Understanding Secure Email

June 2017

Version 3.0 FINAL

Contributions from:

Mark Brett Programme Director, NLAWARP

Nick Woodcroft, Government Digital Service

Emma Summers and Clive Star, NHS Digital

George McLeod, National Police Information Risk Management, Home Office

Paul Day and Sandie Slater, Bracknell Forest Council

Bob Wilde, Medway Council

Bruce Thomson, London Borough of Hillingdon

Neil Chadwick, Stoke-on-Trent City Council

1. Purpose

We are living and working in an inter-connected environment. The use of email for sending messages, exchanging information and assisting with workflow is commonplace across the public sector.

There will be times when councils need to send and receive personal and sensitive information through email, for example when sharing a citizen's information with GPs and hospitals, the police and probationary service, housing associations, care homes as well as with citizens or citizen representatives.

The use of email sent securely has its benefits in that it can replace paper based processes and can support automation of processes. However, it can be confusing to understand how to do this when individual organisations have multiple arrangements for receiving and sending information securely – or where different approaches are used by organisations across a local area. This confusion can be heightened when there are changes to existing processes, for example the recent changes to the government's current private network known as GCSX and move away from relying on the domain name (e.g. .gcsx) for assurance that the email being received has been sent securely.

Whilst we recognise that it is important that councils and their partners work together to ensure that information is kept safe and secure – it is also critically important that there is a flow of information to support effective public service delivery. The presumption is always to share information for the benefit of the citizen.

Increasingly, councils are adopting platforms that enable collaboration (both within an organisation and across local places) through technologies such as Skype for Business or Google Hangouts as well as shared address books and calendars. These forms of collaborative technologies are changing the way professionals across local areas are interacting, although of course many of these will also supply an email solution.

The purpose of this guidance is to support councils to exchange information in a secure way across multiple organisations to better join-up and co-ordinate their support and services for their citizens. Whilst the emphasis of this guidance is on secure email, it should be read in conjunction with the data handling guidelines[1] which have been produced to assist councils. Similarly, councils and their partners will also need to consider security arrangements when using collaboration tools such as Skype for Business or Google Hangouts.

It is important to ensure that information transmitted between organisations is done so safely and securely. There will of course be a cost to councils for putting in solutions which enable the secure flow of information. Local organisations will need to balance reputational risks, legal implications of fines (through the DPA or forthcoming GDPR which significantly raises the standards that organisations need to meet) and other consequences with the amount they intend to invest in local solutions.

Safe and secure transfer of information can be undermined by poor handling of that information (for example information from the email may be printed onto paper and

[1] Local Public Services Data Handling Guidelines, iStandUK, February 2017: https://www.socitm.net/publications/data-handling-guidelines

mishandled by individuals, teams or organisations). Securing email for safe transmission is only one small part of the process to ensure that information is handled effectively.

This publication is not a technical guide (although it does signpost people to appropriate technical guidance). Rather, it is intended for senior leaders across councils to help them ensure that information is sent safely and securely, supporting the joining up and delivery of local services in an area.

2. What is secure email and why is it important?

Few organisations could function without email. However, when email systems were designed, the world was a different place. The threats we now live with around cyber-attacks did not exist twenty years ago. Today it is even more important that information is exchanged securely and safely, with the risks of information being intercepted or viruses or threats planted because of emails with harmful attachments / links being better understood and reduced as a result.

Of course, these threats can never be totally removed and human error will always be a cause for such breaches. However, by putting in place the necessary security arrangements, by supporting staff, and ensuring that email systems are correctly configured, these threats can be significantly reduced.

Organisations may have different arrangements for sending information securely – these are described in section 4 below. Like other services, many email solutions are bringing benefits of reducing cost, improving reliability and showing continuous improvement.

Organisations in a local area do not need to move to the same email solution / network to send information securely. However, it is necessary that organisations can communicate with one another effectively, using common standards and are able to easily send information which may include personal and sensitive information.

