



Service Definition

G-Cloud 15

Contents

e-shot™ is the digital communications platform trusted by the public sector to send highly effective campaigns. Whether it is newsletters to millions or messages to individuals, e-shot gives you a simple solution for sending omnichannel and accessible messaging to your audience.

Introduction

Why e-shot.....	4
Versions.....	5
Limits.....	6
Accounts.....	7
Procuring e-shot via G-Cloud	8

Use Cases	9
Newsletters.....	10
Omnichannel engagement	10
Behaviour change	10
Internal communications	11
Service communications.....	11

Functional Specification

Email campaigns.....	12
SMS campaigns.....	13
Whatsapp campaigns.....	14
CRM.....	15
Design.....	16
Forms.....	19
Analytics	21
Intergrations.....	22

Non functional Specification

Service scope.....	23
User support	23
Support levels	25
How will users work with your service	27
Onboarding and offboarding	28
Data importing and exporting	29
Analytics	30
Scaling	31
Public sector networks	31
Data-in-transit protection	32
Asset protection	33
Availability and resilience	35
Governance	37
Operational security	38
Staff security	41
Secure development	42
Identity and authentication	43
Audit information for users	45
Accessibility.....	47
Onboarding	48
Training.....	48
Account management.....	48
Design	49
Professional Services	49
Custom development.....	50

Why e-shot

e-shot is trusted by a broad range of local authorities, central government departments, emergency services, NHS trusts and many other public bodies to digitally engage with residents, patients, staff and other stakeholder groups. The platform was originally developed to help the National Institute of Clinical Excellence as a secure way to transfer medical guidelines digitally. We have built on that public sector pedigree over nearly a quarter of a century.

Service

We proactively help customers to improve their digital communications whilst making sure we are always available to help when needed – our median support response time is under two minutes! We also provide full and comprehensive training to help councils get the best out of the platform.

Security

Our commitment to security is reflected in strict policies and standards such as ISO 27001 and Cyber Essentials Plus. Every member of the team has passed security. We use gov.uk and nhs.uk domains to send messages and host content – this ensures communications from the platform are highly trusted

Simplicity

Creating highly engaging campaigns is easy with e-shot. Our tools have been designed to efficiently enable users to do both the basics and brilliantly sophisticated campaigns in one, comprehensive platform. We put a strong emphasis on accessibility and user experience in everything we do.

Police officers and public servants with no prior marketing experience use it just as confidently as communications professionals. Our user interface is fully accessible, and we provide training to customers to help them ensure their campaigns are highly effective.



Versions

There are three versions of e-shot to choose from with increasingly sophisticated functionality and higher limits on some functions.

Basic

e-shot basic provides a comprehensive email platform with CRM, forms and analytics. It provides a fully functional newsletter solution.

Pro

e-shot pro adds automation and SMS capabilities along with higher limits for functions such as landing pages and website popups.

Omni

e-shot omni adds WhatsApp and Microsoft Teams to the channels through which you can send campaigns, providing a true omni-channel solution.

"We had 73% of the database resubscribe for garden waste collections, it generated for the council approximately £1,800,000 in revenue, we worked out the cost to be £1,300 generated for every £1 spent on the campaign, it was extremely worth while, great to work with e-shot. "

Alan Furguson,

Web Manager

UnAward winner for Best Use of Email in 2026

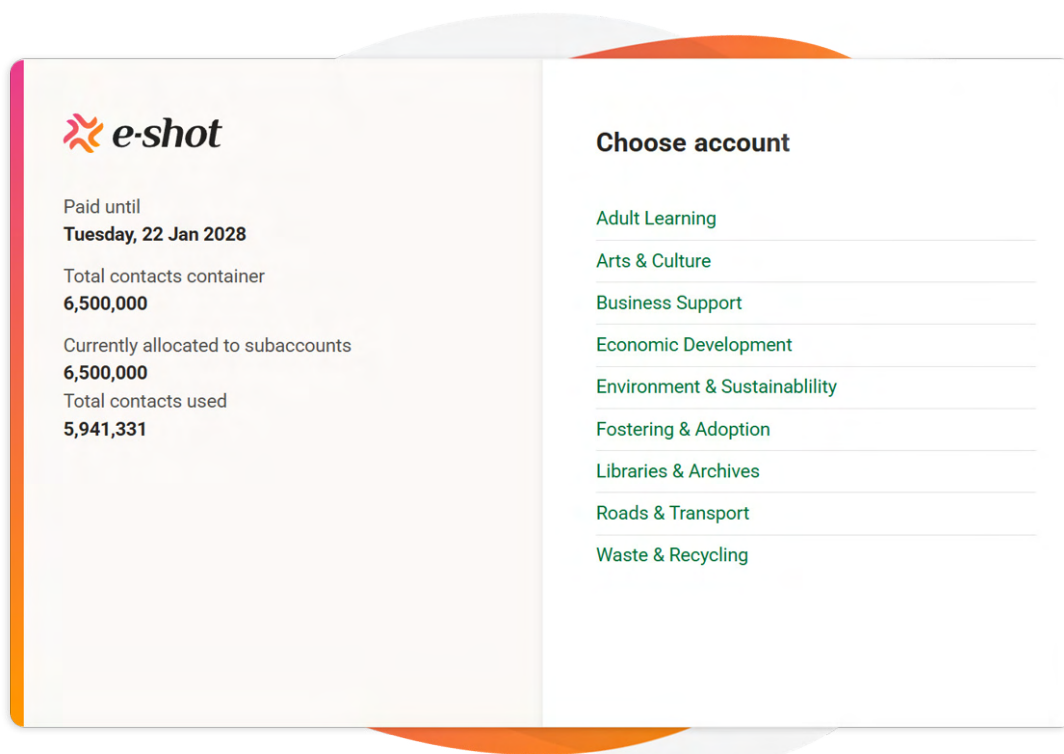
Central Bedfordshire County Council

Limits

Key features	Omni	Pro	Basic
Email campaigns	✓	✓	✓
SMS campaigns	✓	✓	✗
WhatsApp campaigns	✓	✗	✗
Marketing automation	✓	✓	✓
Landing pages	✓	✓	✓
Forms & Preference Centre	✓	✓	✓
Website tools	✓	✓	✗
Articles	✓	✓	✓
OmniChannel campaigns	✓	✓	✗

Platform limits	Omni	Pro	Basic
Users	Unlimited	Unlimited	Unlimited
Emails	Unlimited	Unlimited	Unlimited
API calls per hour	5,000	2,000	1,000

Account limits	Omni	Pro	Basic
Preferences *	Unlimited	100	50
Saved filters	100	25	10
Landing pages *	100	25	3
Automated Series *	100	25	3
Website popups *	100	25	1



Accounts

Additional accounts can be added to your e-shot subscription to give different departments their own area of the platform. This is a popular feature with councils as different services and directorates can manage their own campaigns with a high degree of autonomy and complete data separation.

The most common basic use case for accounts is to separate external communications from internal communications.

Subscriptions

Accounts provide a way to configure how opting in and out of communications works for each department. It can be disabled completely for use cases such as internal communications or it can be linked between Accounts for other use cases, such as when a council has accounts for different service areas, but wishes to offer residents a single solution to manage their data.

Designs and templates

Digital assets can be shared across Accounts or restricted to a specific one. This makes it easy for administrators to control the designs and digital assets that each department can use.

Data and custom fields

The same contact can be stored in different Accounts with different data points, enabling each department to maintain records specific to their operational needs.

There are various options for how Accounts can be added and configured as part of your e-shot subscription.

Procuring e-shot via G-Cloud

Organisations that procure e-shot via G-Cloud 15 can look forward to a range of additional benefits offered as added value to our regular solution and service.

Benefits include:

Best price guarantee

G-Cloud represents the easiest way to procure our platform and therefore also the best value way. We guarantee the best available price via the G-Cloud framework. If you have bespoke requirements, we are happy to participate in tenders and other forms of procurement exercise, but our G-Cloud offering usually accommodates most use cases.

Clarifications

You will find a wealth of information in our service definition and pricing documents, but if you have specific questions, you can always reach out to us via email at sales@forfront.com or call us on 020 3320 8777.

Scoping and quotes

If you would like a formal quote based on the G-Cloud pricing, then get in touch and we will be happy to provide proposal, quote or pro-forma to help you with the procurement process. If you would like to discuss the specifics of your requirements, then we offer complimentary pre-scoping services to work out exactly what you need. We can also help with data protection and security questionnaires and provide any documentation that you require including accreditations and insurances.

