freedom to focus

Tackling public sector digital transformation

Article 1:
Challenges on the horizon

Article 2:
Digital inclusion and accessibility

Article 3:
The problem of interoperability

Your data protection

Foreword by:
Glen Hymers, Head of Data Privacy & Compliance and Information Assurance, Cabinet Office

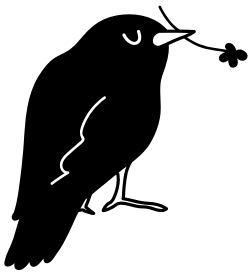
Contributors:
Robert Montgomery, Audit & Governance Lead Manager, Telford & Wrekin Council

zivver

Research approach
We conducted interviews with a selection of public sector professionals using the specialist market research consultancy, Insight Avenue.

Sponsored by

Oscar Krane



Contents

The snapshot 03

Setting the data protection standard 04
by Glen Hymers
Head of Data Privacy & Compliance and Information Assurance, Cabinet Office



Introduction 05

Challenges on the horizon 06

Digital inclusion and accessibility 07

The problem of interoperability 10

The simplest (and smartest) solution 11

Modern data management in the public sector 13
by Robert Montgomery
Audit & Governance Lead Manager, Telford & Wrekin Council



Conclusion 15

The snapshot

Embracing a digital future

Public sector organisations are in the midst of digital transformation. Employees must be empowered, rather than hindered, by technology to truly benefit:

- **58%** of employees state too much bureaucracy and "process overload" are barriers to work
- **42%** of employees feel there are too many different IT systems across their organisation

Prioritizing people

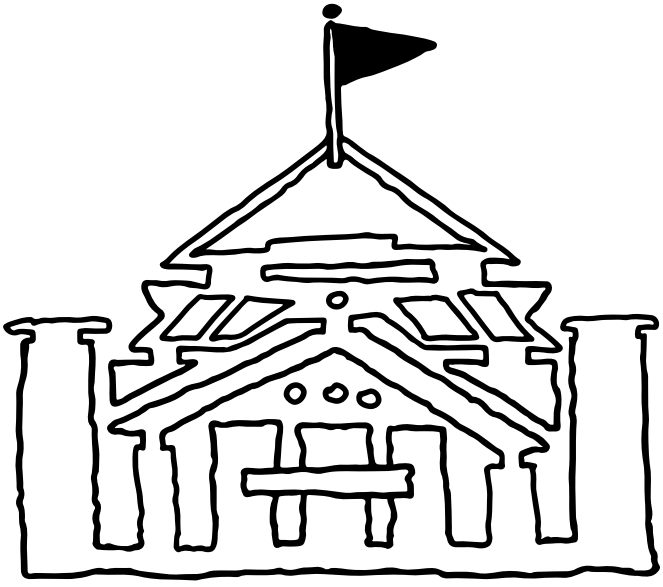
For the benefit of local communities, it has never been more important to bridge the communications gap between siloed public sector organisations:

- **79%** of employees rely on email to get their job done
- **91%** of employees consider email to be the most secure method of communication

Don't overcomplicate

Email is universal and accessible. The focus must be on leveraging existing systems rather than implementing clunky alternatives:

- **87%** of employees would experience improved morale and better productivity if their organisation invested in tech to reduce data security concerns when using email



Expert contribution



Glen Hymers BA (Hons), DipCSMP, Cert HE, CIPP/E, CIS LI, GDPR P, M_o_R,
Head of Data Privacy & Compliance and Information Assurance, Cabinet Office

Setting the data protection standard

by Glen Hymers

As we move further into the digital age, data protection and privacy have become increasingly important concerns across all sectors. The introduction of numerous data protection legislation such as EU GDPR, UK GDPR, CCPA, PIPL have seen a rise in public awareness as to their business's obligations to them as a result. However, the public sector in particular holds a unique responsibility to safeguard the personal data of citizens.

As a forward thinking society, we rely on our public sector organisations to provide essential services, whether they be healthcare, education, or government administration. As part of this provision, sensitive personal data is often collected, stored, and processed. Therefore, it is paramount that the public sector upholds the highest standards of data protection and privacy. A breach of personal data within any public sector organisation can have severe consequences for individuals and communities, eroding trust and potentially leading to identity theft and other forms of fraud being perpetrated against them, harming not only those directly impacted by revictimising the victims of the breach but also undermining public trust in the ability of the public sector to protect their personal data.