The use of non-governed, non-secure (i.e. poorly configured) email accounts to exchange personal or personal and sensitive information, can lead to information leakage and unauthorised sharing. The risks of loss and damage of this information to the individual can be significant, particularly when it comes to privacy and harm. This is certainly the case when we consider child protection records, adult safeguarding information or medical records. Care professionals in these circumstances will need to consider carefully what information is going to be exchanged (i.e. only the minimum needed) and how that information is shared.

3. What information should be exchanged through secure methods?

The Data Protection Act (DPA) (to be replaced by the General Data Protection Regulations[2] (GDPR) from May 2018) provides a legal requirement for the protection of personal information.

[2] Overview of the General Data Protection Regulation – Information Commissioner's Office: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

As a principle, all personal data should be encrypted (whether sent by information or accessed on a mobile device). The ICO provides guidance on the area of data transfer[3]. This means ensuring that information is adequately protected from the point of transmission. This can be achieved using secure methods as described in sections 4 and 5 below. This will need to include network protection through encryption (called Transport Layer Security), protecting the Domain Network Service (DNS), protecting the integrity of the actual email in transit and having governance in place to reject untrusted / spoofing emails. Rejecting untrusted emails reduces the risk of an individual inadvertently clicking malicious links and activating malware. Care needs to be taken to balance this with an approach which reduces the quarantining of legitimate correspondence.

Secure information exchange however, refers to more than just email. It is about risk management, information governance and network security. There are a number of factors that need to be considered when sharing information. The key principles at the end of this publication supports councils in this area.

There are three levels of Government classification for the handling of information[4]. This scheme operates within the framework of the Official Secrets Act (1911), the Freedom of Information Act (2000) and the Data Protection Act (1998). The classification divides data into three categories – OFFICIAL, SECRET and TOP SECRET.

For councils (and many other public sector organisations such as Health, Fire and Rescue, Community Policing as well as Charities) there is only one classification – OFFICIAL. The threat profile, information risks and attackers may differ, but the OFFICIAL level is consistent across those public-sector bodies. Indeed, all personal information protected under the Data Protection Act, including health and care information, is classified at this level.

Within this, OFFICIAL-SENSITIVE is not a separate level but instead is a handling caveat for a small subset of information which is marked as OFFICIAL which requires special handling by staff. For example, a Council committee report with options for a re-organisation, a child protection file containing Police intelligence information, patient medical files and an internal fraud investigation file could all be marked as OFFICIAL-SENSITIVE. In each of these cases, the marking of 'sensitive' it is about the handling of the data and the 'need to know', i.e. who is allowed to see it.

4. What solutions are available to councils to exchange information securely?

There are broadly four options which councils can use to exchange information securely. The aim for many councils is to make the transfer of information simple and straightforward for end-users. Historically councils have had multiple email accounts - .gov.uk for regular correspondence, .gcsx for secure information exchange and sometimes additional accounts using cloud (portal) encryption solutions. This can cause

[3] Data Transfer – Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/data-transfer/
[4] Government Security Classifications – Cabinet Office: https://www.gov.uk/government/publications/government-security-classifications

confusion amongst staff as to what is the most appropriate solution for sharing information.

The trend now is towards simpler arrangements for council staff (if possible having one, rather than multiple, email accounts). There are a number of councils adopting the Government Secure Standard – using cloud based email solutions (such as Google Apps or Office 365) and putting security in place to enable sharing through the existing .gov.uk domain. This does require clear communication arrangements with partners who may have historically placed assurance for security on the .gcsx (or similar) domain.

It also means that cloud (portal) based solutions or supplementary email solutions that are described in this guidance are only used when there is a necessity.

It is for each organisation to decide what works best for them and their local situation. The aim of this guidance is to support councils by considering each approach in turn.

