Keeping e-safe?

- Employees must remember that they are contractually bound to keep council business confidential.
- **Discussing council business on social networking sites may give rise to disciplinary proceedings.**
- Your Social Networking site is not the place for a “rant” or to let off steam about work.
- **Do not transfer confidential information from work onto your home PC. Try to use ESCC supplied equipment for all work-related matters.**
- If you have got work related material of a confidential nature on your home PC, you need to think about how it will be securely deleted. Talk to CRD ICT about this.
- **E-safety is never done. New opportunities arise all the time and the purpose of the technology is to make life easier.**
- Data owners have many rights under the Data Protection Act and Human Rights Act. Data users have a responsibility in law to use the data **only** in accordance with the Privacy Notice **and** to take due care of it.
- **Together, we can make E-Sussex, E-Safe.**

Further information

People are innovative, thinking human beings. They will find ways of streamlining processes and workloads, but they may not be aware of the legislation affecting what they do.

This legislation changes frequently and is not always well promulgated. CEOP e-safety ambassadors are available through the e-safety working group.

It is far better to report an issue and have it found to be a non-event, than to not report something and hope it will go away.

We need to understand what risks we are dealing with in the County and only by teams reporting when they have experienced a problem can we build up the database we need to target support efficiently.

The Bare Bones of e-safety

(A general guide for all teams and departments)

East Sussex County Council

eastsussex.gov.uk

In a nutshell….
E-safety is divided into two areas. One is the physical environment and ensuring that adequate anti-virus, anti-spyware and anti-malware systems are in use, and that any wireless networks are secured to at least WPA2 standard.
By far the biggest area however, is adopting safe practices when using the technology. E-safety is largely a behavioural matter. There is also an element of being able to recognise when risks are developing in an increasingly sophisticated world. Identify theft and other threats are becoming increasingly realistic.

Step one…
What technology are you engaging with for your day-to-day-business? An audit is a good place to start. You should also accept that over time, behaviours and practices can creep in that make your team or department vulnerable. They may have been started with the best of intentions, but laws change and you may be at risk without knowing it. There is a lot to be said for an external audit or consultancy to identify this. Some team members may be reluctant to divulge what they have been doing to a line manager, but will do so to an external consultant, particularly if they are guaranteed of anonymity.

Step two…
What do you need, to carry on with business as usual, or to advance your business? Do you already have everything that you need or are there new technologies that would result in efficiency savings or a better experience for your clients?

Step three….
The Law. The main pieces of legislation that affect you are the Computer Misuse Act and the Data Protection Act, although there may be others such as the Human Rights Act. Do all your team know what is and is not accepted as good practice?

Step four….
Working patterns and changes therein. Do you have home workers? Do you have nomadic workers? How do they access the data they need for their respective roles? How do they move this data around? Have they got into bad habits?

Step five….
Your clients. How do they engage with technology? Are you using the best systems for them too? Do they know, by way of an up-to-date privacy notice how their data is being used? Are there opportunities for efficiencies in changing the way you do things?

One of the most difficult things for managers is to listen to the horror stories and maintain an arm's length distance from it. Your staff need to be able to tell you if unsafe practices have developed in a "no blame" culture.

This leads to you designing an Acceptable Use policy. There are some non-negotiables in this which you will find from ICT. (For example, the internet and email training, the customer services training etc.)

How often should I review this?
E-safety is one of the fastest moving areas of safeguarding that there is. New devices and new technologies are available all the time and as we create more and more technically proficient users, they will want to engage with the technology, particularly when they see it as saving them time. It was not that long ago where teachers, for example took all their planning to and from home in a large, (sometimes VERY large) ring binders. Then came memory sticks and then came the learning platform which negated the need to take much information home at all.

E-safety needs reviewing annually. Schools are taking up the offer of an annual half day visit e-safety "Health Check". Teams and departments may like to think about building this into their team development too.

There is a lot of information on the internet, however, it is not efficient for all teams and departments to undertake their own research as we have CEOP trained e-safety ambassadors in house. The e-safety team (e_safety@eastsussex.gov.uk) are your first port of call regarding e-safety matters. If they do not know the answer, they know somebody who does!

Together, we can make E-Sussex E-Safe.