To avoid such negative outcomes, it is crucial that the public sector takes a proactive approach to data protection and privacy. This means implementing strong technical and organisational measures, ensuring that our security measures are fit for purpose, the technology we use is fit for purpose and configured correctly, and that we train all of our staff on data protection and privacy best practices. This way we will embed not only privacy and data protection by design but will ensure that the culture of the sector is fit for purpose also.

This report will explore the importance of data protection and privacy in the public sector, it will highlight how organisations can successfully implement strong data protection and privacy measures, as well as examine the challenges and the opportunities presented by emerging technologies.

I invite you to read on and discover how the public sector can continue to lead the way in data protection and privacy, building trust and creating a safer digital world for us all!



The public sector is encountering a growing catalogue of challenges: tightening budgets, restricted resources, outdated IT infrastructure – the list goes on.

For IT leaders in local authorities, the landscape is particularly complex. These professionals face pressure to advance their organisation's digital strategies in the face of ample skills shortages and evolving data protection laws, balancing user-experience for both residents and employees with compliance and security.

While the COVID-19 pandemic escalated a shift to online services and emphasized the potential for technology to drive sustainable, positive change for service delivery long into the future, public sector leaders are now realizing the answer does not lie in swamping tech stacks with new solutions and platforms. In fact, getting the most out of existing systems is now the objective for IT professionals.

The aim for local authorities is to improve the lives of citizens and this relies on cohesive, consistent and secure communication across public sector organizations. Agencies must find interoperable methodologies for driving engagement with each other and service users, whilst arming their people with skills and solutions to utilise data efficiently and securely, without complicating workflows. The way employees handle data must be secure and compliant, too. Employees must be empowered to utilize data to improve service delivery without fear of causing an accidental data leak each and every time they come to share a file with a partner organization.

But what does this look like? Where do IT leaders begin? And what challenges will they face along the way to sustainable, effective digital transformation?

Challenges on the horizon

How to do more with less – that's the name of the game for public sector leaders this year. According to reports, local authorities face a funding gap of around £7.3bn to £9bn by 2025-26. With increasingly tight budgets, public sector leaders remain under pressure to deliver quality services to their local communities.

We see more and more councils turning to technology to transform service delivery. Central government programs such as Future Councils are designed to address barriers to change by bringing together digital services and cybersecurity reform to multiple areas within a local authority. Indeed, **53%** of IT leaders believe that more use of smart technologies is key in progressive risk management.

However, powering digital transformation to address challenges across public sector agencies and departments is no simple feat. While technological change presents opportunities to connect administrations and their communities, it also presents barriers concerning accessibility, security, and legislative requirements, including:

- Restricted resources
- Digital inclusion
- Interoperability of technology across siloed teams
- Data protection and legislative compliance

Technology is the solution to improved service delivery but the roadmap remains unclear. This report investigates how public sector bodies can tackle each challenge to achieve effective digital transformation.



Digital inclusion and accessibility

Communication is at the heart of all public sector organisations. A culmination of the global pandemic and digital transformation means that methods used to engage with stakeholders are increasing: social media, email, websites and online forms, portals, file transfer sites, traditional print and post – the list goes on.

So many channels of communication result in a lack of cohesion between departments and frustration for residents. For IT professionals, vectors for data security become broader and harder to maintain.



> Our employees are engaging with a variety of agencies and stakeholders everyday, such as housing agencies, tenants, benefits agencies, NHS organizations, and other councils. Even when emailing other government bodies, we need to secure sensitive data. We recently received a query from the electoral roll. They send huge quantities of sensitive information relating to residents to their poll clerks, for example, and this data needs to be encrypted (...) When we email residents via their personal email address regarding council tax or benefits, we need to protect sensitive data, then, too. The recipient experience is also important to us.
>
> **South Kesteven District Council**

User-experience for employees and service users is vital for all public sector organizations, be it the police dealing with cases of domestic violence, or local authority employees concerned with Looked After Children. When engaging directly with citizens, administrations must take into account all levels of digital ability. Requiring residents to create accounts and navigate clunky portals to engage with their council reflects poorly on the organisation.

