Information Security and Data Protection

When the Data Protection Act 2018 became law in the United Kingdom on 25 May 2018, it represented the biggest change to how data is collected, stored and processed by any organisation in twenty years. We have updated our policies and guidance to comply with the new laws, but it is fair to say it is a complex area.

We have produced a number of summaries to help everyone that works for us understand their role in securing data, and what to do if data about a customer is lost.

• A summary as an employee – this tells you why we hold personal data about you when you work, or volunteer for us.
• A summary as an organisation – this tells you why we hold personal data about customers.

As part of the Act, we have published privacy notices on our website which set out what data we collect, why and how it is used.

We have also refreshed the publication and retention scheme, which launches on 11 October.

A mandatory e-learning package has been developed, and is available via your normal Moodle login here. If you need a reminder of your password. Everyone that works for us is required to complete the e-learning, and the associated post-course assessment by 14 December 2018. For on-call staff a payment of one hour at flat rate is payable.

The e-learning gives simple tips on how to protect yourself and the organisation from the risk of losing information, and potentially receiving a fine from the Office of the Information Commissioner.

What should I report?

You should report any incident where you think the personal data of either someone that works for us, or a member of the public has been lost, provided to someone else that shouldn't have it, or changed without permission. The following are fictitious but plausible examples:

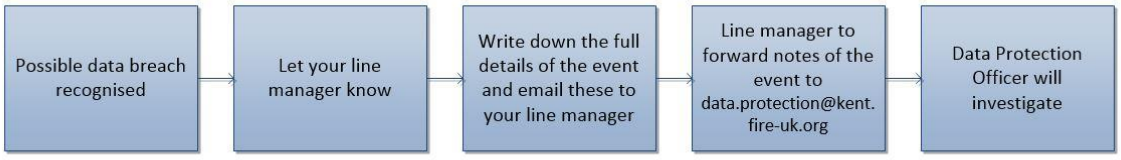
• You work in the Safe and Well team. You have printed a list of names and address of today's home safety visits. When you finish an appointment, you can't find your list and think you have left it at the last visit you made. Although obviously you should go back and get it, the loss should be reported as for a period of time the document is out of our control.
• You are sending a letter to all staff. But in creating the mailmerge, an error occurs where the wrong names have been attached to the wrong addresses. This is not realised until you start receiving queries from recipients. This should be reported as the content of the letter could have released sensitive data
• You are given access to a team SharePoint site as part of your work. In looking through the site, you come across a file which when you open it, lists the days sick taken by members of a particular team. This should be reported as it is sensitive personal data which you don't have permission to view. Holding the data in a team site may be reasonable, but it should be password protected.

Now I know what I should report, how do I?

We do not expect everyone that works for us to have detailed knowledge of the Data Protection Act 2018. We do expect everyone to have an awareness of the principles though – namely if it feels

wrong, report it. If you know, or even suspect, a loss has occurred [technically known as a breach] tell your line manager, in writing. In your note give as much detail as you can.

Recognising a Breach



What might happen to me if I lose data?

Accidents will happen, and losing data occasionally is inevitable. It is far better to be honest and report, than hope it goes away and no one notices. If you lose some data, and it's a one off, than sanction is unlikely, depending on the scale and sensitivity of the data.

If any data is shared without permission outside of KFRS, then that is a different issue and could be investigated under the Authority's Code of Conduct.

A member of my team has reported a data loss to me, what should I do?

The first step is to make sure that the note is comprehensive and includes all relevant details. Once you are happy with it, forward it to data.protection@kent.fire-uk.org. It is important to remember that we have 72 hours to notify the ICO of any significant losses. The DPO will then be in touch.

Need further guidance?

Email data.protection@kent.fire-uk.org