Secure Messaging: Options for Councils	
Option 1: Cloud or On-Premise Email Solutions (securing to the Government Secure Standard)	Cloud-Based Email Solution (e.g. Office 365 or Google G-Suite)
	On-Premise Email Solution (e.g. Locally configured Microsoft Exchange)
Option 2: Cloud (Portal) Based Email Encryption Solutions	Portal Based Solutions (e.g. Cisco Registered Envelope, Trend Micro, Egress Switch)
Option 3: Extended use of GCSX in the Public Services Network	Extended use of GCSX through the Government Convergence Framework (GCF)
Option 4: Supplementary Email Solutions	Additional Email Services (e.g. NHSmail)

Option A: Cloud Based or On-Premise Email Solutions (securing to the Government Standard)

Increasingly councils are moving towards newer software packages which include email. This includes cloud based solutions such as Google G-Suite (such as is the case in the London Borough of Hillingdon), the use of Microsoft Office 365 as well as ‘on premise’ email services (such as Microsoft Exchange). These can all be correctly configured, using the secure Government standard to enable the effective and secure flow of personal information. This approach can reduce the need for users to having to use separate email accounts or solutions.

Further information on how to correctly configure such solutions can be found on the Cabinet Office pages here and is described in section 5 below: https://www.gov.uk/guidance/securing-government-email

Importantly, assurance and confidence for the exchange of information comes from configuration of the services rather than the domain. As a result, a number of councils are now enabling information to be sent securely using their .gov.uk domain. This means that there will cease to be an emphasis on the domain name providing the mechanism for an email being sent securely. This requires awareness raising both locally and nationally as Councils (and others) begin to use these arrangements.

Case Study: London Borough of Hillingdon – Adopting Government Secure Standard using a cloud based email solution

What is the local approach?

In summer 2015 London Borough of Hillingdon were informed that there would be changes to GCSx and towards the end of 2015 the council decided to be an early adopter of the secure email guidance from Common Technology Services (CTS).

There were several reasons for the change. There were 3,000 users with approximately 600 of them using GCSx email. This meant there were two email clients and complex rules about which email could and couldn't be used. In addition, the ageing email solution didn't fit with the changes the council had implemented in June 2012 when they moved to the use of Google Apps.

How it was implemented

The challenge for Hillingdon was ensuring that all email gets delivered. With the Domain Name System (DNS) controls required as part of the secure email guidance, it was anticipated that there may be a risk that some email could be marked as spam or deleted.

The council rebuilt devices with Windows 7 and then tested them to ensure they met the necessary standards published by CESG. This happened alongside end-user communications to ensure everyone knew what was happening and why it was needed.

The council spent time correctly configuring to the technical standards (including investing the DMARC reports) to ensure that emails to residents were received and not filtered as spam.

Hillingdon Council benefitted from Common Technology Service (CTS) support during the implementation. This helped with advice during each stage as well as on dealing with technical aspects.

More information on the technical detail of the Hillingdon approach can be found here: https://governmenttechnology.blog.gov.uk/2016/11/01/securing-email-in-a-london-borough/

Contact details

Bruce Thomson, IT Security Manager for the London Borough of Hillingdon.

Case Study: Stoke-on-Trent City Council – Adopting Government Secure Standard using an on premise email solution

What is the local approach?

Having followed the progress of the PSN with interest from the drawing board stage to implementation, Stoke-on-Trent City Council applied for access as soon as it was available to local authorities and completed their first Code of Connection. The main driver at first was access to DWP data although the council identified the potential of GCSx email services as a way of securing communications to our public sector partners.

How was it implemented?

Stoke-on-Trent City Council never had the intention of replacing regular email with GCSx. The council established an application process with staff who needed to use it and then set up training (subsequently online training) to support employees. GCSx has proved very popular, particularly in social care and with the teams that regularly communicate with the police.

Around 15% of email users have access to GCSx, which is quite high for a local authority of the size of Stoke-on-Trent (around 5,000 email users in total).

With a vision that the whole .gov.uk domain would be secured, the council intends to cease the use of GCSx from the end of March 2017 using its Exchange on premise solution. The council have followed documentation on how to set up email incorporating technologies to protect against inception and spoofing.

It is too early to say how email users will find the new arrangements, but from the conversations that have happened, it is expected that users will find the new experience positive. The advantages over GCSx include users not needing to log in to a separate mailbox to work securely whilst the list of organisations that have done the same means there is a much larger range of domains that can be contacted securely than in the early days of GCSx and it is growing quickly.