Understanding the needs of users is the first step in establishing what solutions will work best for teams: who do employees engage with and what are the specific needs of recipients? What kind of information do they handle?

Often the service users most dependent on local government are those most impacted by the digital divide. Like the majority of developed countries, the UK has a growing elderly population and, today, digital exclusion is a social care issue. Digital transformation sees vulnerable communities left behind and now it is up to local authorities to rectify this issue.

Accessibility is an in-house problem

Last year, the Central Digital and Data Office (CDDO) introduced a cross-government digital and data strategy named Transforming for a Digital Future which seeks to address long-standing digital transformation challenges.

The CDDO acknowledges that, compared to the private sector and other countries around the world, the UK government lags behind in the way it utilizes technology and data to drive efficiencies and improve service delivery.

In fact, according to the National Audit Office (NAO), increasing recruitment challenges left the CDDO concerned that digital teams would not have the skills and expertise to implement the missions outlined in its roadmap. A report published by the NAO details that only **4%** of civil servants are digital professionals – a striking comparison to other sectors, in which between **8-12%** are digital professionals.

The reason for this is two fold: cost and availability. Public sector pay levels simply do not attract the talent needed to address the scale of transformation required, and recruitment is fragmented across the UK, meaning finding professionals with the relevant skills is inconsistent and ineffective.

This presents some serious challenges for IT leaders looking to empower employees to work efficiently and securely.

While compulsory training, cyber attack simulations, and security policies go some way in preventing security leaks, they can also create a fear culture and hinder productivity. In fact, in a study of over 6000 employees, just **67%** had received some kind of data security training in the last two years. Of these, only **36%** stated they have applied their learnings in their core role.

National Audit Office, Digital transformation in government: addressing the barriers to efficiency



IT leaders: What are the barriers to employees focusing on core role at work?

58%
Too much bureaucracy and “process overload”

42%
Too many different IT systems

26%
Time-consuming security processes and protocols

25%
Worrying about other work-related issues

13%
Training programmes that don’t add value to their core role at work

13%
Other IT problems

2%
Nothing

That is not to say that training does not have a place in the public sector. Educating employees in digital security best practice is very important. However, people require more than compulsory training to harness and develop digital skills that have a truly positive impact in their day to day work.

It stands to reason that, wherever possible, the best course of action is to simplify digital initiatives. Ultimately, employees must be empowered by technology to deliver quality services for residents, without putting data at risk.



The problem of interoperability

Digitalization is all well and good but only when delivered consistently, with the needs of all public sector bodies taken into consideration. In this way, interoperability is the enabler to effective digital transformation, empowering administrations to share information cross-departmentally, with residents and other organizations. Simply put, when systems integrate, so, too, can separate teams, increasing efficiency, reducing red tape, and facilitating data flows and engagement between administrations and citizens.

Systems which do not talk to each other cause friction and open organizations up to digital security risks and reputational damage. Incompatibility of technology and IT infrastructures limit interoperability between and within organizations.

Yet, in the wake of tightening budgets, limited guidance, and lacking digital skills, what are local authorities to do? Differing requirements across the public sector make wide-spread adoption of interoperable frameworks nigh on impossible. Legal obstacles also cause friction, as well as legacy infrastructure and technical constraints to name a few. Siloed teams implement platforms to meet their short-term needs, as we saw happen during the global pandemic – solutions today which are causing more damage than good.

Custom built platforms rarely deliver a positive user experience; firewalls can cause blockages when communicating with agency partners, such as the police or private sector institutions. Often, recipients are required to navigate clunky in-house portals and create accounts to access data. Social housing agencies, for example, engage with local authorities with regards to universal credit and adult social care. These teams handle particularly sensitive data and lots of it, and require an efficient, reliable and consistent way of sharing data that ensures compliance. Revenue and benefits teams, for example, cannot run the risk of an accidental data loss incident. Communication methods must be watertight.

