Information to staff on the Workplace Surveillance Act 2005

What is the Act about?

The Act regulates, but does not outlaw, the use of surveillance by employers in the workplace.

What types of surveillance are covered by the Act?

The Act covers surveillance of an employee at work by an employer using camera, computer or tracking surveillance.

Camera surveillance = This means surveillance by use of a camera that monitors or records visual images of activities.

Notification requirements for camera surveillance are:

• cameras or camera casing used for the surveillance must be clearly visible, and
• signs notifying people that they may be under surveillance must be clearly visible at each entrance, but
• a notice to an employee is not required at a workplace that is not their usual workplace.

Computer surveillance

This is the use of software or other equipment that monitors or records the information on a computer (including emails and the Internet websites).

Notification requirements for computer surveillance are:

• the surveillance must be carried out in accordance with a policy of the employer on computer surveillance of employees at work (Computer Policy), and
• the employee must be notified in advance of the Computer Policy in such a way that it is reasonable to assume that the employee is aware of and understands the Computer Policy.

An employer must not prevent email or Internet website access by an employee unless:
in the case of preventing delivery of an email, the employee is given notice as soon as practicable by the employer that delivery of the email has been prevented, unless the email is spam, has a computer virus, or would be regarded by a reasonable person to be menacing, harassing or offensive. If an email is blocked then a "prevented delivery notice" must be provided to the employee.

The Computer Policy cannot prevent delivery of an email or access to an Internet website merely because an email was sent by or on behalf of a union or because the Internet website or email contains information relating to industrial matters.

Tracking surveillance

This is the use of an electronic device for the primary purpose of monitoring or recording geographical location or movement. Thus tracking surveillance must not be carried out unless there is a notice clearly visible on the vehicle or other thing indicating that the vehicle or thing is the subject of tracking surveillance. This is not applicable to schools.
**Overt and covert surveillance**

The Act describes surveillance as either:

*overt*, where the employees are given written notice of the manner, nature and duration of the surveillance; or covert where surveillance has not been notified and is only able to be carried out in circumstances where the employer has first obtained court approval to do so.

**Overt surveillance**

Surveillance will be lawful overt surveillance where an employer gives its employees at least 14 days' written notice of the surveillance before it begins (or a lesser period if agreed). The "in writing" requirement is satisfied if the notice is given to employees by way of email. New employees must be notified of any surveillance before employment commences. This would be satisfied by including the information that surveillance is being undertaken in the workplace in a new employee's letter of appointment. The notice in both cases must specify:

- the **type of surveillance to be carried out**;
- how the surveillance will be carried out;
- when the surveillance will commence; and
- whether the surveillance will be continuous or intermittent.

Any surveillance that does not meet all the requirements of notified overt surveillance will be deemed to be covert surveillance.

Employers must be able to prove that notice was given and that it was understood by the employee.

Surveillance does not include normal business practices like backing up hard drives, network performance monitoring, software licence monitoring, computer asset tracking, or normal document saving, unless they were used to conduct surveillance or to read an employee's emails.

Employers will also be prohibited from preventing or restricting e-mail delivery or website access. However, if an employer has an Internet and e-mail policy that employees have been notified of and the restrictions are contained in this policy, an exemption can apply.

**Covert surveillance**

To conduct covert surveillance lawfully, an employer must first obtain a 'covert surveillance authority' from a magistrate. To do so, the employer must demonstrate a reasonable suspicion that an employee is involved in an unlawful activity while at work, and explain the steps the employer has already taken to detect the unlawful activity. An employer may apply to a Magistrate for the issue of an authority authorising surveillance generally for the purpose of establishing whether one's employees are involved in any unlawful activity while at work.

All covert surveillance must be conducted for the sole purpose of establishing involvement in unlawful activity and will be overseen by a court-appointed 'surveillance supervisor'. Breaches of workplace policies will not generally amount to unlawful activity, and will not be sufficient to justify a covert surveillance authority.

Covert surveillance is prohibited unless authorised (subject to a defence related to security of premises or personnel) and carried out solely for establishing whether or not an employee is involved in an unlawful activity at work.
Who is covered as an employee?

The Act places obligations on employers extending beyond obligations owed to their employees, and includes obligations in relation to voluntary workers and individuals who work under a labour hire contract and employees of a related corporation of the employer.

Where are employees covered?

The provisions extend beyond the traditional workplace to any place where an employee is working including where working at home on a work computer.

Offences and personal liability

Employers who conduct covert surveillance unlawfully may be subject to fines of up to $5,500 per offence. Directors and others involved in the management of the company may receive convictions for breaches.

If a corporation contravenes any provision of the Act, each director of the corporation or person who is concerned in the management of the corporation is taken to have contravened the same provision but only if the person knowingly authorised or permitted the contravention.

Proceedings for an offence against the Act may be instituted by the secretary of a union whose members are subject to any unlawful surveillance.

The consequences for an employer of a breach of the Act could be far reaching, including for example:

- being unable to rely on damming evidence during unfair dismissal proceedings; or
- being unable to use vital evidence relating to the misuse of the employer's intellectual property or confidential information in an injunction application

What has changed in respect to monitoring of computer systems?

There is no change to the way in which system monitoring is conducted. The current Acceptable Use Policy issued in December 2004 includes information on system monitoring. The updated Acceptable Use Policy provides additional information as required by the Act.

What changes have been made to the Acceptable Use Policy?

Further information has been included in the section on "Monitoring" on page 3 of the Policy to comply with the Act.

What is the CEO doing to comply?

The following steps are being taken by the CEO:

1. The Acceptable Use Policy is being updated to comply with the requirements of the Act in respect to computer surveillance. The policy will be redistributed to schools in hard copy in the near future. In Term 4, sufficient hard copies will be made available to schools to distribute to each staff member.
2. A notice via email will be forwarded all employees from the CEO notifying employees of computer surveillance and referring employees to the updated Policy which can be accessed on line at www.ceowoll.catholic.edu.au.

3. The updated Policy will be posted on the CEO web site.

4. Further advice regarding prevented delivery notices will be distributed in early Term 4

Should you have any queries regarding the above please contact Gary Brown or Stephen Corblishley.
Notice to Employees of the Catholic Education Office, Diocese of Wollongong pursuant to s10 of the Workplace Surveillance Act 2005 (NSW).

This Notice is provided pursuant to the provisions of the Workplace Surveillance Act 2005 (NSW). In accordance with the Policy on the Acceptable Use of the Internet, Intranet, e-mail and other Electronic Communication Devices ("the Policy") employees are advised that their Internet and email use may be monitored by system administrators and others, as nominated by the Principal or CEO or by third parties nominated by the CEO. Computer surveillance is currently operative, it is continuous and ongoing. By logging on to the network, you acknowledge that you have read and understood this Notice and the Policy. The Policy on the Acceptable Use of the Internet, Intranet, e-mail and other Electronic Communication Devices may be accessed at www.ceowoll.catholic.edu.au

Gregory B Whitby
Director of Schools