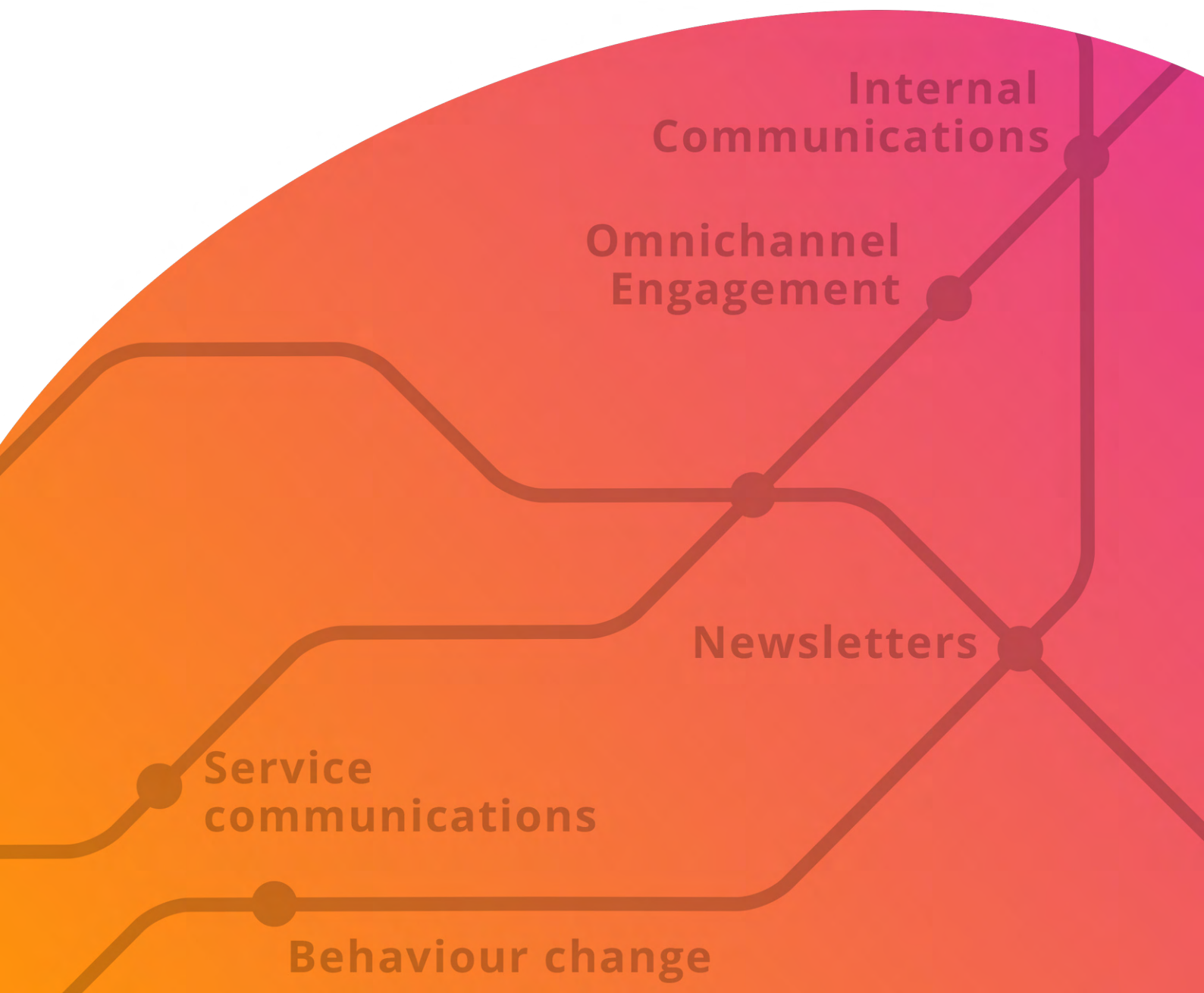


Use Cases

There are many ways e-shot can be used within public sector organisations and we work proactively with customers to find innovative ways our technologies can help them to improve engagement, drive behaviour change, deliver digital outcomes and save time and money.

The ability to add accounts to the platform for different departments means that it is easy to use e-shot for separate use cases in a single subscription. The following describe other common use cases amongst our customers:

- Newsletters
- Omnichannel engagement
- Behaviour change
- Internal communications
- Service communications



Newsletters

Whether your organisation offers a single newsletter or many options to residents and other stakeholders, e-shot provides an efficient and effective way of designing, sending and analysing email newsletters.

You can fully automate the creation and dispatch of emails from website content and our forms can be used to acquire new subscribers.

Omnichannel engagement

With 85% of the UK adult population using email daily and 96% of the UK adult population using WhatsApp daily, e-shot provides the ability to reach residents and other stakeholder groups like no other platform. Moreover, the engagement and tracking data can be used to deliver omnichannel experiences that adapt automatically to target people through the channels they are most active on.

Behaviour change

Council strategic priorities sometimes require long-term campaign planning to deliver an impact. The automation tools combined with the channel mix available in e-shot enable you to deliver highly targeted and personalised communications at scale.

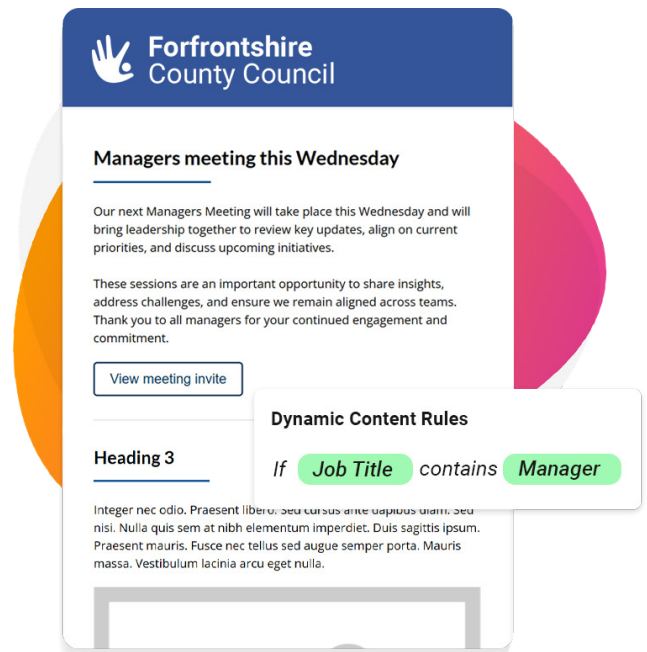
Common use cases include:

- Nurturing prospective foster carers
- Improving understanding of service offerings such as libraries
- Promoting commercial propositions such as garden waste recycling
- Maintaining interest in public health priorities such as smoking cessation



Internal communications

Email still underpins internal communication and staff newsletters represent a highly effective way of informing your organisation at scale. e-shot helps you take this even further with departmental segmentation, automation of HR messaging, integration with your staff directories and omnichannel capabilities to reach remote teams via WhatsApp and SMS along with Microsoft Teams notifications to boost reach and engagement more generally.



Service communications

Improve service delivery and reduce service demand by automating proactive messaging to residents. Common use cases for automated service alerts include:

Common use cases for automated service alerts include:

- Bin reminders
- School closures
- Transport disruption
- Incident response

Email campaigns

Digital engagement through email communication remains one of the most cost-effective ways of messaging at scale.

Newsletters

Single send campaigns enable you to rapidly configure newsletters for any future date and time with useful segmentation, testing and approval tools.

Automated series

Create nurture campaigns and other forms of marketing automation with an easy-to-use workflow editor. Inclusion or exclusion in an automation can be configured based on a range of behavioural tracking mechanisms. Automations can be entirely email-based or use the omnichannel capabilities of the platform to improve reach and engagement.

Recurrent Campaigns

Watch website pages or blogs and automatically trigger emails when new content is added to the relevant digital source. Newsletter dispatch can also be fully automated using RSS or API feeds. These campaigns can also be used to send reminders to a repeating pattern.

Split testing | *Available in e-shot Pro & Omni*

Optimise campaign performance with flexible testing tools that enable you to try different subject lines, sending times and designs.

Email forensics | *Available in e-shot Pro & Omni*

Pre-flight your campaigns to ensure there are no surprises. The Email Forensics tool will provide accurate renders of your emails across more than 40 devices and identify any technical issues that could impact deliverability or inbox placement

Start

Contact is added into group(s):

Fostering event QR code

Fostering event follow-up

Wait

Wait until the day/time is:

Monday - Friday

9:00 AM - 17:00 PM

Send email

Design name:

Upcoming fostering events

 LOREM IPSUM COUNCIL

Upcoming events

Event title 1

When: Date and time

Where: Location

Outline: Donec quis rutrum mauris. Praesent ornare, quam a gravida suscipit, neque lacus maximus leo, eget convallis mi ligula vitae urna



View email report

SMS campaigns | *Available in e-shot Pro & Omni*

Send SMS text messages to maximise engagement and leverage omnichannel communications capabilities. Local authorities use SMS for important notifications to vulnerable groups and for event marketing. SMS can also be used in an emergency communications capacity.

SMS editor

Easily write SMS messages and include links, dynamic content and emojis to optimise response. Messages can be scheduled or triggered depending on the requirement.

Dedicated SMS numbers

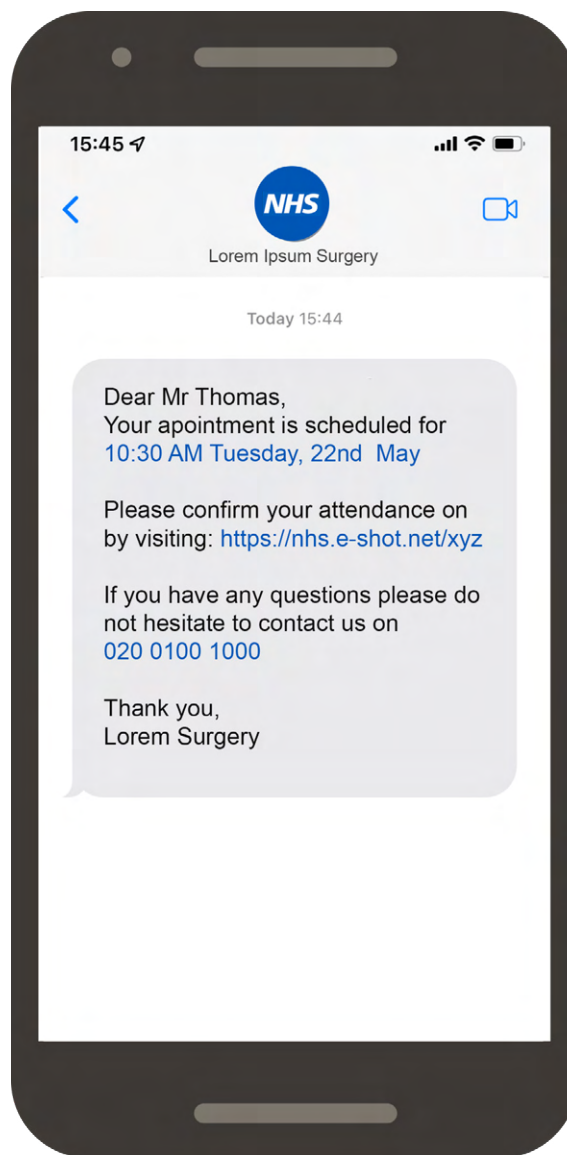
Reassure contacts that they are consistently receiving messages from the same source with a dedicated number. SMS numbers can also be masked to brand your messages

Manage replies

Reassure contacts that they are consistently receiving messages from the same source. SMS numbers can be masked with a short code to brand your messages.

