Data Protection

Police Law

Data Protection
Computer Misuse

Overview

Slater and Gordon regularly represent police officers in both criminal and misconduct proceedings as a result of their alleged computer misuse and breaches of Data Protection.

Police officers can access the Police National Computer (PNC) and Force Intelligence Systems for an authorised or "policing" purpose. An authorised purpose essentially means the investigation, detection and prevention of crime. It is an offence under Section 55 of the Data Protection Act 1998, to obtain or disclose personal data without the consent of the Data Controller (Chief Officer). Section 1 of the Computer Misuse Act 1990 creates the offence of unauthorised access to any programme or data held on a computer. Depending on the nature of the allegation, officers can be prosecuted for the serious common law offence of Misconduct in Public Office.

Standards of Professional Behaviour

Regardless of whether criminal proceedings follow, unauthorised access to Force systems would undoubtedly constitute a breach of the Standards of Professional Behaviour in relation to "confidentiality" or "orders and instructions". There appears to be a level of inconsistency in relation to the severity assessment imposed in these sorts of cases but officers should work on the basis that there is every likelihood that computer misuse will be assessed as Gross Misconduct.

In short, offences of this nature can lead to prison sentences in the most serious cases and dismissal without notice. It is vital that police officers fully understand and appreciate what constitutes an authorised or policing purpose.

Despite Forces being heavily reliant on flash screens, "E" learning packages, updates via email and Chiefs orders, the understanding of what constitutes a policing purpose is often misunderstood by many. Checks relating to you personally, family, friends and associates should all be approached with extreme caution. Approval from a Line Manager must be obtained to ensure you are not in breach of the law or Standards of Professional Behaviour.

It is not only an officer's use of computers as part of their duties that now comes under scrutiny. More and more of our clients are being prosecuted and appearing in misconduct hearings as a result of their use of social networking sites.

The Standards of Professional Behaviour are listed in the Police (Conduct) Regulations 2012. A glance at the Regulations should give you a clue as to how something on your Twitter or Facebook account may breach the Standards of Professional Behaviour in relation to "Honesty and Integrity", "Authority, Respect and Courtesy", "Confidentiality" and "Discreditable Conduct" to name but a few.

Choosing your words carefully is important. Could what you are about to post be deemed as offensive, racist or sexually motivated?

Social Networking and Professional Standards

There have been examples across the country of individuals using Twitter to reassure their followers about the progress and status of particular investigations. However well intended, such tweets should be approached with caution and individuals should not leave themselves open to allegations that their conduct has prejudiced an investigation or been defamatory towards a suspect, particularly one who has not yet been charged.

All Forces have policies regarding inappropriate associations and the disclosure of relationships which could jeopardise or embarrass the Force and or individual officers. Monitoring of Facebook accounts may provide a link between you and "a person of interest". However brief or inadvertent the association, this would not prevent an investigation into your conduct.

Social networking can lead to criminal allegations and we have acted for officers charged with offences such as Misconduct in Public Office, breaches of the Data Protection Act and Harassment as a result of their use of social networking sites. Consider whether your actions could be in breach of an existing Court Order. Recent high profile examples in the media have highlighted breaches or Orders relating to the anonymity of victims in sexual offences through the use of Twitter. You could also fall foul of the Malicious Communications Act 1988 by sending any electronic communication which conveys a message which is indecent or grossly offensive, a threat or information which is false and which you know to be false.

Contact us

Please feel free to discuss your own position and concerns.
Contact your nearest office on:

T: 0808 175 7805
E: enquiries@slatergordon.co.uk
W: www.slatergordon.co.uk/policelaw