Care needed when monitoring internet use

Phil Teece
Advisor,
industrial relations &
employment
phil.teece@alia.org.au

Several years have passed since internet and e-mail technology became a standard feature of most Australian workplaces. Yet there is still uncertainty about penalties for its improper use.

Legislation offers little help, with definitions of what is serious misconduct making no reference to these matters. Most employers have filled this legal vacuum with internal policy statements on what is and is not acceptable. But many are turning out to be quite inadequate when legal challenges are mounted to disciplinary action taken under them. In a number of unfair dismissal proceedings, industrial tribunals have found against employers because their policies have failed to set out clearly what is not acceptable and what action will be taken when it occurs.

In a case involving the Bank of Western Australia, an employee was sacked for inappropriate use of the e-mail system by storing what the employer described as pornographic images. There was no dispute about the fact that the employee knew that to do so could result in his dismissal. The Bank's policy statement clearly outlawed storage of pornographic, indecent, obscene, violent or abusive material. But the employee challenged his dismissal in the WA Industrial Relations Commission, arguing that the material he had stored was not pornographic. The commission ruled that the images stored were more accurately described as 'dirty jokes', of the kind that might be found in high school playgrounds or universities. It was held that the employee's breach of the policy was trivial and that he had been unfairly dismissed. The more important aspects of the ruling, however, were that while the managing director had warned staff about pornography, he had not extended this to other inappropriate or offensive material. Nor had the bank at any stage explained clearly just what such material might be.

Another 2003 case in the federal industrial relations tribunal swung on the extent to which sexually explicit images can be described as pornographic. The company concerned had issued a new internet policy which stated that 'obscene or sexually explicit' material must not be accessed, downloaded or distributed. The chief executive had granted a 24-hour amnesty, after which any employee who had done so would be subject to disciplinary action. Later, an employee was found to have stored sexually explicit material on her computer. She was dismissed. While at first glance this may seem like a clear breach, the tribunal ruled against the employer, finding the dismissal harsh, unjust and unreasonable. The critical element in this decision was the fact that the employer's amnesty announcement had not specified what was deemed pornographic. Nor had it referred to sexually explicit or obscene material. The Commission indicated that it did not regard the images stored as pornographic.

Less dramatic but possibly even more controversial is monitoring of employee internet and e-mail use to identify time spent on non-work matters. There is no constitutional or common law right to privacy in Australia but objections to e-mail surveillance are growing. The NSW Law Reform Commission recently recommended extension of the prohibition on covert video surveillance be extended to e-mail and internet use. This recommendation has not yet been adopted, but it is clear that employers may run into trouble if disciplinary action is taken after covert review of employee activity. Many employers have moved to advise staff that their e-mails may be monitored. Unions are now asserting that this does not go far enough; they argue that staff should be advised whenever they are monitored.

Recent case law establishes that, even where a breach of policy is proven and policy makes clear that dismissal may result, the tribunals may decide that loss of employment goes too far. In the cases discussed above, for example, it was decided that other forms of disciplinary action would have been more appropriate in all the circumstances. Clearly, there is no guaranteed right of an employer to sack staff for internet/e-mail breaches of this kind, even where their policy entitles them to take disciplinary action. But a properly defined policy may at least reduce costly mistakes. This should include unambiguous instructions that access, storage or distribution of inappropriate or offensive material will not be tolerated; straightforward description of what 'inappropriate' and 'offensive' means in this context; clarification of what is and what is not acceptable private use of the organisation's equipment; and a precise statement of the consequences which will result from any breaches of policy. When this is done, employers must still ensure that, after identifying breaches, any penalty applied is consistent with the seriousness of the offence.

This is clearly an evolving area of labour law. A final position is still some way off. But whatever form regulation of this increasingly important aspect of workplace rights and responsibilities finally takes, employers can probably be sure of one thing. Covert action, taken without real consultation with or detailed instructions to their staff, is likely to bring costly disputes and publicly embarrassing mistakes. That outcome will be just as damaging as the unacceptable behaviour they quite properly seek to eliminate. ■

...employers may run into trouble if disciplinary action is taken after covert review of employee activity...