Privacy controls

Choose whether to track interactions with SMS campaigns.



Whatsapp campaigns

Send WhatsApp messages to achieve optimum engagement and leverage omnichannel communications capabilities. Local authorities use SMS for important notifications to vulnerable groups and for event marketing. SMS can also be used in an emergency communications capacity.

WhatsApp campaigns

Send WhatsApp messages to achieve unrivalled engagement and leverage omnichannel communications capabilities. WhatsApp is used by over 95% of UK adults on a daily basis and represents a modern and versatile way of sending highly engaging messages.

Utility Messages

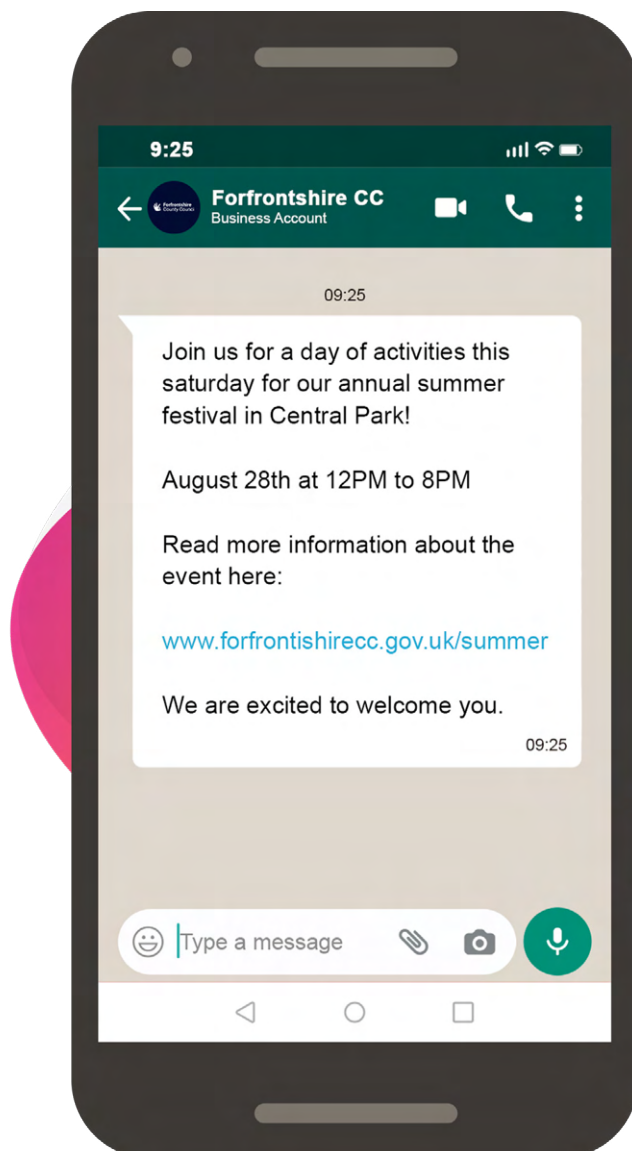
Promote content and deliver rich media messages that can include videos, links and polls to engage residents on a targeted basis.

Marketing Messages

Deliver reminders and alerts automatically and integrate with services to quickly inform residents of important issues or events.

Automated Series

Integrating WhatsApp into automated journeys can help you to improve reach and response rates. WhatsApp can be used as the primary channel in an automated campaign or as a backup when other channels fail to reach residents.



CRM

Keep contact information and activity organised and up to date.

Contacts

A contact record in e-shot captures a combination of demographic and behavioural data with comprehensive auditing of interactions across campaigns. Custom fields provide more detailed segmentation options.

Accounts | *Available in e-shot Omni*

For professional audiences, the account entity caters for tracking multiple contacts from the same organisation. This extra dimension helps to track engagement at an organisational level.

Groups

Groups help you to organise contacts into lists and then use these lists for segmentation and analysis. Groups can also be used in tandem with automations to move contacts through sophisticated campaign journeys.

Engagement

Understand the health of your subscriber lists with automatic engagement classifications. Use these engagement categories to identify those who are consistently interacting and those who are not interacting with your campaigns.

Preferences

Give subscribers the option to opt in and out of specific publications and topics. Subscription preferences are automatically audited on the contact record.

Data import

You can upload contacts from spreadsheets, map data fields, and manage duplicates for efficient bulk update. Email addresses are validated on import and errors logged. Field mappings can be saved to make future imports easier.

Custom fields

Create custom fields tailored to specific organisational needs. Custom fields can then be used for segmentation and personalisation, whilst values can be set to specific data types and limited to a pre-defined picklist of values.

Preferences

Give subscribers the option to opt in and out of specific publications and topics. Subscription preferences are automatically audited on the contact record.

Segmentation and filters

Contact data can be filtered manually or automatically to build highly targeted audiences based on a variety of data points. Behavioural signals such as engagement status and number of campaigns sent in the past 7 days, help you to filter data dynamically based on tracked interactions.

☐	First Name	Last Name	Email	Email Status
☐	Andrew	Thompson	andrew.thompson@email.co.uk	Engaged
☐	Becky	Smith	becky.smith@email.co.uk	Disengaged
☐	Emily	Anderson	emily.anderson@email.co.uk	Engaged
☐	Harry	Bridges	harry.bridges@email.co.uk	Engaged
☐	Holly	McCabe	holly.mccabe@email.co.uk	Slipping Away
☐	Simon	Tweeddale	simon.tweeddale@email.co.uk	Engaged
☐	Winston	Jones	winston.jones@council.gov.uk	Slipping Away
☐	Zoe	Regan	zoe.regan@email.co.uk	

Contact Details
 First Name
Winston
 Last Name
Jones
 Email
winston.jones@email.co.uk

Design

Smart Editor

Designing effective communications is easy with e-shot. Our Smart Editor helps you to create high impact communications with engaging content using a highly intuitive drag and drop editor that allows for a variety of content types such as videos, buttons and countdown timers to name a few.

Design blocks

There are a range of content options in the editor that help you to create highly engaging designs with ease.

Text

The Text block is a fundamental component of every design. Text styles are template driven, but a full range of editing controls over text and paragraph styles. We also offer support for custom web fonts.

Image library

Upload images to a design or link to them from an external URL. Images can be organised into a library and categorised for search. We also offer a royalty-free stock library of images as part of the image library.

Image editor

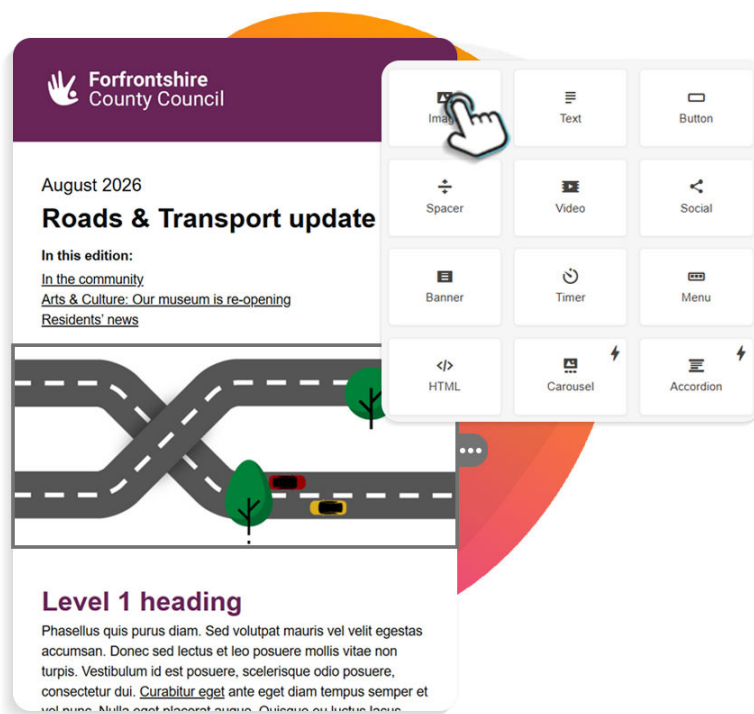
Any image can be edited inside the editor. Tools to resize, crop and colour correct images help you to efficiently amend images without leaving the design.

Video embed

Embed video content in your designs to improve engagement. Add the URL of your hosted video and e-shot will automatically create an embedded video with customisable thumbnail, play button and alt text. Videos will play natively in email when the email application supports it.

Buttons

Buttons are interactive elements in the email editor that can link to URLs, initiate phone calls and serve up special functions. Extensive controls over buttons allow their styling to be customised.





