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.

Avoid email data breaches

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. We use contextual machine learning to efficiently safeguard against the misdirected emails and attachment, and stop data breaches before they happen.

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

March 2019 saw the retirement of the UK GCSX network that enabled local authorities to communicate securely with other organisations. 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’s received CPA certification from the UK government.

“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

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 a 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 Office 365 and Outlook 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.

Comply with GDPR

With stringent data protection rules and large fines under the 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’.

For more information please contact your account manager or call 0203 987 9666

About Egress

Our vision is for a connected world in which people communicate efficiently and securely. To achieve this, we provide human layer security to protect individual users and stop breaches before they happen.

www.egress.com | info@egress.com | 0203 987 9666 | @EgressSoftware

© Egress Software Technologies Ltd 2021. 1298-0821