A nursing home has been fined £15,000 after a laptop containing personal data was stolen from an employee's home

A nursing home in Northern Ireland was fined £15,000 by the Information Commissioner's Office ('**ICO**') when an unencrypted work laptop was stolen from a member of staff's house during a burglary. The laptop contained personal data relating to 46 members of staff including reasons for sickness absence and information about disciplinary matters. It also contained details relating to 29 residents including their dates of birth, mental and physical health and 'do not resuscitate' status.

The ICO drew attention to the fact that although the laptop was password protected (which was a mitigating factor) it was unencrypted. In addition, the employer had no policies in place governing the use of encryption, homeworking or the storage of mobile devices and neither did it provide any (or adequate) security training for its staff.

The Data Protection Act requires data controllers to have appropriate security in place to prevent personal data from being accidentally or deliberately compromised. Employers should:

- design and organise the security to fit the nature of the personal data they hold and the harm that may result from a security breach;
- be clear about who in the organisation is responsible for ensuring information security;
- make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

The ICO has the power to serve a monetary penalty notice if there is a breach of the Data Protection Act, which can be up to £500,000.

For many employers it will be a normal working practice for staff to take laptops or other devices out of the office to work from home and it is important to ensure that personal data is kept secure at all times. The more confidential and sensitive the information, the

more important it is to safeguard against unauthorised or unlawful access and accidental loss. Some key learning points from this case for employers are that:

- encryption should be used to protect any personal information held electronically that would cause damage or distress if it was lost or stolen;
- staff should only be given access to information that they need to do their job and shouldn't be allowed to share passwords; and
- staff should be given appropriate training on data security and the storage of mobile devices both in and out of the office.