Countdown timers

Countdown timers help you dynamically show how long is left until a deadline. This is great for events and perfect for creating a sense of urgency as the time remaining is automatically reflected when someone views the design. You can customise countdown timer styling and set dates and times for any time zone

Single question surveys

Easily gather instant feedback directly within your emails using the Single Question Survey feature. Present a simple question with clickable image or text responses to gauge audience opinion quickly. This is ideal for quick polls and sentiment scoring.

Design preview

Responsive preview

Quickly check your design on both desktop and mobile to ensure it adapts to the device type properly. More comprehensive device testing is available in Email Forensics in Campaigns.

Link preview

Every link will automatically be checked and enable you to see which buttons and other elements link to URLs. If a link is broken, e-shot will warn you.

Accessibility preview

You can automatically check designs for any accessibility issues. The preview will warn against any failures against the WCAG 2.2 AA standard for non-image elements such as poor colour contrast.

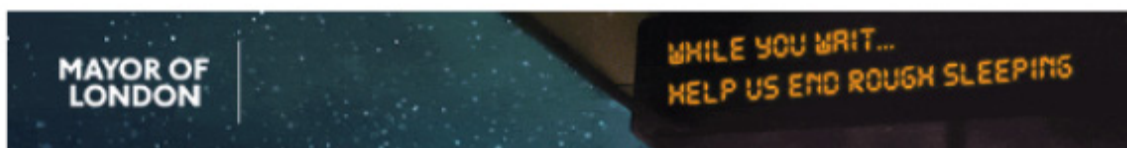
We also offer accessibility training as part of our social value commitments to all customers.

For more information on e-shot accessibility, see [page 47](#)

Modules

Modules are templated, reusable sections of an email design. The module library can be used to quickly add pre-built sections. Modules can also be synchronised, so that a change made once can be reflected across all designs where the module is used.

Advertisement:



Advertising in emails

Emails can be used to promote strategically important messages in a variety of ways. In tandem with the modules function, dynamic blocks can be added to designs that are automatically populated with advertising served from your own inventory or from reputable third-party advertisers.

We work in partnership with CAN to help local authorities generate revenues from their media estate including from their email newsletters.

HTML upload

HTML upload enables you to import email code from a file or a link. The link option enables you to update a design dynamically. This is useful for fully automated email workflows.

Social share

Social share adds a special link to your designs that can be used to invoke native sharing tools on any device. The social share link directs new visitors to a permanent web version of the campaign. It can also be configured to include an additional link to a sign-up form to capture new subscribers.

Templates

Streamline your design creation process and maintain brand consistency using e-shot's template features. Save your own designs as personal or shared templates, or choose from a vast library of best practice templates. Templates use the same Smart Editor to ensure a consistent user experience.

Email library

We share public sector toolkit designs in the template library to help promote a range of government and NHS campaigns, making it easy for local authorities to use or adapt messaging.

Basic dynamic content

You can insert specific contact data, such as first names or custom field information, directly into your email subject line, preview text or design using merge tags. This functionality helps create a more individualised message for each recipient, tailoring the communication to them. Fallbacks can be easily set to cater for missing values.

Advanced dynamic content | *Available in e-shot Pro & Omni*

Vary the content of your design based on rules using advanced dynamic content - this lets you create highly personalised emails. Each section of an email can be tailored based on language, location or a range of other contact-centric values.

Forfrontshire County Council

Email (required)

Preferences

+ **Adult courses and learning**

+ **Business**

Young people & Families

- ☐ Children & Families
- ☐ Fostering
- ☒ Youth Service

10,003

8,803

Forms

Sign up forms

Our simple form builder enables you to create sign up forms and other data capture devices. All forms are automatically formatted to best practices from a responsive design and accessibility perspective. Protect your data integrity by enforcing a double opt in process and engage with new subscribers automatically by triggering welcome emails and pages.

Landing pages

You can host forms and other content in landing pages that are quick to build and amend. Landing pages are automatically responsive and accessible, making it simple to deploy targeted content separately from your website.

Website popups

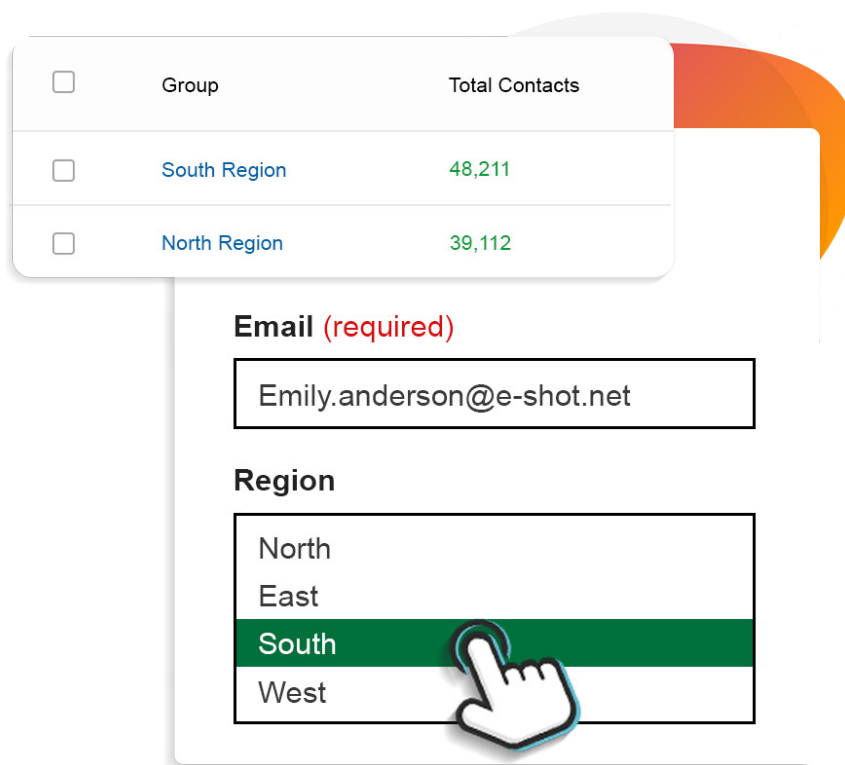
You can deliver timely messages to your website visitors or prompt them to subscribe to your newsletters with popups. Control the criteria for when and how messages appear on your website and how they look and function.

Preference centre

Preference centre gives your subscribers the ability to change the data that you hold about them and the topics that they are subscribed to on a self-serve basis. Everything is tracked and audited to ensure data protection compliance.

Preference categories | *Available in e-shot Pro & Omni*

For organisations with lots of subscription options, preference categories enable you to organise sets of preferences into categories to represent different themes or departments.



☐	Group	Total Contacts
☐	South Region	48,211
☐	North Region	39,112

Email (required)

Emily.anderson@e-shot.net

Region

North

East

South

West

Global preference centre

Provide your subscribers with a single, consolidated platform to manage their data and communication preferences across multiple departments under one e-shot subscription. This improves the subscriber experience and helps maintain consistency and compliance across different service areas.

Form tracking

Unique IDs across forms, QR codes and website popups help you to understand where sign-ups are coming from and track the performance of subscriber acquisition campaigns.

Protected unsubscribe

Ensure data protection compliance with protected unsubscribe. e-shot permanently maintains a contact's email address in a suppressed state, ensuring that even if the data is subsequently re-uploaded to the system, the platform will automatically honour the opt-out and block future campaigns.

Analytics

Campaign metrics

Real time reporting

All interactions are tracked in real time and data is written to both the Campaign Report and the individual Activity Log of each contact. This includes displays, clicks, replies, votes and shares amongst others.

Key metrics

Graphical presentation of opens, clicks, forwards, unsubscribes and bounces of every email campaign you send. Delve in a little further, and you can analyse granular link popularity, interaction timeframes and device usage analysis.

Benchmarking

Trendline analysis of the current campaign results versus previously sent campaigns. Filter previous results by tag to make specific comparisons.

Click overlay

A heatmap presentation of where exactly contacts are clicking on your campaign with the most and least popular links colour-coded.

Anonymisation

All reports can be presented with personal data removed to help with data protection and security.

Engagement categorisation

Instantly understand the health of your database with engagement categories. This identifies macro trends for who is interacting with your campaigns and who is not.

Deliverability

Each e-shot customer has dedicated sending infrastructure which is continually monitored by our deliverability team. This ensures that any issues can be identified proactively and solved quickly.

Official domains

Send emails via gov.uk, nhs.uk and police.uk sending domains to ensure brand protection and so that your communications are seen to be from a trusted source.

These domains can also be used to host landing pages and other content.

Authentication

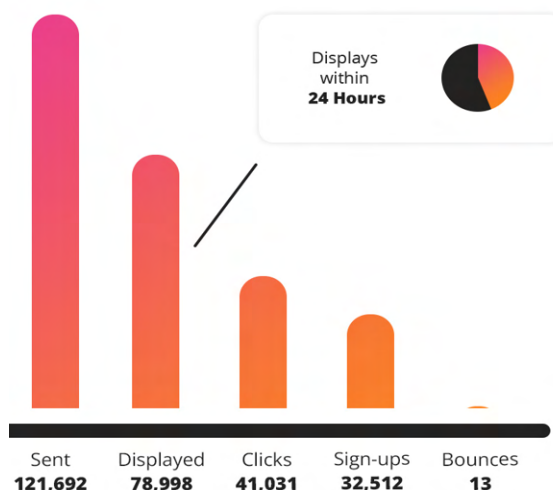
We offer a fully managed DNS service, but can also work with your own technical teams to ensure DNS is setup and maintained correctly.

Email Forensics

Every campaign and design is automatically checked to identify potential problems with language, links, cookies and an extensive range of technical checks so that any problems can be proactively addressed before you send a campaign.

