Borough of Poole Staff (Adult Social Care)

Encryption:

Sending secure, encrypted e-mails & attachments

V8

Contents

What is Encryption?

It is a way of making information unreadable to anyone without authorised access. It is not the same as using a password to protect a document – encryption is a more secure option, and is routinely used by many organisations.

The encryption system used by the Borough of Poole (BoP) is known as the Cisco Registered Envelope Service (CRES), or 'Cisco Ironport', and came into effect in March 2010.

Decryption is the means by which a secure message may be opened to read the content.

Why do I need to know about it?

Sensitive information - such as patient and service user data, National Insurance numbers, etc is known as Person Identifiable Data (PID). This type of information is at risk of being intercepted or read by unauthorised individuals when it is sent in an e-mail (or an e-mail attachment) over the internet, and must be protected. Encryption is the safest and simplest way to achieve this.

There are no additional charges associated with using this service and likewise there is no additional charge for the recipient.

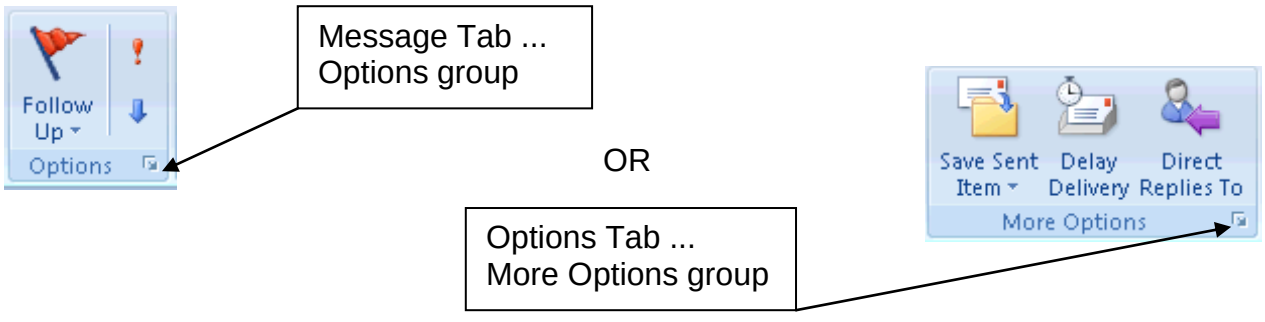
It also ensures we comply with our Information Governance requirements, the Data Protection Act, and the principles of the Caldicott Report.

How do I use it?

To send an e-mail with sensitive information (PID) to an external e-mail address (i.e. not a poole.gov.uk address), the e-mail must be marked Confidential in the Message Options box. To do this first compose the e-mail, then click either on:

- The Message tab > Options group > dialogue launcher arrow
- The Options tab > More Options group > dialogue launcher arrow

... and set message 'Sensitivity' to 'Confidential' (as shown on the next page).