The council are supplementing this with a portal based email where there might be a need for more control.

Are there any outstanding challenges?

It remains to be seen what the impact will be when the new solution goes live – when recipients start to see emails arriving without the familiar "gcsx" in the address. The council has sent communications to regular recipients explaining what is happening.

Of course there is a risk that once staff are aware that the email system is secured they could become less vigilant in the way they use it – perhaps failing to check that recipients have comparable facilities. Training and awareness raising is helping to mitigate against this.

Contact details

Neil Chadwick, Information Assurance Manager, Stoke-on-Trent City Council

Option B: Cloud (Portal) Based Email Encryption Solutions

Personal and sensitive information can also be sent through the use of cloud based email encryption services. Various products are available and these tend to be portal based systems where the recipient has to go to a website to view and reply to the email – such as those described in the two case studies below.

A number of councils have already implemented such solutions in addition to the use of standard email (e.g. using .gov.uk). For example, a number of councils are using this where there is a need for two-way secure flow of information and the recipient organisation does not otherwise have access to encryption tools (e.g. care provider who wants to send and receive a care plan).

These approaches exercise control of the data, who has access to it, allows the data to be remotely deleted and is fully auditable meaning that use by individuals can be traced. These approaches are increasingly being used by car insurance companies, legal firms and other organisations to send information securely.

As some councils move towards cloud-based or on premise solutions as those outlined in option A (securing those to the Government standard), it may be that some councils adopt cloud-based (portal) encryption arrangements where extra control may be needed.

Case Study: Bracknell Forest Council – Portal Based Secure Messaging

What is the local approach?

Bracknell Forest Council chose to implement the Clearswift Secure Encryption Portal. Outgoing emails from the internal email system are classified by the user (through a pop-up when sending) and if either marked as Protect or Restricted the outgoing email will be routed to the hosted Clearswift system. That Clearswift system then sends an email to the recipient advising that a secure email is available for them, and includes a secure link for the user to can log into the portal and retrieve the message. Once logged into the portal, the recipient can also send emails securely back to the originator.

How it was implemented?

The system relies on keywords in the subject field / inserted on the first line of email. A policy on the gateway looks for the keyword and applies the relevant routing. Initially, users were advised to add the keyword manually in the subject field but since then a classifier has been used to force all users to choose the classification on outgoing email.

What are the outstanding challenges?

The classification system (Unrestricted, Restricted, or Protect) is not required, but they still need a method of identifying emails that need to be secured and routed to the encryption portal. The council are considering returning to the use of keywords.

What is next?

The council is currently following the Cabinet Office guidance which will ensure that there is encryption (using Strict TLS) which will mean using their email domain and may limit the use of the encryption portal.

Contact: Paul Day, Chief Officer Information Systems and Sandie Slater, IT Manager Adult Social Care, Health & Housing, Bracknell Forest Council.

Case Study: Medway Council – Portal Based Secure Messaging

What is the local approach?

Medway Council had a requirement to provide a method to transfer files and emails in a secure method. Medway settled on Egress for Secure Email.

How was Egress implemented?

Following the trial period (to test the solution on the network), Medway entered into contract with Egress. Training notes were prepared using the Egress documentation as a guide. Medway have provided an icon that appears on the toolbar on the new email window. Selecting the icon provides three options:

- **Unclassified:** The email will be sent as standard with no encryption
- **Official:** The message and any attachments will be encrypted
- **Official – Sensitive:** As official but recipients will not be able to forward, download or produce screenshots.

What are the challenges?

There has been some opposition to the use of Egress by some local organisations external to the Council. This has partly been overcome through dialogue with partner organisations. There are still some discussions ongoing which emphasises the need for clear guidance across organisations in the public sector.

What next?

In April 2017 Medway Council will start to replace the Microsoft ESA installation with Office 365. This will include SharePoint, OneDrive and cloud based Email. The implementation across the council is planned to take 2 years.