Deliverability Dashboard

Get an instant view on deliverability across a range of signals including authentication of SPF, DKIM, DMARC and MX. 24/7/365 monitoring of loopback, blocklists, Gmail, Microsoft SNDS and all other ISPs. Automatic bounce management, unsubscribe and complaints management tools and daily reputation scoring help to minimise technical



Intergrations



API

Our versatile API can be used to provide integration to other applications

for a variety of use cases. API access tokens can be IP restricted for

added security. Full documentation and API testing tools:

<https://docs.rest-api.e-shot.net>

Zapier

Zapier integration helps you to automate workflows and connect with thousands of apps without coding. This enables streamlined processes like lead capture follow-up, cross-channel campaign coordination, and data synchronisation.

Google Analytics

Links in campaigns can automatically be appended with UTM tracking parameters. This helps you to identify the website traffic, engagement, and conversions driven by your e-shot campaigns directly within your Google Analytics account.

Microsoft Entra

Synchronise contact groups from your Microsoft Active Directory with groups in the e-shot CRM.

This helps to automate internal list management and keep your communications aligned with active memberships. It is a powerful tool for maintaining accurate internal directories for staff newsletters, briefings, and departmental updates.

Synchronise Entra groups with e-shot contact groups

Microsoft Teams | *Available in e-shot Omni*

Integration with Microsoft Teams makes it easy to publish campaigns, proofs or reports to Teams channels or chats.

This can help busy communications teams to organise campaigns whilst also offering a different way to engage staff at scale.

Service scope

Add-ons and extensions

Software add-on or extension: No

Cloud deployment model

Hybrid cloud

Service constraints

Customers are proactively informed of any planned maintenance or service issues via email and the e-shot™ dashboard. Planned maintenance is designed to be carried out with no service downtime wherever possible.

During periods of peak demand, intelligent delivery controls are applied to manage traffic safely and maintain service stability. This protects customer sending reputations, including domains and IP addresses.

System requirements

A standard web browser with internet access.

User support

Email or ticketing support

Email or online ticketing support: Yes

Support response times

Support is provided during standard hours of 09:00 to 18:00 (UK time), Monday to Friday.

24/7 support is available for critical incidents. Systems are proactively monitored 24/7.

Median time to first response (2025): **1 minute**

Median time to resolution (2025): **1 hour 14 minutes**

Customer satisfaction (CSAT, 1 January – 31 December 2025): **97.8%**

User can manage status and priority of support tickets

No

Phone support

Phone support: Yes

Phone support availability

09:00 to 18:00 (UK time), Monday to Friday.

Web chat support

Web chat support: Yes

Web chat support availability

09:00 to 18:00 (UK time), Monday to Friday.

AI chatbot

No

Web chat support accessibility standard

WCAG 2.2 AA

Web chat accessibility testing

Web chat functionality is provided by a third-party supplier who undertakes regular accessibility testing and review. Further information is available at:

<https://www.intercom.com/blog/messenger-accessibility>

Onsite support

Yes, at extra cost

Support available to third parties

Yes



Support levels

Support is provided as part of the software subscription.

Service desk and incident support

A central Service Desk is provided through the Customer Success team, delivering remote support for incidents, service requests, and user assistance. Support covers technical issues, configuration queries, account administration, and general service use.

Incidents are logged, categorised, and prioritised in line with published Service Level Agreements (SLAs). Priority is given to incidents that materially impact service availability or prevent customers from completing time-critical activities.

Request fulfilment and training

Standard service requests include user support, guidance on best practice, and access to training resources. On-demand support materials are provided, including written documentation, interactive guides, and training videos.

Proactive service management

The service is proactively monitored to identify and resolve issues before they impact customers. Service performance and operational health are continually reviewed to support service stability and reliability.

Escalation and specialist support

The Service Desk is supported by specialist internal teams, including Infrastructure, Deliverability, and Development. Incidents are escalated as required in accordance with internal escalation procedures to ensure timely resolution.

Technical account management

Technical Account Management is provided through the Customer Success team, acting as the primary point of contact for service usage, operational guidance, and ongoing service improvement.

Exclusions and chargeable services

Requests that fall outside standard incident management or request fulfilment, and are deemed consultancy or project-based work, may be subject to additional charges. This is agreed in advance with the customer.

Incident prioritisation and service levels

As part of our commitment to service quality, all support requests are logged, tracked, and assigned a priority based on business impact and urgency. Service Level Agreement (SLA) response times represent minimum standards, and in practice we frequently respond to and resolve issues more quickly.

Priority definitions and response targets

Priority 1 (P1 – Urgent/Critical)

Issues requiring immediate attention due to a complete service outage or loss of access to core functionality, such as the inability to send campaigns. All users are affected.

- First response: within 1 business hour
- Initial resolution: within 1 working day
- Final resolution: hot fix release
- Status updates: hourly (workaround proposed within 1 hour where possible)

Priority 2 (P2 – High)

Issues that significantly affect service use for a large number of users or impact critical functions, such as sending campaigns, where the service is partially available.

- First response: within 2 business hours (or 4 hours out of hours)
- Initial resolution: within 2 working days
- Final resolution: hot fix release or next maintenance release
- Status updates: every 4 working hours

Priority 3 (P3 – Medium)

Issues that have a limited impact on service use and do not prevent access to core functionality. A subset of users may be affected.

- First response: within 1 working day
- Initial resolution: next maintenance release
- Final resolution: next maintenance release
- Status updates: within 1 working day

Priority 4 (P4 – Low)

Low-impact issues that do not affect core functionality and typically relate to minor defects, usability improvements, or general enquiries. One or very few users are affected.

- First response: within 1 working day
- Initial resolution: future release
- Final resolution: future release
- Status updates: within 1 week

Escalation and governance

Incidents are managed by the Customer Success team and escalated as required through Operations Management and senior technical leadership. Escalation paths are clearly defined and applied in line with incident priority and impact.

How will users work with your service

Browsers

Web browser interface: Yes

Supported browsers

- Microsoft Edge
- Firefox
- Chrome
- Opera

Installation

Application to install: No

Mobile

Designed for use on mobile devices: Yes

Differences between the mobile and desktop service

Email and campaign authoring is available on the desktop service only. Mobile access is provided for reporting and analytics.

Service interface

Service interface: No

User support

User support accessibility: WCAG 2.2 AA

API

API: Yes

What users can and can't do using the API

e-shot™ provides a REST API accessible over HTTPS. API access is controlled via API keys, which can be restricted to specific accounts and IP addresses where required. API keys are issued following a request from an authorised administrator.

The REST API provides full read and write access to core entities, including contacts, campaigns, sources, groups, and website activity.

API documentation is available at:

<https://docs.rest-api.e-shot.net>

API documentation

Yes

API documentation formats

- OpenAPI (Swagger)
- HTML
- PDF

API sandbox or test environment

Yes

Customisation

Customisation available: Yes

Description of customisation

e-shot™ can be extensively customised to meet organisational requirements. Customers can configure user management, branding, templates, and sending identities. The platform can be structured into multiple accounts to support different organisational units, each with their own configuration.

Accounts can be white-labelled with customer branding, including logos displayed in the user interface and reports. Users can customise reporting, analytics, and selected interface elements, including accessibility preferences.

From an integration perspective, the API supports bespoke implementations, allowing e-shot™ functionality to be embedded into third-party systems where required.

Onboarding and offboarding

Getting started

A fully managed onboarding service is provided. The G-Cloud pricing document sets out a range of onboarding options designed to support different public sector organisations and use cases.

The onboarding service includes project management, consultancy, training, and design support to configure the service to customer requirements. Simple implementations can be completed within days. Larger or more complex projects, such as those involving integrations or migration from another platform, typically take between 6 and 8 weeks.

Training for new users is included as standard and can be delivered at any time. Bespoke training can also be provided remotely or in person if required.

For all G-Cloud customers, a dedicated testing account is provided. The service supports official domains and includes proactive DNS monitoring via NCSC Mail Check. A GovDelivery migration service is also available where required.

Documentation

Service documentation: Yes

Documentation formats:

- HTML
- PDF
- Documentation accessibility standard: WCAG 2.2 AA

End-of-contract data extraction

The service supports bulk export of data via the user interface or API, subject to appropriate permissions.

End-of-contract process

Contracts end when the licence expires, unless a renewal is agreed. The licence includes access to the software, hosting, product updates, and standard support for the duration of the contract.

All customer data, reports, and templates can be exported without charge up to the contract end date. After this point, the account is closed and archived. Following the archive period, the account is permanently deleted, with only an archived backup retained for the period required under data protection legislation.

email	Name	Surname	Postal Address
oliver.smith@email.com	Oliver	Smith	BS1 4AB
amelia.jones@email.com	Amelia	Jones	M14 7QP
harry.williams@email.com	Harry	Williams	SW3 5UD
isla.taylor@email.com	Isla	Taylor	LS6 2HT
george.brown@email.com	George	Brown	CB2 3PL
poppy.davies@email.com	Poppy	Davies	OX1 1JD
charlie.wilson@email.com	Charlie	Wilson	L18 4NX
ava.evans@email.com	Ava	Evans	B3 2LH
alfie.thomas@email.com	Alfie	Thomas	NE2 1AA

New Import

Field Mapping

Imported Columns

Email

Name

Surname

Postal Address

Organisation

Job Title

Contact fields

Email Address

First Name

Last Name

Post Code

Organisation

Job Title

Source

Waste & Recycling Service

Import

Data importing and exporting

Data export approach

Data can be exported via the user interface by authorised users only.

