

LEWISHAM CALDICOTT GUARDIAN CIRCULARS

Lewisham's Caldicott Guardian is John Agboola ext 48676

To discuss this or any other information or security matter, you should contact David Barlow, Information Governance Manager ext 46736



LEWISHAM CALDICOTT GUARDIAN
CIRCULAR # 1 October 2007

Use of USB Memory Sticks & other storage devices

Over the last few months the use of USB memory sticks (also known as Flash Drives) has been increasing as the availability of these devices has grown and their costs fall.

Staff need to be aware of the security issues surrounding the use of these memory sticks, and, to consider the use that they put them to.

Personal identifiable information should not be stored on memory sticks that do not use encryption (that's a technical way of "scrambling" the information so even if it is viewed it can not be read by unauthorised individuals).

If you use memory sticks to store information from your workplace you must consider the following :-

- Do you really need to store this information on an insecure device?
- If the answer is "yes" be clear why you need to do this and perhaps discuss the matter with your line manager
- Does your memory stick contain personal information ?
- If the answer is "yes" you should let your line manager know you are storing this data in this way.
- If you really must use the memory stick and take it off Lewisham premises you must ensure that the memory stick is password protected. This is easy to do and gives a small measure of security but is not encryption and is not tamper-proof.
- Be aware that you have a personal responsibility under the Caldicott Principles and the Data Protection Act to ensure that you do not use personal identifiable information unless absolutely necessary, and this information must be kept securely at all times.

What the Caldicott Guardian is doing

Lewisham's Corporate Security Manager is looking into the security issue of all storage devices that can be removed from our premises (laptops, tablets, PDAs, phones, USB memory sticks etc).

A policy will be made on how best to manage these security issues & you will be advised on what you need to do to safeguard information.

In the meantime please be aware of the security implications and protect your USB memory sticks and any other mobile devices that you may use with password and encryption (if possible).

UPDATE on the use of USB "memory sticks" & other devices

The following advice is current and comes from Simon Berlin's Technology & Transformation Team workspace (mentioned IN Circular 2, below) :-

" If information put on such a device is of a sensitive or confidential nature and is lost or stolen then there could be legal and other implications. These devices should not be in general use to store any personal data, whether encrypted or not.

USB memory sticks are not totally reliable and could be corrupted or damaged making retrieval of the messages impossible. Such devices are easy to lose and data on them could be compromised.

If you are using these devices to store or transfer personal data (particularly where such data is merely a "copy" of data held on the LBL network) **you should cease to do so immediately.**

Portable devices may be used to store or transfer "non-personal" data although it is recommended that such use is keep to a minimum".

There will be ongoing advice on this matter.

LEWISHAM CALDICOTT GUARDIAN
CIRCULAR # 2 December 2007

Information Security & Data Protection

You will all, of course, have heard about the loss of sensitive data between the offices of Her Majesty's Revenue & Customs and National Audit Office.

There are many lessons to be learned from this catastrophic loss of personal data and of course many questions raised which will, in time, be answered by the various internal enquiries.

However tempting it is to point fingers and apportion blame it is vital for us all not to allow this episode to turn into a knee jerk reaction against technology.

The lessons for us are clear - the way that we manage and handle our data must be more transparent and we must all take personal responsibility for our part in keeping this data safe and secure. These actions must also be subject to greater scrutiny.

We all share our own personal information in many ways these days and we must all take responsibility for what we share and when we share it. Remain vigilant at all times and do not be fooled by spoof emails. Remember you will never be asked to disclose your user name or password by any legitimate organisation.

In our work for Lewisham and its customers better information sharing has major benefits - it can cut costs, speed up transactions , cut back bureaucracy, avoid duplication, and help keep the vulnerable safe.

Joined-up services are what we are aiming to provide. At a recent House of Commons Home Affairs committee hearing on the "surveillance society" much of MPs' criticisms commented that there were too few joined-up systems, rather than too many !!

What is Lewisham currently doing ?

Following the revelations about HMRC we are conscious that Officers throughout the Council may be reflecting on their responsibilities for storing and transmitting data and other information.

Our Technology & Transformation Team have set up an helpful workspace where you can raise concerns & queries . These questions can be viewed by all (if appropriate) and offers an opportunity to us all to ask those questions that you have always wanted to ask !

The workspace site also points you to further documentation and guidance available on SharePoint , and to key contacts expert in this area.

You should have received this link in an email from Simon Berlin (Head of Technology & Transformation) . Take some time to have a look at the workspace Concerns Regarding Information Security & Data Protection

<http://team/sites/PQP/Concerns%20Regarding%20Information%20Security%20and%20Data%20Protection/default.aspx>

Lewisham are also reviewing all staff guidance in these areas to make sure it is easily available, clear and unambiguous. Keep an eye open for leaflets, flyers, and electronically delivered information.

The lost data disks at HMRC are indeed "an extremely serious failure" (Alistair Darling MP Chancellor of the Exchequer) but the lessons from the failure must be used to draw our attention to the areas and issues that need our attention within our own workplaces and in Lewisham Council as a whole.