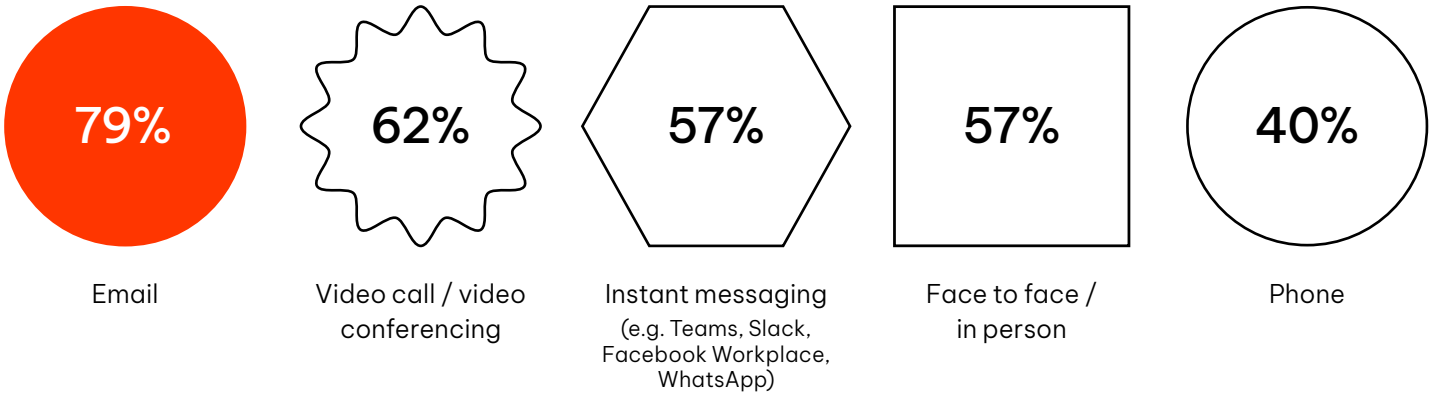
As a result, time-poor employees seek alternative solutions for engaging with stakeholders. For example, when under pressure to fulfil information access requests within a time limit, employees understandably weigh up the consequences between failing to fulfil their duty and risk action from the ICO, and the security and accessibility risks associated with third party file sharing solutions. Often, this is how public sector organisations find themselves in the headlines for a small mistake with the large consequences.



Information Commissioners Office, Action we've taken, Previous Reports

The simplest (and smartest) solution

IT: Methods of workplace communication employees most rely on to get their job done:



Nearly **80%** of local and central government employees rely on email to get the job done. The reason for this is simple; email is universal. Unlike alternative communications platforms, email does not require time-consuming training for employees and does not cause a break in service delivery for implementation. Residents do not need to create accounts to access information. It offers up a convenient and simple way for residents to engage with their local council.

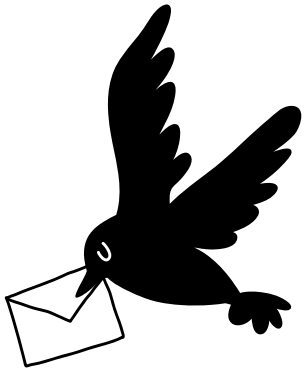
However, IT leaders are all too familiar with the security flaws here. In fact, **45%** of security leaders are concerned about data loss through employee email errors.

According to the ICO, in 2022 local and central government bodies reported the third highest number of data incidents, second only to the healthcare and education sectors.

The reputational damage of a data leak for a public sector organisation is incalculable, comparable only to the devastating financial impact. Of the reported incidents in 2022, nearly **90%** were non-cyber related incidents – i.e. non malicious attacks.

To put this in perspective, over 400 incidents were due to human error, including information accidentally emailed, faxed or posted to the wrong person, failure to redact emails, and misuse of Bcc. These four incidents accounted for more than half of all incidents reported to the ICO in local/central government. In comparison, only 10 incidents were the result of malware and ransomware.

Due to its decentralized nature, security protocols are not widespread across email. The beauty of email lies in its ability to get a message from point a to point b as quickly and efficiently as possible, regardless of the sending and receiving client. This means data is often unencrypted and left open to inception during transit or when at rest.



Information Commissioners Office, Action we've taken, Previous Reports

80% of IT leaders believe smarter email security will reduce employee security errors



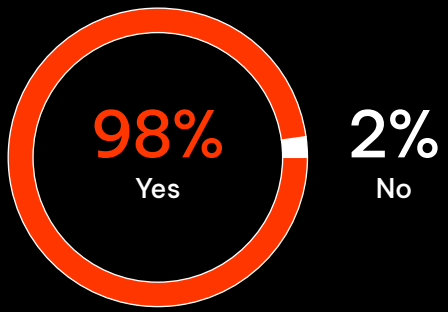
In addition to missing encryption functionality, email lacks a host of security and productivity features needed to work efficiently and compliantly, including file transfer capabilities, email recall functionality, expiration controls, multi-factor authentication – the list goes on.