Data export formats

- CSV
- Other

Other data export formats

Data can also be exported via the API or through integrations, subject to role-based permissions and access controls.

Data import formats

- CSV
- Other

Other data import formats

- Excel
- Via API or integration

Access controls

Data import and export actions are restricted using role-based access controls. Only users with the appropriate permissions can import, export, or access data via the API. API access is controlled through secure API keys, which can be limited to specific accounts and IP addresses where required.

Analytics

Metrics

Service usage metrics: Yes

Metrics types

All interactions with campaigns sent through e-shot are tracked and reported in real time. Metrics are recorded at both campaign level and individual contact level through a detailed activity log.

Reporting includes graphical views of key engagement metrics such as email opens, clicks, forwards, unsubscribes, and bounces. Users can create, save, and reuse custom reports directly within the user interface using flexible query-style filters.

Saved reports can be run on demand and shared across the organisation. All service usage metrics are also available via API for integration with external reporting or analytics systems.

Role-based access to analytics and reporting

Access to analytics, reports, and underlying data is controlled through role-based permissions.

Administrators can define which users can view, create, edit, export, or share reports, ensuring access is limited to authorised users only.

API access to analytics data is also subject to role-based controls and secure authentication.

Reporting types

- Through an API
- Real-time dashboards
- Regular reports
- Reports on request

Resource tagging

No

FOCUS resource tagging

No

Scaling

Independence of resources (NCSC Principles A, B and C)

The e-shot platform is hosted on dedicated infrastructure within a secure UK data centre and is designed to scale to meet varying levels of demand without impacting service security or availability.

Customer data is logically segregated, with each customer's data stored in a dedicated database. This separation supports strong data isolation between tenants, reducing the risk of data leakage and supporting compliance with data protection requirements.

The platform is designed with sufficient capacity headroom to ensure that increases in usage or peak demand do not adversely affect performance or service stability for other customers.

Resilience and availability (NCSC Principle E)

The architecture supports independent scaling of system components, helping to maintain service availability during periods of high demand. This approach reduces the risk of resource contention and supports continued operation in the event of component-level issues.

Public sector networks

Connection to public sector networks

No

The service does not connect to, depend on, or require access to public sector private networks such as the Public Services Network (PSN). Access to the service is provided over the public internet using secure, encrypted connections only.

In line with **NCSC Cloud Security Principle E (Network Security)**, network boundaries are clearly defined and controlled. The service is designed as an internet-facing application with no direct connectivity into customer internal networks or government network environments.

All external access is restricted to required service endpoints and protected through industry-standard network security controls. There is no inbound connectivity from the service into customer environments.

This network model is consistent with the service's hosting and data residency approach. The platform is hosted in secure UK data centres, and all customer data is stored and processed within the UK. Network controls are applied to support secure access while maintaining strong separation between customer environments and government internal networks.

Data-in-transit protection

Protection between networks

Data protection between buyer and supplier networks

All data transmitted between customer networks and the service is encrypted in transit using industry-standard cryptographic controls.

- **TLS version 1.2 or above** is enforced for all external connections
- Connections are made over the public internet; no reliance on private or public sector networks (for example PSN)
- Weak protocols and insecure cipher suites are disabled

This approach aligns with **NCSC Cloud Security Principle E1 (Network protection) and E3 (Encryption in transit)**, ensuring data confidentiality and integrity for all internet-facing communications.

Protection within the supplier network

Data protection within supplier network

Data transmitted between internal system components within the supplier environment is protected using encrypted network connections.

- **TLS version 1.2 or above** for service-to-service communications
- **IPsec or TLS-based VPN gateways** used where network segmentation or additional protection is required

Internal network traffic is secured to prevent interception, tampering, or unauthorised access, in line with **NCSC Principle E2 (Network separation) and E3 (Encryption in transit)**.

Certificate management and cryptographic assurance

All TLS certificates are managed centrally and issued by trusted certificate authorities. Certificates are monitored for validity and renewed prior to expiry to prevent service disruption or weakened security.

Cryptographic controls follow current industry best practice and NCSC guidance:

- Strong, approved cipher suites are enforced
- Deprecated algorithms and protocols are not supported
- Encryption configurations are reviewed regularly to remain aligned with evolving security standards

This supports **NCSC Principle E4 (Network integrity and assurance)** by ensuring encryption mechanisms remain robust, current, and correctly implemented.

Summary of NCSC alignment

E1 – Network protection: Secure, controlled internet-facing access

E2 – Network separation: Segmentation and isolation within supplier networks

E3 – Encryption in transit: TLS-protected communications end-to-end

E4 – Network integrity: Managed certificates and strong cryptographic assurance

Asset protection

This service is designed and operated in line with **NCSC Cloud Security Principle B (Asset protection)**, ensuring that customer data is protected throughout its lifecycle: creation, storage, use, backup, and secure disposal.

Data storage and processing locations (Principle B1 – Data location)

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

United Kingdom

User control over data storage and processing locations

No

All customer data is stored and processed exclusively within the United Kingdom. Data does not leave the UK for storage, processing, backup, or recovery purposes. This supports UK GDPR compliance and public sector data residency and sovereignty requirements.

Datacentre security standards (Principle B2 – Physical protection)

The service is hosted in secure UK data centres that comply with recognised international assurance standards, including **SSAE-18 / ISAE 3402**. These standards cover physical security, access control, environmental protection, and audited operational processes.

Physical access to infrastructure is strictly controlled and limited to authorised personnel only.

Penetration testing (Principle B3 – Secure design and operation)

Penetration testing frequency

At least once per year

Penetration testing approach

Independent IT Health Checks are carried out by a CHECK-accredited service provider in line with NCSC guidance.

Findings are assessed, prioritised, and remediated through formal risk management and change control processes to maintain the ongoing security of the service.

Protection of data at rest (Principle B4 – Data protection controls)

Customer data at rest is protected through strong physical, environmental, and logical controls. Storage systems are hosted within secure facilities and access is restricted to authorised personnel and systems only, in accordance with **SSAE-18 / ISAE 3402** requirements.

Backup and recovery (Principle B5 – Data availability and resilience)

Customer data is backed up in line with defined operational procedures to support service resilience and recovery. Backups are stored securely within the UK and protected using the same security controls as production data.

Backup processes are designed to support data restoration in the event of accidental deletion, corruption, or service disruption, ensuring continuity of service in line with availability and resilience requirements.

Data retention (Principle B6 – Data lifecycle management)

Data is retained only for as long as necessary to deliver the service and meet contractual, legal, and regulatory obligations. Retention periods are defined and enforced through documented policies and operational controls.

At contract end, customers are able to extract their data prior to account closure in line with agreed exit arrangements.

Data sanitisation and disposal (Principle B7 – Secure deletion)

Data sanitisation process

Yes

Data sanitisation type

Deleted data cannot be directly accessed. Data is removed using cryptographic erasure, ensuring it is rendered unreadable and unrecoverable.

Equipment disposal approach (Principle B8 – Secure asset disposal)

All equipment disposal is managed in accordance with recognised standards, including ISO/IEC 27001, CSA CCM, and CAS (Sanitisation). Storage media is securely sanitised or destroyed at end of life to prevent data recovery.

Summary of NCSC Principle B alignment

- B1:** UK-only data location and processing
- B2:** Physically secure, audited data centres
- B3:** Independent CHECK penetration testing
- B4:** Controlled protection of data at rest
- B5:** Secure UK-based backups and recovery
- B6:** Defined data retention and lifecycle controls
- B7:** Cryptographic erasure of deleted data
- B8:** Standards-based secure equipment disposal

Availability and resilience

The service is designed and operated in line with **NCSC Cloud Security Principle E (Availability and resilience)**, ensuring that the platform remains available, can recover from disruption, and continues to protect customer data during incidents.

Service availability (Principle E1 – Availability)

The service operates with a **target availability of 99.9%**, excluding scheduled maintenance. Planned maintenance is carried out outside standard business hours wherever possible to minimise user impact. Customers are informed of service-affecting incidents through email and in-platform notifications. For high-priority or crisis incidents, customers receive regular status updates until service is restored.

Availability commitments and response times are measured against standard service hours of **09:00 to 18:00 (UK time), Monday to Friday**.

Monday to Friday, excluding public holidays.

Full details are defined in the Service Level Agreement (SLA):

<https://www.e-shot.net/customer-promise>

Resilient architecture (Principle E2 – Resilience)

The platform uses a **high-availability architecture** designed to minimise single points of failure. Workloads are distributed across multiple components, allowing the service to continue operating during component-level faults.

Capacity headroom and intelligent workload management are used to maintain performance during peak demand, including time-critical public-sector communications.

Monitoring and incident response (Principle E3 – Detection and response)

The service is monitored **24×7×365**. Automated alerts notify the Operations team of service degradation or outages, enabling rapid triage and escalation.

Customers are notified of confirmed service issues via the platform and by email to authorised administrators. For significant or unexpected outages, targeted communications are issued to affected customers.

Post-incident information, including root cause and mitigation actions, is available on request.

Recovery objectives (Principle E4 – Recovery and continuity)

The service is designed to support timely recovery following incidents:

Recovery Time Objective (RTO): The service aims to restore availability within agreed SLA targets following a service-affecting incident, depending on incident severity.

Recovery Point Objective (RPO): Data recovery objectives are aligned to regular backup processes, ensuring minimal data loss in the event of system failure.

Backup, recovery, and restoration processes are tested and reviewed as part of ongoing operational assurance.