This will provide Medway with a wide choice for secure document collaboration. O365 email provides an encryption service and Egress integrates with Outlook on O365. Additionally O365 allows the user to place a security classification (encryption) on a document, which then follows the document wherever it is sent.

Contact details

Bob Wilde, ICT Change Manager, Medway Council.

Option C: Extended use of GCSX within the Public Services Network (PSN)

Councils have had the opportunity to use GCSX email. This was originally established to get councils inter-connected to Government Department's using GSi email for example with DWP (you can identify this by the domain .gsi.gov.uk email address). Many councils have used GCSX (.gcsx.gov.uk) email for sending personal and sensitive information.

Councils have been able to purchase GCSX email through the Government Convergence Framework (GCF). Up until now the GCSX (and Government GSi email) has been provided by a single supplier. This historically has been Cable and Wireless

although they were acquired by Vodafone in April 2014 and currently provide services under the GCF.

As of the1st April 2017, councils now have a choice over the provision of email services (in the same way that there is now a choice of PSN network providers). The current single supplier approach has come to an end, although Vodafone will continue to offer a commercial version of GCSX email.

Vodafone have also committed to carry forward existing services where customers intend to purchase their future commercial GCSX offer. This offering will come with all of the services which formed part of the GCF.

However, this option is not a long-term solution. GCSX arrangements will only be continuing until March 2019 so councils need to be putting plans in place over that period for how they will move away from this.

As highlighted above, there has been a change of Government policy meaning that councils can use their own email services (those outlined in option A). Correctly configured these can be deemed 'secure' at the OFFICIAL level.

Option D: Supplementary Email Services (e.g. NHSmail)

Of course, some councils may wish to choose to use other solutions in addition to their core email solution. For example, some councils have secured a small number of NHSmail accounts to enable the use of shared calendars (e.g. to support integrated or multi-disciplinary team working).

As it becomes more commonplace to share infrastructure and platforms that enable organisations to use instant messaging across organisations or have access to shared calendars or address books across multiple collaborative solutions then having multiple email solutions could challenge this principle aim.

Councils may also be interested to know that a number of care provider pilots (care homes and home care) have or are in the process of establishing NHSmail accounts which can be obtained from NHS Digital[5]. This includes work with the Care Home Vanguards as well as plans for broader rollout later in the year. Guidance[6] is available for care providers to support their IG Toolkit submission, which will need to be in place if care providers are using NHSmail.

A new nationally provisioned solution for supporting care homes onto NHSmail is in development which will provide a central support model for provisioning accounts and for on-going support once the accounts are enabled. Pilots for the national approach, which are expected to commence by the autumn, will remain dependant on IG compliance.

[5] Joining NHSmail - https://portal.nhs.net/Help/joiningnhsmail
[6] Guidance for Care Homes completing their first IG Toolkit - https://www.igt.hscic.gov.uk/WhatsNewDocuments/Guidance%20for%20Care%20Homes%20on%20Completing%20their%20first%20IG%20Toolkit%20v2.0.pdf

5. How organisations can be assured that the information they are receiving from councils has been sent securely

It will be important for organisations (and individuals) to know that the information they are receiving has been sent securely. Historically the emphasis has been to rely on the domain the information is being received from e.g. the email address is .gsi.gov.uk or gcsx.gov.uk. Vodafone still provides the GSI mail service and councils can continue to buy this service including GCSX email from Vodafone as part of the bundled service offering highlighted above.

However, it is important to be aware that assurance and confidence for the exchange of information does not come from the domain (e.g. .gsi.gov.uk or .gcsx.gov.uk) but rather from the configuration of the services used to support and deliver the email.

The direction of travel is that all councils (and Government departments) will be encouraged to move to a simplified .gov.uk domain and move off networks like GCSX. Of course, some councils may wish to retain the .gsi.gov.uk / .gcsx.gov.uk domain where the .gov.uk domain meets the secure email assessment criteria.