For example, a neighbourhood officer dealing with instances of antisocial behaviour needs to be able to engage with police, social services, and residents. They will handle special category information regarding the individuals involved and that data must be protected. Traditional email falls short here. If an email is accidentally sent to the wrong person, or the recipient were to forward a file containing personally identifiable information of the individuals involved using cc instead of Bcc, a data incident occurs. There is also no way for information protection officers to track the scale of the incident once an employee presses 'send'.

While email does bridge the gap for siloed teams, it must be enhanced to ensure communications are protected before, during, and after sending.

Employees: Is email the most secure way to send sensitive information?

Central or local government



Expert contribution



Robert Montgomery,
Audit & Governance
Lead Manager,
Telford & Wrekin Council

Modern data management in the public sector

by Robert Montgomery

Part risk manager, salesperson, counsellor and subject matter expert – the modern Data Protection Officer (DPO)/Information Governance (IG) Manager really does have more roles than a bakery!

By far, one of the biggest challenges for any public sector DPO/IG Manager is the requirement to facilitate compliance with the different threads of data protection whilst ensuring an embedded privacy culture exists within the organisation in an environment that requires fast, efficient, cost effective and transformational secure digital commerce/data sharing. It can often feel like knitting spaghetti.

The appetite for consuming data digitally is at an all-time high and increasing daily, particularly with the growing use of, and interest in, AI both on the part of businesses and consumers. The digital landscape now encompasses an individual member of the public wanting digital commerce at a low level through to public sector analytics where teams of people are slicing and dicing significant volumes of both personal and non-personal data to provide senior management with data to support evidence-based service transformation.

Added to this is the complication of digitally sharing data sets securely with partners, suppliers and other third parties. Sharing must be legal and secure but, above all, it must be shared with a stated purpose in mind. A lack of purpose, particularly when digitally processing, can lead to project creep, over sharing and ultimately non-compliance with legislative requirements leading to a data breach.

Embedding a privacy-centric culture in any organisation is the critical foundation on which all data handling should be built but particularly in a world of ever-increasing reliance on digital services processing data. Getting yourself in front of key stakeholders, particularly the senior management team, and communicating simple messages on privacy and good governance is essential; perhaps more important, however, is ensuring they are also aware of any challenges that exist in the organisation which might undermine that privacy-centric culture and how to tackle them. A house will collapse without sound foundations and so will your organisation's digital privacy arrangements without a sound, embedded privacy culture. Get in front of senior people regularly and don't regurgitate the law to them. Know their services, talk business to them and help them achieve their objectives. Information governance is about sound facilitation and not putting speed bumps in the road.

Earlier I mentioned public sector challenges with digital consumption particularly in terms of security,

compliance and overall efficiency of service provision. I think there are common mistakes being made in organisations where the method of digital commerce is shaping service provision and the actual IT solution is seen as the 'end' and not a 'means to an end'. Firstly, the purpose/service requirement should decide the IT solution and not the other way around.

Secondly IT solutions are an enabler to support your purpose and should not 'be' your purpose.

There are lots of powerful digital solutions to allow you to process (store, analyse, share, etc.) vast amounts of data real time, a veritable digital pick 'n' mix. But sometimes in life there can be too much choice. If I want to share data electronically now, I have 6 or 7 different methods to choose from. Are all of these options really needed? Are we confusing end users? Are we implementing new technology for the sake of it? Is this choice creating risk rather than mitigating it?

It's an exciting time to be a DPO/IG Manager. Whether its evolution or revolution that your organisation is looking for, make sure you are in the middle of it and being heard.

Be relevant...always be relevant! Digital transformation, privacy and data protection are here to stay!



Today, we can embrace email without accepting its flaws.

Universal and accessible, email remains our preferred digital communication solution; it empowers employees of all digital abilities.

