicated to reducing our environmental impact, contributing to social causes, and making a positive

We are holders of ISO 14001 across all operations

We are proud supporters of the trussell trust charity

Opia have globally committed to Net Zero by 2050

Regular volunteer days with ‘charity free days’

OPIA

Mon-Fri,9 am – 6pm

London Office

184, Shepherds Bush Road,
London, W6 7NL

Mon-Fri,9 am – 6pm

Gateshead Office

Baltimore House, Abbots Hill,
Baltic Business Quarter,
Gateshead, Tyne & Wear,
NE8 3DF

Alex Catton | Public Sector Lead

+44 20 8078 4290

Ian Allison | BPO Sales Director

+44 75 8668 2191

publicsector@opia.com