In the Know....

IT Security & Data Protection

The Information Commissioner has issued guidance for small businesses on how to ensure their data is kept securely to reduce the risk of data protection breaches. Here, we take a look at what the guidance contains.

What is caste?

Under the Data Protection Act, employers are responsible for the security of personal information collected and used by the business. The ICO has released a practical guide containing tips for small businesses on how to keep IT systems safe and information secure to avoid breaching data protection legislation.

Assessing the risks

The first step to improving practices or introducing new systems is to look at the current situation regarding personal data and to assess the risks to the business. To decide what level of security is needed, employers will need to review the personal data held and examine all processes surrounding the collection, storage, use and disposal of data. Consideration should also be given to how sensitive, confidential or valuable the information is and what damage this could cause to the individuals if security is breached.

Importantly, putting measures in place does not have to be difficult or expensive for employers to do. If there is only a small risk, then putting in place small measures may be sufficient to eliminate this. The UK Government's Cyber Essentials Scheme recommends introducing five key controls and these range from installing internet protection such as firewalls through to controlling access of data by simple techniques such as usernames and passwords.

Securing data on the move

It is an important part of many job roles that information is required to travel from place to place, usually via a form of mobile equipment such as laptops, mobile phones or USB drives. The inevitable loss of equipment can mean that personal information is vulnerable to be accessed so steps should be taken to prevent this. This could be through increasing the physical security of devices, such as locking them away when they're not in use, or preventing the accessibility of information through ensuring control systems, such as password protection on files, or through encrypting data held on these devices.

Training staff on data protection

Large numbers of data protection breaches occur through accidental disclosures by staff who are unaware of laws regarding personal information. Simple errors such as sending an email to the wrong person or opening a link containing malicious software will constitute a data protection breach. All staff at every level should be trained on how to recognise threats, how to report any risks they are alerted to and how to be generally security aware. Where threats have occurred, these should be communicated to staff with an update on how to avoid these and what they should be looking out for to avoid it occurring again.

Putting a data protection policy in place

Robust data protection policies will ensure employers can address any risks, breaches or threats in a consistent and effective manner. This policy should document the controls that are in place in the business, any processes in place regarding the monitoring and compliance of systems, and how breaches will be managed. Alongside this, the policy should state how staff should be using data securely to ensure compliance and highlight any responsibilities staff have regarding the processes in place.

Technology is an area that continually updates and as this occurs threats to data often become more sophisticated and dangerous. As the business introduces new initiatives, the policy should be updated in line with this to ensure all staff have full knowledge of the data protection in place.

The content of this briefing is correct at the time of publishing.