Summary of NCSC Principle E alignment

E1: Defined availability targets and maintenance controls

E2: High-availability, fault-tolerant architecture

E3: Continuous monitoring and structured incident management

E4: Defined recovery objectives and tested restoration processes

Governance

This service is governed in line with **NCSC Cloud Security Principle A (Governance)**, ensuring that security is owned at senior level, embedded into organisational processes, and subject to ongoing oversight and improvement.

Security ownership and accountability (Principle A1 – Responsibility)

A named, board-level individual is accountable for information and service security. This role provides senior leadership oversight, ensures appropriate resources are in place, and is responsible for the effectiveness of the organisation's security governance arrangements.

Clear lines of responsibility for security are defined across the organisation and supported by documented roles, policies, and procedures.

Security governance framework (Principle A2 – Governance framework)

The organisation operates a formal security governance framework aligned to recognised standards and best practice.

Software Security Code of Practice: Yes

Security governance certified: Yes

Security governance standards: ISO/IEC 27001:2022

The Information Security Management System (ISMS) is independently certified and subject to regular internal review, external audit, and management oversight.

Security policies and assurance (Principle A3 – Policy and assurance)

Comprehensive information security policies and supporting processes are in place and apply across the organisation. These policies define requirements for risk management, access control, secure development, incident management, and compliance.

The organisation is ISO/IEC 27001 certified and Cyber Essentials Plus compliant, providing independent assurance that security controls are effectively implemented.

Policies and procedures are reviewed at least annually, and additionally following significant changes to the organisation, systems, or threat landscape.

Secure development and change management (Principle A4 – Secure lifecycle management)

Security is embedded throughout the software delivery lifecycle using defined DevOps practices. Development, User Acceptance Testing (UAT), and Production environments are strictly separated.

All code changes must progress through Development and UAT before deployment to Production using controlled, automated deployment processes. Direct deployment to Production is not permitted.

Web applications are developed and maintained in line with **OWASP security standards**, reducing the risk of common application vulnerabilities.

Summary of NCSC Principle A alignment

A1: Named board-level security accountability

A2: Certified security governance framework (ISO/IEC 27001)

A3: Documented policies with regular review and independent assurance

A4: Secure development lifecycle and controlled change management

Operational security

Operational security controls are implemented in line with **NCSC Cloud Security Principle C (Operational security)**, ensuring systems are securely configured, maintained, monitored, and updated throughout their lifecycle.

Configuration and change management (Principle C1 – Secure configuration and change control)

Configuration and change management standard

Supplier-defined controls

All changes to the service are managed through a formal change management process. Change requests are documented in a User Acceptance Criteria (UAC) driven specification, including delivery estimates and consideration of agreed customer standards and applicable security requirements, such as OWASP best practices.

Approved changes are broken down into tasks within the issue tracking system and delivered through controlled sprint-based development. Code changes are version controlled and linked to specific tasks, providing a full audit trail.

Development, UAT, and Production environments are strictly separated. Only the release management team can promote changes to public-facing environments, using an automated deployment platform. Direct deployment to Production is not permitted.



Secure baseline configuration (Principle C1 – Secure configuration)

Systems are built and maintained using defined secure baseline configurations. Baselines are designed to minimise attack surface by disabling unnecessary services, ports, and functionality.

Baseline configurations are reviewed regularly and updated to reflect changes in security guidance, platform requirements, and emerging threats. Any deviation from approved baselines is controlled through the formal change management process.

Patch management (Principle C2 – Vulnerability management)

Operating systems, infrastructure components, and third-party software are kept up to date through a structured patch management process.

Security patches are assessed for risk and applied in a timely manner based on severity and impact. Critical and high-risk patches are prioritised and deployed according to defined timescales, with testing performed prior to release to production environments.

Patch deployment is coordinated through controlled release processes to minimise service disruption while maintaining security.

Vulnerability management (Principle C2 – Vulnerability management)

Vulnerability management type

Supplier-defined controls

Vulnerabilities and operational issues are identified through multiple channels, including user reports, automated monitoring, and security tooling.

- User-reported issues are triaged by first-line support
- System- and monitoring-detected issues are triaged by the Operations team

Issues are prioritised using defined **Critical, High, Medium, and Low severity levels**, aligned to published SLAs. Critical issues are those where the service is unusable or critical business functions cannot be performed and no workaround exists.

SLA details are available at:

<https://www.e-shot.net/customer-promise>

Protective monitoring (Principle C3 – Logging and monitoring)

Protective monitoring type

Supplier-defined controls

Protective monitoring is in place to detect security events and operational issues. This includes continuous monitoring of firewall logs, application alerts, and infrastructure telemetry.

Cloud-based security controls are used, including:

- Web Application Firewall (WAF) aligned with OWASP protections
- DDoS detection and mitigation

Monitoring supports timely detection, investigation, and response to incidents.

Incident management (Principle C4 – Incident response and recovery)

Incident management type

Supplier-defined controls

Security and service incidents can be reported via phone, email, or web chat. Formal incident management procedures define roles, responsibilities, escalation paths, and communication requirements.

Affected customers are provided with updates during incidents, particularly for high-priority issues. Root cause and mitigation details are available on request to authorised administrator contacts.

Cryptographic assurance

Post-quantum cryptography secure

Yes

Cryptographic controls are reviewed regularly to ensure continued alignment with current standards and emerging cryptographic risks, supporting long-term confidentiality and integrity.

Summary of NCSC Principle C alignment

C1: Secure baseline configuration and controlled change management

C2: Patch management and structured vulnerability remediation

C3: Continuous protective monitoring and threat detection

C4: Defined incident response and recovery processes

Staff security

Staff screening

Staff security clearance

Staff screening is performed but does not conform to BS7858:2019.

BS7858 screening is typically required for roles involving physical access to secure sites or direct handling of highly sensitive operational environments. The e-shot service is delivered as a cloud-based service hosted in secure UK data centres, and staff do not require unsupervised physical access to customer premises or government secure facilities.

As such, BS7858 screening is not proportionate or required for the delivery of this service. Instead, screening is applied in line with role-based risk and government guidance for digital services.

All staff with access to systems or customer data undergo pre-employment screening appropriate to their role, supported by contractual confidentiality obligations and mandatory security policies.

Government security clearance

Government security clearance level

Baseline Personnel Security Standard (BPSS)

All Forfront staff are screened to the Baseline Personnel Security Standard (BPSS). This includes staff involved in service delivery, support, development, and operations, in line with UK government requirements for work involving access to official systems or data.

BPSS screening provides assurance covering identity verification, right to work, employment history, and relevant criminal record checks where applicable.

Ongoing personnel security

Personnel security is maintained throughout employment through:

- Mandatory information security training at induction and annually thereafter
- Clear acceptable use, confidentiality, and data handling requirements
- Role-based access controls aligned to the principle of least privilege
- Formal disciplinary procedures for breaches of security policy

These controls align with **NCSC Cloud Security Principle A (Governance) and Principle C (Operational security)**, ensuring personnel-related risks are appropriately managed.

Secure development

Secure software development is implemented in line with **NCSC Cloud Security Principle D (Secure development)**, ensuring that security is built into the design, development, testing, and deployment of the service.

Secure development lifecycle (Principle D1 – Secure design and development)

Security is embedded throughout the software development lifecycle. Development practices form part of the organisation's certified **Information Security Management System (ISMS)**, independently assessed against **ISO/IEC 27001**.

Development, User Acceptance Testing (UAT), and Production environments are strictly segregated. All code changes must progress through Development and UAT before being deployed to Production using controlled, automated deployment pipelines. Direct deployment to Production is not permitted.

Web applications are designed and built in line with recognised secure coding standards, including OWASP guidance, to mitigate common application security risks.

Secure code review (Principle D2 – Code quality and assurance)

All code changes are subject to structured code review prior to release. Reviews assess security, quality, and maintainability, and are performed by appropriately skilled developers.

Code changes are version controlled and linked to tracked work items, providing a clear audit trail. Where appropriate, additional peer review or security-focused review is applied to higher-risk changes.

Dependency and third-party component management (Principle D3 – Managing third-party risk)

Third-party libraries, frameworks, and dependencies are managed through controlled processes. Dependencies are assessed for security risk and kept under review to identify known vulnerabilities.

Updates to third-party components are evaluated, tested, and applied in line with patch and change management processes to reduce exposure to known security issues.

Testing and assurance (Principle D4 – Verification and validation)

Security testing is integrated into development and release processes. Changes are tested prior to deployment, and the service is subject to independent security assurance through certification, audit, and penetration testing.

Secure development practices are reviewed regularly to ensure continued alignment with evolving threats, standards, and best practice.

Summary of NCSC Principle D alignment

- D1:** Security embedded throughout the development lifecycle
- D2:** Structured secure code review and change traceability
- D3:** Controlled management of third-party dependencies
- D4:** Ongoing testing and independent security assurance

Identity and authentication

Identity and authentication controls are implemented in line with **NCSC Cloud Security Principle I (Identity and authentication)** to ensure that only authorised users and administrators can access the service.

User authentication (Principle I1 – Secure authentication)

User authentication needed

Yes

The service supports multiple secure authentication mechanisms to meet different organisational requirements, these are enforced across all clients:

- **Multi-Factor Authentication (MFA)**
- **Username and password authentication**
- **Identity federation** with existing identity providers (for example Microsoft)
- **IP restriction**, access restricted to client network
- **Passkeys**

MFA can be enforced at account level for all users. Authentication methods can be selected and configured to align with customer security policies.

Access restrictions for management interfaces and support channels (**Principle I2 – Access control**)

Access to management interfaces and support channels is restricted to authorised users only.