This can be done without purchasing .gcsx.gov.uk services from Vodafone. Government departments are themselves moving to the simplified .gov.uk domain, for instance @cabinetoffice.gov.uk.

The Government Digital Service will maintain a list of domains which have been correctly configured known as the whitelist which, organisations (and individuals if necessary) can use to ensure that the information they are receiving is from a domain that meets the necessary standards.

The electronic whitelist is part of the domain information service[7] used by the domain configuration tool and is integrated into the email service configuration as a validation rule. Whilst it is possible to login in and look up whitelisted domains, we recognise that for hard pressed frontline staff that this is not practical.

The intention is towards using the whitelist and building this into the automated email configuration service so this will automatically check the sender's email address is recognised at an organisational level so that users do not need to check this individually. **It does however require organisations to be made aware that they should not place reliance on the .gcsx domain name.** As a result it is essential that organisations work together in notification and implementation of these changes.

6. How councils can be assured that the information they are receiving from other organisations has been sent securely

Whilst the guidance above has explained approaches that are being used by councils, there is a need for councils to interact and exchange information with other services who may have alternative solutions or approaches. This section therefore provides details on the approaches by key partner organisations. This is not intended to be

[7] Domain Information Service - https://domaininformation.service.gov.uk/

exhaustive but provides an overview of key sectors, their approaches and how they interact with Local Government.

- **NHSmail - .nhs.net**

NHSmail provides 'opportunistic' encryption to all sent and received email. This means that if the receiving or sending system is able to encrypt the transmission between NHSmail this is automatically done but if an encrypted connection cannot be established the email is exchanged with no encryption. NHSmail users also have the option of using a built in encryption service to non-secure email systems.

NHSmail is free to the health and social care organisations that meet its access policy and who may find it easier to use already configured email services. It includes Skype for Business instant messaging and additional options are available for storage and video conferencing.

In addition, the NHS has created its own Secure Email Standard[8] (SCCI1596). This establishes the minimum security requirements for email systems in health, public health and adult social care. Under the 2012 Health and Social Care Act, health and adult social care organisations must have 'due regard' to the standards. As a result, all organisations delivering health and social care services are expected to meet this standard by September 2017. NHSmail and Office365 (if correctly configured) already meet this standard and others are also in the pipeline. NHSmail has also been recognised by Cabinet Office as a suitable secure email for inclusion on the GDS whitelist. Organisations can self-certify conformance and good practice is available to support this[9]. Health organisations self-certifying will be required to use the domain .secure.nhs.uk.

The following domains currently meet the standard:

- **Health and Social Care using** .nhs.net - NHSmail
- **Local Government / Social Services** using .gcsx.gov.uk
- **Central Government** using gsi.gov.uk, .gse.gov.uk, gsx.gov.uk
- **Criminal and Justice using**.cjsm.net, .scn.gov.uk, .pnn.police.uk
- **Military using** .mod.uk

With the introduction of local email solutions (option A above) it means there will be a significant increase in the number of secure email domains available for use. It will no longer be practical to expect users to remember, or check, which domains are secure.

Going forward, users of NHSmail are being advised to use [secure] in the subject line. Given the growing number of localised secure email domains NHSmail will either send the email securely to a secure domain or encrypt the email if the recipient domain is not secure.

[8] NHS Secure Email Standard for Health and Social Care Organisations: https://digital.nhs.uk/nhsmail/secure-email-standard
[9] Guidance to support self-certification against the NHS Secure Email Standard: http://systems.hscic.gov.uk/nhsmail/emailstandards

Importantly, **organisations with Public Sector (HMG) certification do not need to accredit to the NHS standard as well.**

- **Criminal and Justice Services – cjsm.net**

The Criminal and Justice Secure Mail (CJSM) is operated on behalf of the Ministry of Justice. Egress is the current provide of this service.

The CJSM network is a closed community dedicated to processing information between parties involved in activities associated with the Justice Community. Being a closed network only members of the CJSM service can communicate between each other.

There are exceptions to these e.g. where an existing secure email solution is being used or the domain has been approved and registered with the CJSM platform.