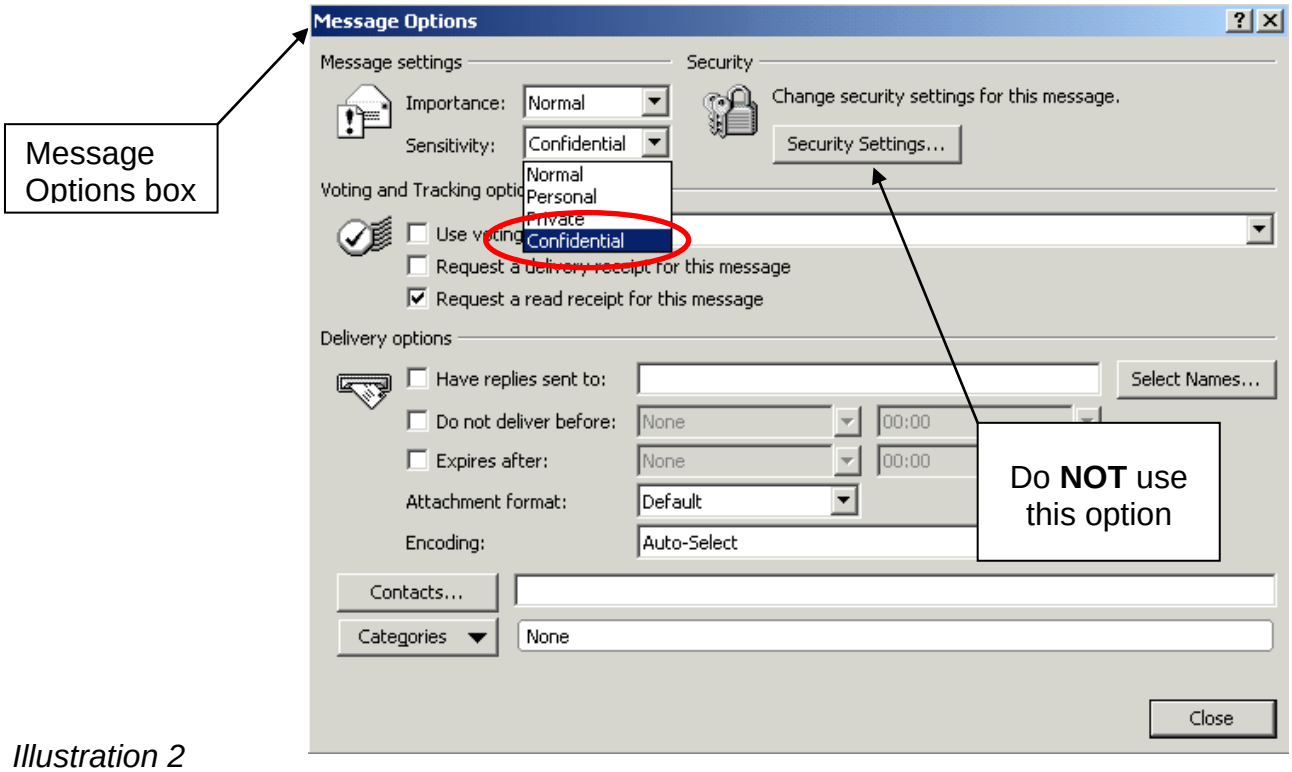


Illustration 2

The e-mail and any attachments are now ready to send.

What should the recipient expect?

The first time your recipient receives an encrypted e-mail from the Borough of Poole they will have to register with the CRES, for which there is no charge.

> The e-mail they receive will guide them on how to do this, and their employer/in-house ICT dept should provide any additional support. However a supplementary Private & Voluntary sector guide also exists for their use – see 'Assisting the Recipient' on pages 6 & 7 of this guide.

Registration is a one-time only activity, and thereafter they will only have to enter their password 'key' (which they set when registering) to open subsequent encrypted e-mails and their attachments.

Passwords

The Borough of Poole ICT Helpdesk cannot assist with lost or forgotten CRES passwords. If this happens the recipient must use the 'lost password' link (shown right) which is included in the encrypted message they receive. See 'Assisting the Recipient' on pages 6 & 7 of this guide.

Who can read them

Once you have clicked Send, the e-mail will be intercepted by the encryption system and rendered unreadable except by the intended recipient(s).

However they cannot be forwarded to the third party: if they are the e-mail will remain unreadable even if the third party recipient has already registered with the CRES service. Only those copied in to the *original* e-mail can open and read the content of the encrypted e-mail.

All attachments in a confidential e-mail to an external address will be encrypted. This includes Adobe PDF and Word documents.

Once sent you receive an automated confirmation (as right) that your message has been encrypted. If you – the sender – do not receive this, your e-mail has not been encrypted! Should this happen, contact the ICT help desk immediately.

Note: the encryption system used by the Borough will scan for some keywords in outgoing e-mails to help ensure no sensitive information is sent out unprotected: this includes attachments. You may therefore discover that the encryption system occasionally auto-encrypts an e-mail or document containing text it has deemed to be confidential.

Nevertheless, the responsibility always lies with YOU, the sender, to ensure such information is protected by selecting the Confidential message option in Outlook (as described on pages 3-4 above)

What items should be encrypted?

Any email and/or document that contains PID (Personal Identifiable Data) which can identify someone or includes sensitive information about them - e.g.:

- health or social care information
  - including the fact that they are 'known' to Social Services
- financial information
- personal information including:
  - names
  - addresses
  - phone numbers
  - bank account details
  - relationships or associations
  - behaviours
  - background information
  - case history
  - criminal records or questionable activities

... and so on.

In additional it should only be sent to someone who has a genuine need to view the data. If in doubt ask yourself:

“Is the information, which I am about to email, something I would be willing and comfortable to share if it related to me?”

Assisting the Recipient

IMPORTANT: if the recipient is using a generic e-mail account, ie it is used by several members of staff, it is their responsibility to note down and store the password and answers to the security questions (created during the registration process) in a secure place where colleagues can access them should, for instance, the person who registered with CISCO then leave.

- If they have mislaid or forgotten their password, they should click the ‘forgot password?’ link (as right) to prompt a link to their security questions. Five wrong attempts will lock them out for one hour.

- If they have forgotten/mislaid both the passwords and answers to their secret questions, they should e-mail cres-support@ironport.com, or call them on 0800-917-5578. *BoP staff cannot request their password is reset for them*.

Recently, some NHS e-mail domains (addresses) have joined a scheme that auto-encrypts all e-mail traffic between BoP and themselves. HOWEVER, not all domains are included and ICT Security advises that all sensitive data should continue to be encrypted as above to all domains.

