

Information Sharing – Use of Secure E-mail

Background

The Council has a responsibility to its citizens and businesses to respect the confidentiality and sensitivity of information they provide, in particular when such data is covered by the Data Protection Act.

The Council is permitted to share such data with other organisations provided that the any such information sharing is either with the consent of the data subject and/or is permitted by the Data Protection Act. Note, whilst we do not always require explicit consent to share data, it is good practice to inform the data subjects that we may share information about them, and the reasons why we do this.

Recent Examples of Unsecure Data Sharing

There have been a number of examples of data loss in the last 6 months, including the HM Revenues and Customs loss of customer data sent by post, loss of Ministry of Defence data held on laptops and memory sticks and loss of other data.

One aspect that has until now not been highlighted is the potential insecurity of the normal email system. Most emails are sent in a plain format, are not encrypted (changed into a format that cannot be read unless you have the decode key) and actually travel down the public internet network.

You should not send confidential or sensitive personal information by email outside the council without taking appropriate security measures. Emails transmitted over the internet cannot be guaranteed to be secure from interception or misdirection.

There are a number of ways to improve security of emails; these include purchasing individual encryption keys for each mail user (which is expensive); or joining a secure email network where the email is routed using secure connections. In particular we have two options for sending secure emails that do not require the use of personal encryption devices.

The first option is relatively easy and incurs no additional costs as it uses the Criminal Justice Secure eMail network (CJSM). The second is to apply for access to an NHS mail account via the Primary care trust; this may incur some costs if the PCT decide to pass on the costs of security tokens and configuration work to the Council.

Option 1 - Using the Criminal Justice Email System

The London Borough of Sutton and Sutton LEA (SWAN) have joined the Criminal Justice Secure E-mail service. This service was initially created as you might expect for sending and receiving emails in respect of the criminal justice system; And is run by the government's Criminal Justice Service on

behalf of any public authorities, such as local authorities and health agencies, which have occasional links with the justice system.

This is available to all Sutton staff who have a current email account and there is no additional technical work required to configure your mailbox. However because this forms part of the governments nationally agreed secure systems we can also use this facility to send secure emails to other approved organisations who have their own criminal justice system connection.

Other organisations who are signed up include those shown below:

| Organisation | Normal email Suffix | Secure email suffix |
|---------------------|----------------------------|----------------------------|
| Education | @suttonlea.org | @suttonlea.org.cjsm.net |
| NHS | @nhs.net | @nhs.net.cjsm.net |
| Metropolitan police | @pnn.gov.uk | @pnn.gov.uk.cjsm.net |
| Government Dep'ts | @gsi.gov.uk | @gsi.gov.uk.cjsm.net |
| | @gov.uk | @gov.uk.cjsm.net |
| Councils | @gov.uk | @gov.uk.cjsm.net |
| | @gsx.gov.uk | @gsx.gov.uk.cjsm.net |

The secure email system, however, guarantees that the email you send from you address to another **.cjsm.net** address is guaranteed to be delivered securely to that recipient's network. The fact we have a link to the Criminal Justice System secure network means that emails sent or received with the csjm.net suffix are not routed via the public internet connection but via the secure private network connection.

Anyone with a LBS email address (eg kimbrown@sutton.gov.uk) can send emails securely to someone with a **.cjsm.net** address, and can receive emails securely in return.

To send an email to someone with a **.cjsm.net** address, you simply type their normal address and add **.cjsm.net as an additional suffix** to the end of their standard email address. If you regularly send emails to the same person you can add them to your personal contacts list (address book) with the csjm suffix.

For example, if you normally write to j.smith@merton.gov.uk, you can now transmit confidential information securely by writing to j.smith@merton.gov.uk.cjsm.net or if you normally write to j.bloggs@nhs.net you can now transmit confidential information securely by writing to jbloggs@nhs.net.cjsm.net

Your correspondent can write securely to you by sending their email to kimbrown@sutton.gov.uk.cjsm.net

Make sure you type their address in full: do not accept the "auto-fill" address which Outlook may put in the "To: field when it recognises whom you are writing to.

Who can you write to on .cjsm.net?

To be certain that your correspondent can receive secure emails via .cjsm.net, you have to ask them!

In general, anyone with an address ending **.nhs.net** will be able to receive secure emails from you by adding **.cjsm.net** to their address. The fact that an organisation is a member of **.cjsm.net** does not always mean that all their staff will be able to receive these emails, so check first.

The use of the Criminal Justice Secure E-mail service is fully explained on their website www.cjsm.cjit.gov.uk/, including instructions for other organisations on how to join the network. If you want to encourage your collaborating organisations to use secure email, refer them to this website for further information.

Secure Email at Sutton – Signing up for NHS Mail Accounts

In addition to the use of the CSJM secure email system certain Sutton staff are eligible to apply for NHS mail accounts. This will normally only apply to staff working in adult or children's social care.

This involves the provision of a remote access security token (either a keyfob or a credit card type device) and the installation and configuration of some software. It also requires any staff requesting such to sign an undertaking to agree to the NHS security policies in addition to the Council's security policies.

This would normally be better for staff who either work part time for both the NHS and the Council and/or are engaged on joint projects. The benefit this has over and above the Criminal Justice Email is that it would allow you to access shared calendars and the NHS address book and any global email distribution lists.

This works by setting up a web interface by which you can log onto the NHS email system from your Sutton computer. To access your NHS emails you will have to enter your NHS user name, a PIN code and a random generated number from the security token.

This will be a separate email system to your council mailbox, and could mean you have to check to mail systems both for incoming mail and for diary appointments. This is more cumbersome than using the Criminal Justice Secure email system. If all you need to do is send and receive emails I would recommend you use the CJSJ system; if you need to do more than that and share address books, calendars, task lists then you may need to apply for an NHS mail account.

To apply for an NHS email account the following steps are involved:

- 1 Submit your name or a list of names to Ivor Evans or Chris Brooks at the Sutton and Merton PCT. To maintain an inventory of such accounts you are asked to make these requests via Leandro Barretto or Barry Griffith who will forward your request onto the PCT.
- 2 The PCT will send a you copy of their acceptable use policy, which you will be required to agree to prior to being given an NHS mail account.
- 3 IT staff at the PCT will then forward your request to their IT service desk who will arrange for the account to be created and will notify you when this is ready.
- 4 You will then have to contact the PCT service desk to book an appointment for physical configuration and to sign and return the acceptable use policy; this will have to be at the Wilson (Mitcham)
- 5 Once this has been complete can then log on remotely via a web portal from LB Sutton offices, or from home
- 6 Users must send and receive email form the NHS accounts, both email addresses have to end nhs.net