Providing there is a business need connected with the Justice community (e.g. children's services), and if this is needed locally, then councils can continue to register for the CJSM platform at no extra cost and the .cjsm accounts will continue.

Egress will be providing significant upgrades to the service over the course of the next year as new capabilities are deployed which will broaden the service offering to end users.

7. What can national organisations do to support councils?

It is evident that organisations or sectors do not have a 'common email solution' for exchanging information. It is therefore important that national organisations support the most effective exchange of information whilst ensuring that there are standards in place that make sure this information is kept safe and secure.

There is a need therefore for common standards and approaches with different parts of the public sector (NHS, Government Digital Service and Government Departments) working together to ensure there is an aligned and consistent approach.

Our recommendations are therefore that:

- GDS / Cabinet Office leads collaborative working across Government and with Local Government to ensure that there is a common understanding of the known issues and agreed solutions which are published and promoted.

- That resolution is found to help organisations and individuals recognise and check easily that the information they are receiving is sent with secure configuration. At present there are a variety of approaches (e.g. assurance that an organisation is communicating with another organisation securely is based on the domain e.g. secure.nhs.uk vs assurance is on a white list held by the Government Digital Service).

- That there is collaborative work across Government and with Local Government for individuals working in the public service to raise awareness of threats and standards for safely and securely handling information. This should align with the General Data Protection Regulation engagement plans.

- That there is ongoing work with Government to refine the current white list approach so this is more user friendly to enable frontline staff easily identify they are exchanging emails with a trusted source.

Key Principles for Councils

1. **Keep personal / sensitive information in emails to the minimum necessary for the task.**

If you using a remote, mobile or portable device, only carry the minimum amount of information with you. For instance, a care worker who works remote from the office and uses a tablet for client records, set the email preferences to only store a week's worth of email on the device. This reduces the amount of information held and minimises the threat if the device is lost.

2. **Only use email when there isn't an alternative.**

Email is not the best medium to use for communicating personal / sensitive information. Over the years email has become pervasive. Some email systems provide flags, markers or categories. Use these to clearly identify those emails which contain personal / sensitive information. This makes it easier to manage and delete these emails as soon as possible.

3. **Talk to partners, discuss and understand the flows of information to be sent by email. Regularly review and discuss agreements and decisions made.**

As organisations change their methods of sharing information securely (such as in the options described in this paper) it is important that there is a dialogue with partner organisations to whom information is going to be sent to ensure they are aware and are able to test this flow of information. This should be regularly reviewed across local organisations.

4. **Do not store personal / sensitive information in emails for longer than necessary**

Only keep emails with personal information in them for the minimum time necessary to complete the task. This is especially important for portable and mobile devices.

5. **Always consider the environment you are in, when accessing personal / sensitive information.**

If you are not in your office environment, be aware of your surroundings, especially if in public places, in the home of clients, on public transport etc. Can you be overlooked? Can unauthorised people see the information your reading or what you are typing?

6. **Always check with the owner of the information before forwarding it to a third party.**

It is very important to "Think before you click" especially when entering email addresses and forwarding personal / sensitive information to a third party. Do you have permission to send the information? Is it your information to send? Do not forward work related emails with personal / sensitive information to personal email accounts.

7. **Avoid storing and accessing personal / sensitive information on untrusted devices.**

If you use your own device for work, think very carefully about what you access and store on your own device. You do not own that data. If the device is lost or stolen there could be real issues.

8. **If you are not sure about anything relating to personal / sensitive data, seek advice.**

If you are not sure about anything relating to personal / sensitive data, seek advice. It is better to get advice and training than make a mistake that could lead to a data breach, loss or theft.

9. **Always report issues, loss or data breaches as soon as possible.**

You should always report issues or suspected incidents as quickly as possible. This will always allow the most time to solve and fix problems.

10. **Ensure any devices accessing personal / sensitive information are regularly updated and secure.**

Always ensure devices are kept up to date with security patches and that you regularly scan the device. Ensure all security settings are switched on. Regularly delete unnecessary personal information you have stored.