The following page gives a summary of typical issues and actions

Typical Issues and Actions

ISSUE	ACTION
External Recipient	
The recipient does not know the password associated with an e-mail address	They should use the 'lost password' link on their e-mail. CISCO will send a 'New Password' message to their email address containing a link to their security questions. They should answer the questions to access the 'Create New Password' page. If they answer incorrectly 5 times they will be locked out of their account for one hour. If they have not specified security questions, the 'New Password' message contains a link to the 'Create New Password' page. They should choose a new password, and use it to log in to their account.
In addition to above, the recipient does not know the answers to the secret questions prompted by using the 'lost password' link	They need to reset their password and should e-mail cres-support@ironport.com requesting their e-mail account is reset (and include the e-mail address affected). OR they can phone CISCO on 0800-917-5578. NOTE: Borough of Poole staff can ONLY request password resets for BoP staff. The user should also be reminded to keep their password and answers in a secure central place accessible by those who need to use it in the future.
The recipient receives normal e-mails, but not encrypted e-mails	This is almost certainly a local issue such as a spam filter or pop-up blocker that needs addressing by their own ICT provider. May also refer user to page 10 of the P&V User guide on the BoP website.
When trying to save the attachment, the recipient receives various error messages: '*This type of attachment must be saved to disk. Right click the link and then click 'save target as' to save the attachment.*' or: '*securedoc.html cannot access this file; check security privileges over the network drive*'	The user should first contact their own ICT provider as it is likely to be an issue with their local settings barring them from downloading encrypted data.
The recipient receives an error message ' *system is unavailable, try again later*', or they cannot type anything into the password field	This is probably a Java (computer software) issue that should be dealt with by the user's own ICT provider.
The recipient cannot progress beyond opening the 'securedoc.html' attachment, eg the 'Open' button does not appear; their e-mail address does not show in the 'To' field; the password field does not show	They should forward the entire e-mail to mobile@res.cisco.com. In return they will receive an e-mail with a link to the encrypted message which they can open by entering their password

BoP Worker	
The BoP worker receives an error message relating to 'certificates' when trying to encrypt an outgoing e-mail:	They have probably clicked on the 'security settings' button, rather than selecting the confidential flag as indicated in the user guide
The BoP worker does not know their Ironport password nor the answers to their *own* secret questions prompted by using the 'lost password' link	They should contact the ICT Help desk to raise a work order requesting CISCO initiate the process to reset the worker's password.

Receiving & Managing Encrypted E-mails

Separate instructions exist to guide users through the process of registering for the encryption service itself, enabling them to receive encrypted e-mails from external sources. Click on the following link to access them.

- **How to Register ~ click here** to open the BoP website where the External Recipient (P&V) user guide can be downloaded on the top right of the screen. It includes instructions on registering for the service and managing received e-mails.

Notes about encryption

- Under the Data Protection Act and in line with the Caldicott Principles, the responsibility for protecting service-user information lies with each of us, especially when sharing this information with other authorised bodies. This includes our NHS partners, other Local Authorities and social care agencies.
- The e-mail encryption service is currently available to Borough of Poole Adult Social Care staff, as well as a small number of other service units.

What emails will and will not be encrypted?

- Only e-mails which are marked Confidential in the Outlook 'Message Options' AND are being sent to external e-mail addresses e.g. to a.n.other@glasgow.nhs.uk, or a.n.other@yahoo.co.uk etc will be encrypted.
- Confidential e-mails sent to Government Connect (GCSX) e-mail IDs will be encrypted
- Confidential e-mails sent to internal BoP e-mail addresses will NOT be encrypted
- Confidential e-mails sent to an internal e-mail address but not in Adult Social Care and then forwarded to an external e-mail address will NOT be encrypted
- Calendar appointment messages which contain sensitive information AND are being sent to external e-mail IDs will be encrypted
- Encrypted e-mails forwarded to a 3rd party will be unreadable to the recipient unless they were copied in on the original e-mail

Dos and Don'ts

- If there is any doubt always use the 'Confidential' message option and encrypt the e-mail
- Never assume that someone else or the encryption system will handle confidentiality on your behalf
- Do copy (cc) other persons who you believe should have access to the information on a need to know basis, as other recipients of your e-mail will not be able to forward your encrypted message
- If a recipient of your encrypted message decides that someone else (a 3rd party) should have access to the content of your message they may either:
    - Contact you as the sender to forward a copy to this 3rd party / person
    - Copy the information from the 'decrypted' message to their computer, then forward it themselves in a secure manner to this 3rd party / person.
- Do not copy (cc) other recipients of a confidential message 'just in case'

- **Remember:** the responsibility for the secure transport of sensitive / confidential information rests with YOU, the sender.

For more information on encryption please see the Ironport e-mail link on the ICT Security homepage.

Manual links to further support (copy & paste links into browser):

- Cisco Customer Support: https://res.cisco.com/websafe/help
- Guide:http://www.ironport.com/pdf/Cisco_Registered_Envelope_Recipient_Guide.pdf
- FAQs: https://res.cisco.com/websafe/help?topic=FAQ

MY NOTES