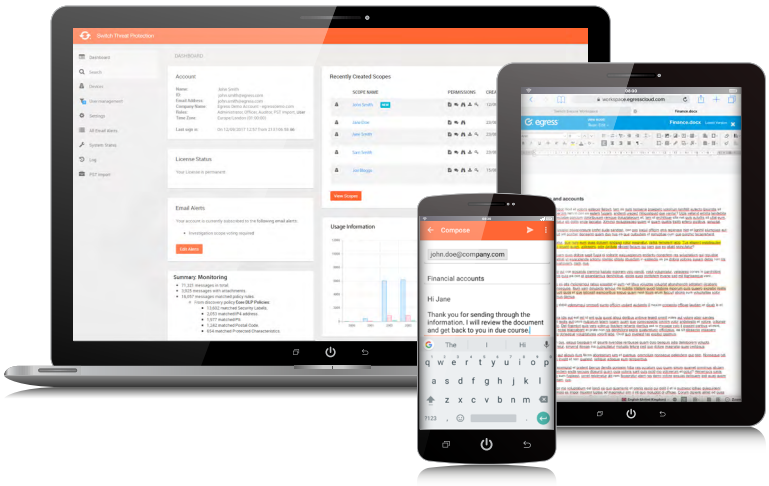
Egress for **Local Authorities**

The **go-to data security overlay** for local authorities, enabling user-friendly secure sharing, data breach prevention and GDPR compliance.

Working closely within the community, local authorities frequently need to communicate sensitive information internally and with external partners, such as police, health and social care services, and schools.

Ensuring this data remains protected means tackling the largest data breach risk factors, including human error and weakly implemented encryption. The Egress platform ensures that local authorities can protect citizens' personal information, while maintaining effective service delivery. Here are five ways Egress adds value to a local authority's data security.



About Egress and Local Authorities

- Large footprint across the UK (35% of local authorities)
- Used by over 350 government organisations (Local, Central, NHS and Blue Light)
- Trusted by the UK's largest charities and over 300 education and social services organisations
- The first and only email and file encryption solution to achieve NCSC CPA certification to OFFICIAL and OFFICIAL-SENSITIVE
- One of only 30 suppliers under the Cyber Security Supplier to Government Scheme

1. Avoid the accidental send and a data breach

Email remains the most used business communication tool, yet it also represents one of the largest data security risks: staff accidentally or intentionally sending sensitive data to the wrong person. Most email encryption solutions only guarantee secure delivery, not whether the recipient is correct. Attempts to solve this issue by turning off autocomplete functionality can affect productivity, especially considering the need to communicate with multiple third parties. Egress solutions use machine learning to efficiently safeguard against the mis-sending of email content and files, going beyond typical data protection techniques to analyse core user behaviour and help stop data breaches before they happen.

2. Prepare for GCSX retirement

The UK GCSX network that enables local authorities to communicate securely with other organisations is being retired in March 2019. Government advice going forward is to use Transport Layer Security (TLS) when sending and receiving emails. TLS often requires a configuration process between sender and recipient, something that is not always possible when sending emails to citizens or private businesses. When TLS is not enabled, local authorities need an alternative method for communicating securely. Using Egress to send encrypted content, they have the assurance that they are using a trusted, vetted solution that is currently the only email and file encryption platform to receive CPA certification from the UK government.

3. Protect and control shared data

A local authority's responsibility for sharing sensitive data often requires end-to-end security, as well as levels of control and auditing that only message-level encryption can provide. As the only CPA-certified email encryption solution, Egress helps thousands of local authority staff protect emails and attachments every day, upholding the highest data protection standards.

Integration with MS Outlook and G Suite provides a simple end-user experience and it is free for local authorities' varied networks of third-party recipients to communicate securely with them, ensuring confidential information is protected throughout its lifecycle. Egress manage all third-party helpdesk support issues, bringing significant cost and efficiency savings. Egress also allows users to revoke access to information in real time, even after it has reached the recipient's mailbox.

4. Share files and collaborate securely

Local authorities often need to collaborate on complex projects such as adoption and fostering cases, involving multiple stakeholders sharing sensitive data like panel papers and child placement information. This often requires many large files to be shared with these trusted third parties, with all content stored in one location, and control over document version and user actions, including download.

Egress provides a secure environment where all stakeholders can collaborate on documents and files. Users can access the platform from any web browser, while administrators employ role-based permissions to manage access. Data owners can control how recipients use the files they receive, including view-only permissions, and multimedia files can be streamed from within the secure system.

5. Comply with GDPR

With stringent data protection rules and large fines under the EU General Data Protection Regulation (GDPR), no local authority can risk the legal exposure, financial penalties and reputational damage caused by a data breach. Egress can be used to comply with articles of GDPR that specify personal data must be made technically secure and auditable at a fine-grained level. Egress compliance tools also allow organisations to perform specific searches to fulfil subject access requests as part of Article 15, including searching across Egress-encrypted content and proving the data subject's identity. Data relating to a specific person can also be deleted from within the system, in compliance with 'The right to erasure'.

> "Egress was chosen because of its level of integration with Microsoft Outlook, the ease of use for end users and the fact that the implementation took no time at all so we could be up and running quickly."
>
> **TECHNICAL PROJECT LEAD, UK CITY COUNCIL**

About Egress Software Technologies Ltd

Egress helps protect unstructured data to meet compliance requirements and drive business productivity. The company's AI-powered platform enables users to control and secure the data they share.

info@egress.com
0844 800 0172
@EgressSoftware
www.egress.com

CESG Certified Product Foundation Grade DGEE378428688-1104

Common Criteria

bsi. ISO/IEC 27001 Information Security Management