Authentication is protected using username and password credentials, with optional enforcement of MFA. Access can also be **restricted by IP address** on request, providing additional protection for sensitive administrative access.

Identity federation using Microsoft accounts is supported, enabling customers to apply their own identity and access management controls.

Access restrictions are tested at least every six months to ensure controls remain effective.

Management access (Principle I3 – Privileged access management)

Management access authentication

Management access uses strong authentication controls, including:

- **Multi-Factor Authentication (MFA)**
- Public key authentication (including TLS client certificates)
- Identity federation with existing providers
- Dedicated secure network connections
- Username and password authentication

Description of management access authentication

Administrative management of the e-shot™ platform is restricted to a separate office network. This network is connected via a dedicated, permanent IPsec site-to-site VPN tunnel.

The VPN connection is secured using **AES-256 encryption and SHA-256 authentication** with a pre-shared key. Access over the VPN is further restricted at user level to authorised personnel only, using encrypted authentication mechanisms provided by third-party access control software.

This layered approach ensures strong protection of privileged access in line with the principle of least privilege.

Audit information for users

Audit logging and monitoring controls are implemented in line with **NCSC Cloud Security Principle C3 (Logging and monitoring)** to support accountability, incident detection, investigation, and compliance.

Audit for buyers' users' actions (Principle C3 – Activity logging)

Access to user activity audit information

Yes – authorised users have access to **real-time audit information** for their account.

Audit logs record user actions performed within the platform, including access, configuration changes, and operational activity. This provides customers with visibility of how the service is being used and supports internal governance and assurance requirements.

How long user audit data is stored for

User-defined

Retention periods for user audit data can be configured by the customer to align with organisational policies, audit needs, and data protection requirements.

Audit for suppliers' users' actions (Principle C3 – Privileged activity monitoring)

Access to supplier activity audit information

Yes – authorised users have access to real-time audit information.

Audit logs capture relevant actions performed by supplier-authorised personnel when supporting or administering the service. This provides transparency over privileged activity and supports customer assurance.

How long supplier audit data is stored for

User-defined

Retention periods can be configured to meet customer governance and audit requirements.

System logging and retention (Principle C3 – Log retention)

How long system logs are stored for

At least **12 months**

System-level logs are retained for a minimum of 12 months to support security monitoring, incident response, forensic investigation, and compliance with operational and regulatory requirements.

Tamper protection and integrity of logs (Principle C3 – Log integrity)

Audit and system logs are protected against unauthorised access, modification, or deletion. Access to logs is restricted to authorised users and administrators only, using role-based access controls.

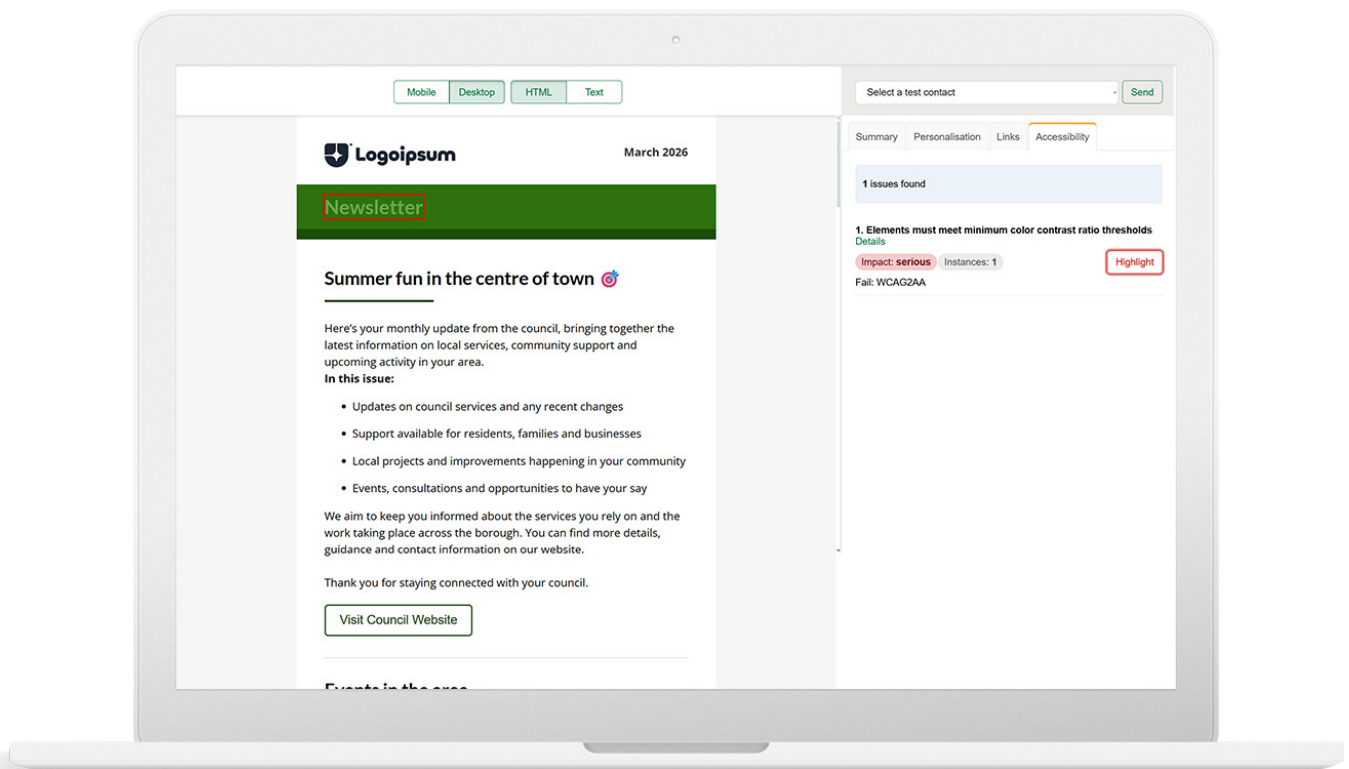
Logs are stored in a controlled environment and protected through technical and procedural controls to preserve integrity and support reliable investigation and assurance activities.

Access control to audit information (Principle C3 – Controlled access)

Access to audit logs and reporting is governed by **role-based permissions**. Customers can control which users are permitted to view, export, or manage audit data. Supplier access to audit information is similarly restricted and logged.

Summary of NCSC Principle C3 alignment

- Comprehensive logging of user and privileged activity
- Real-time visibility of audit information for authorised users
- Configurable retention aligned to customer policy
- Tamper protection and integrity controls for audit logs
- Role-based access controls for audit data



Accessibility

As a supplier to the public sector, we take our responsibilities around accessibility seriously.

Some of what we do on accessibility:

- The user interface is tested to the **WCAG2.2 AA standard**.
- All platform development is subject to accessibility testing before release.
- Content produced using the platform has the facilities built in to make it accessible.
- The design preview includes inbuilt accessibility checks.
- Our customer success team help customers to design accessible content and offer training and advice on an ongoing basis.
- We provide accessibility training every month.

We can commission independent accessibility tests including disabled user testing as part of onboarding at extra cost.

Onboarding

Moving to a new platform can be a challenge when you need to continue your operations without disruption. That's why the e-shot onboarding process is designed to ensure a smooth and effective transition, enabling your team to quickly leverage the full capabilities of the platform.

A dedicated project manager will oversee the implementation and consult with you to produce a statement of works and critical path. We will also usually suggest a schedule of weekly project delivery calls.

A typical deployment for a unitary authority looks something like this:

Week 1 – Scoping and specification

Week 2 – Templates, account provision and IT setup

Week 3 – Basic training and testing

Week 4 – Integrations, form and landing page deployment

Week 5 – Advanced training and user acceptance testing

Week 6 – Live testing

Our professional services team are highly experienced in migrating from other platforms and we can offer advice on the best way to move as part of scoping. Alternatively, we do offer a full migration service where we do almost everything for you for an additional charge.

Training

As part of onboarding, we provide three levels of user training: Basic, Advanced and Administrator. New user training is available as needed throughout your contract with us, as part of your subscription. If there are specific areas of e-shot that you wish to arrange training for, we can also provide this as well.

Training is included in our platform fees and usually delivered via Microsoft Teams.

An extensive self-service library of video tutorials, help articles, and interactive guides is also available, with content regularly updated to reflect new features and best practice.

Account management

A dedicated account manager is assigned to your organisation to ensure you achieve your strategic objectives. They will conduct quarterly and annual reviews, proactively introduce new features, and provide best-practice advice to continually add value.



Design

Our team help you to improve the quality of your digital communications by regularly providing best practice templates along with national toolkit templates from other agencies and departments.

Email design principles on accessibility and usability underpin our work as we help customers develop branded communications that are highly engaging for everyone.

Professional Services

Our teams have the skills and experience to deliver highly bespoke solutions on behalf of public sector customers. We have a wealth of experience working with other councils and can provide fully managed campaign delivery on a range of common council requirements such as:

- Foster care recruitment
- Public health
- Adult education
- Garden waste subscriptions
- Internal communications
- Public consultation
- Events

We also work closely with industry partners to provide an integrated approach to campaigns that work across channels.

Custom development

The standard version of e-shot™ comes with an incredibly broad set of functionality to fulfil most customer needs, but we can develop specific features or functions if there is something bespoke needed.

We have the relevant credentials and security clearances, and we do not outsource for quality assurance purposes. All work is fully scoped and costed in advance, so you know exactly what you're getting and investing.

Thank you

We would welcome the opportunity to discuss your requirements and can support pre-scoping, including strategic and technical consultancy.

Phone: 020 3320 8777

Email: sales@e-shot.net

Web: <https://www.e-shot.net>

