There could still be some content in which a blogger or poster has a legitimate expectation of privacy, even though it appears on a site that a potential employer could technically access. Such an expectation is however only likely to exist in respect of information of a particularly private nature which is not openly or widely disseminated. Information regarding sexual orientation or religious belief may appear on a social networking site. It would be illegal discrimination for a potential employer to take account of this information when deciding how to progress a candidate's application.

Can I discipline or dismiss in respect of conduct on the internet?

A common concern for employers is what action they can legitimately take should they suspect that an employee is misbehaving in the virtual world. Where such behaviour takes place in the course of employment and would easily be identifiable as misconduct in the 'real' world, there should be little difficulty in following standard disciplinary or dismissal procedures. For example, work-related internet-based conduct which amounts to bullying, sexual or racial harassment or obscenity would normally be categorised by a well-drafted disciplinary policy as gross misconduct and can be dealt with in the usual way.

However, matters become more complicated where the behaviour takes place outside work in course of the employee's personal life. It is in these situations that the employer would have to link conduct to a breach of the employment contract – usually by dint of the impact on a legitimate interest of the employer's business.

Bringing the employer into disrepute

An excellent example was the case of Ellen Simonetti, the Delta Airlines flight attendant whose blog 'Queen of the Sky' resulted in the termination of her employment. The Queen of the Sky reported various adventures, apparently all part of her experience as a flight attendant, accompanied by photographs of Ms Simonetti in uniform (who later insisted her Queen of the Sky character was merely fictional). Delta Airlines were not impressed: they relied on the misuse of their uniform and logo to establish a case for dismissal on grounds of bringing the company into disrepute.

In the UK such conduct is more likely to be categorised as a breach of trust and confidence but it is easy to see how employees might get themselves into trouble along similar lines: a disillusioned worker posting negative blog comments regarding his employer or colleagues could find himself on the end of

'A disillusioned worker posting negative blog comments could find himself on the end of a disciplinary charge'

a disciplinary charge. It may not avail the employee that the comments were true and therefore not defamatory and the whistleblowing provisions of s.47(B) of the Employment Rights Act 1996 (as inserted by the Public Interest Disclosure Act 1998) will not generally be of assistance to an employee in circumstances where the disclosure could reasonably have been made to the employer rather than the public at large.

Misuse of employer's property

Another avenue for employers is where the alleged conduct takes place using property belonging to the employer which has been misused. It is perhaps trite to advise that in this area prevention is better than cure. A good internet and e-communications policy will have clear guidance on use of social networking, virtual reality and P2P sites (and most likely access to the same will be restricted). Equally there should be parameters for reasonable usage (in terms of time, content and purpose) of BlackBerries, laptops, mobile phones and other equipment issued by an employer to assist an employee in carrying out his duties. It may be necessary to give separate consideration to homeworkers using personal internet connections in the policy.

It is worth an employer's while to use the policy to remind employees of the risks involved in inappropriate internet usage. In *Moonsar v Fiveways Express Transport* [2005] IRLR 9, the employer was held liable for sex discrimination where a female employee was exposed to obviously degrading and offensive pornographic material downloaded by male colleagues on their nearby PCs.

However, a well-drafted policy alone will not render a subsequent dismissal for breach fair and non-discriminatory. It is important to enforce policies and not simply use them as a smokescreen for dismissal on other grounds such as disapproval of a workplace affair, or merely as an excuse to get rid of an awkward employee. Tribunals will be astute to investigate the genuine reasons underlying a decision to dismiss in circumstances where it appears that an individual may have been scapegoated or unfairly selected for unusually harsh treatment.

If an employee is seriously over-using internet and email resources during work time, it may be that he is in breach of his contractual obligation to render the services which he has promised to provide. Such a breach is unlikely to form grounds for instant dismissal.

All but the most extreme case would justify some form of lesser disciplinary sanction and an opportunity to improve behaviour. In any situation where it is within an employer's power to remove the temptation (for example by blocking access to a particular social networking site) a move to dismiss such an employee immediately would probably be considered unfair.

Big Brother – monitoring employee's usage

In practice, difficult questions of enforcement arise, particularly in relation to mobile or senior employees who enjoy greater autonomy and are less likely to be directly supervised. The only real method is to monitor internet usage, which immediately raises questions of privacy and free speech.

Cyber-vetting has been a vexed legal question, previously resulting in successful ECtHR proceedings against the *UK (Copland v UK* (62617/00) ECHR). Email and internet activity falls within the scope of an employee's Article 8 right to a private life, even if sent from or received at work, unless an employee has been given due warning that his activity is liable to monitoring.

Following secondary legislation on the point (Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 SI 2000/2699) it is clear that an employer is legally entitled to monitor email and internet traffic for the purpose of ascertaining whether it forms part of the legitimate business of the employer, so long as all reasonable efforts have been made to inform the employee that such interception may take place.

Once the snapshot of activity has been taken, the evidence will need to be preserved and subjected to expert analysis before it can be used as part of an investigation or disciplinary proceeding.

Managing expectations

While the internet and email are invaluable aids to business and workplace communication, unless expectations are managed on both sides of the employment relationship there is much potential for trouble and dispute. A well thought out, sensibly enforced and monitored usage policy is essential.

Sarah Crowther is a barrister at 3 Hare Court