However, email is also lacking. It falls short on vital security functionality which leaves employees and their organizations vulnerable to the leading causes of data leaks. By enhancing email clients (Outlook and the Microsoft workspace) with advanced (but non-intrusive) technology, IT leaders can ensure compliance, manage employee behaviour without interfering with workflows, and extend security awareness to a company wide culture. Siloed teams can communicate seamlessly, sharing data safely and efficiently across departments and organisations, powering data-driven decision making to improve service delivery for communities.

This technology is within reach for administrations today, in the shape of:

1

Advanced encryption

Through seamless integration with their existing email clients, employees can work within their familiar email workspace, with the added benefit of advanced encryption to protect emails before, during, and after sending.

This technology allows users to effortlessly send secure emails to recipients using public sector DCB1596 accredited domains (gov.uk, NHSmail, police.pnn etc). These trusted domains receive emails sent securely directly to their inboxes like a 'normal' email.

For residents and stakeholders without government domains, the sender can set multi-factor authentication controls to secure emails, (often a code sent via SMS or pre-agreed password) ensuring emails containing sensitive information are accessed only by the appropriate recipient. This does not require the recipient to create accounts or navigate clunky workflows – the process is user-friendly and convenient.

This means that from the moment the email is created, to when the email is accessed by the recipient, the email is encrypted, with the right sized security depending on the recipient and content, with the keys held in a smart and secure way, only by the sender and intended receiver.

2

Seamless user experience

Platforms which require recipients to create accounts and navigate clunky workflows to access communications deliver a poor user-experience, and hinder proactive, effective engagement with residents, government agencies, hospitals, police etc. Email is a reliable and user-friendly platform and, when enhanced with an extra layer of encryption, enables public sector organizations to engage effortlessly and compliantly with all stakeholders.



3

Recall and expiration controls

Microsoft and Outlook make recalling emails practically impossible – functionality which is absolutely integral today for ensuring compliance and protecting employees and their organisations from the leading causes of data leaks.

Enhancing email clients with the functionality to enable email recall allows employees to control access to their email after sending, without time limits. Users can share sensitive data by email quickly and easily, safe in the knowledge that, in the instance that something goes wrong (and naturally, on occasion, it will) they can revoke access to their emails and rest assured a data incident has been avoided.

4

Large file transfer

For fulfilling subject access requests or sharing multiple files and media types, the ability to send large attachments is key for public sector employees across all departments.

Yet this most simple task is often one of the most frustrating. Outlook, Gmail and M365 limit file sizes to just 25MB, forcing employees to switch to third party file transfer sites, often over-complicating processes for both the sender and their recipient.

Keeping file transfer within the native email client supports compliance, streamlines workflows for employees, and ensures accessibility for recipients both inside and outside of the organisation.

"We fulfil a huge number of Subject Access Requests. Previously, we were limited by Outlook which prevents users from sending over 20 megabytes. We had to send multiple emails marked as 'Email 1 of 4' and so on. This wasn't a great experience for the recipient and was time consuming for staff, too. Now it will be a much easier process for all involved." North Kesteven District Council.

5

Data logging

From a data protection standpoint, maintaining an overview of communication performance is key for meeting compliance, particularly with the GDPR.

Automated data logging and certifiable Proof of Delivery tools enable data protection professionals to view the status of every email sent and received within their organisation and beyond, ensuring organisations are prepared in the instance of a data loss event.

"On occasion, it is useful to be able to evidence that an email has been received and opened. For example, if a dispute with a resident ends up in court, we have a complete audit trail evidencing when emails were sent, received and opened." South Kesteven District Council.

6

In the moment error prevention

Sending emails to the wrong person, misuse of Bcc/cc, accidentally sending sensitive data in the body or attachments of emails – these are the most common causes of data loss incidents today. The more data employees handle, the more frequently these mistakes happen.

Empowering employees with smart technology to prevent these errors means people can get on with their days without fear of causing a major data leak. Machine learning technology, embedded within their email client, has the potential to alert users to potential mistakes before they happen, so they can take action to review and correct errors, apply encryption, and ultimately take control over their sensitive communications.

This technology is within reach for public sector organisations today.

By enhancing our most accessible and universal platform with digital security features fit for the digital world, we can meet the needs of both employees and stakeholders – protecting people and their data, without compromising workflows.

Local Government Chronicle, Doing more with less – 2023's challenge for UK local authorities

zivver

To find out more about how Zivver can help your organization embrace the next generation of secure digital communications, please visit zivver.com

