factsheet

BACKGROUND

The issue of internet use by employees at work has exploded over recent years, driven partly by the popularity of social networking websites such as Facebook and Twitter. In the UK alone, 24 million people are estimated to use Facebook daily, which allows them to message friends, share photographs and interact with other members of the site in numerous different ways.

For people with access to the internet at work, there is now even more opportunity to communicate and organise on personal matters during working hours. In reaction to the growth in popularity of these websites, a number of employers have imposed blankets bans on accessing sites, in the belief that it will reduce "time-wasting" and protect productivity levels.

The current climate echoes previous debates and media coverage on the use of the internet and e-mail for personal use at work. UNISON believes that where personal internet and e-mail use is sensible and proportionate, it can benefit both the employer and the employee. Blanket bans and draconian IT policies serve only to disillusion staff and block what is a perfectly legitimate form of communication.

The way to stop irresponsible use of the internet at work is to have a balanced, well publicised and clearly understood IT usage agreement. This factsheet gives the key information on how to reach such an agreement and what kind of issues it should cover.

LEGAL CONTEXT

Before we come onto the details of what should be in a good internet and e-mail agreement/policy, we need to understand what the legal context is. What are the rights of employees and employers when it comes to the internet at work?

An employer has the legal right to specify which websites can or cannot be visited by staff and to introduce e-mail usage policies that preclude or limit personal use. Where the law becomes more complicated is when employers seek to monitor, intercept or even spy-on the electronic communications of their staff.

There are three pieces of legislation that are relevant to the issue of monitoring e-mails and electronic communication at work. They are the Human Rights Act 1998, Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000.

This legislation overlaps in several areas and has created an unclear legal framework for employees and employers when it comes to knowing their rights and responsibilities. However, knowing the principles of the legislation will help in understanding how an internet and e-mail agreement might be implemented at your workplace.

Essentially the law does give the employer the right to monitor and record employee e-mail and internet communications, but only under certain conditions. They are:

- when workers are told they are being monitored
- when the advantage to the business outweighs the intrusion into the workers' affairs
- when they carry out an impact assessment of the risk they are trying to avert
- when information discovered through monitoring is only used for the purpose for which the monitoring was carried out
- when the information discovered is kept secure
-

- when employers are careful when monitoring personal communications such as emails which are clearly personal
- employers can only undertake covert monitoring in the rarest circumstances where it is used for the prevention or detection of crime
- to ensure compliance with regulatory practices
- to ensure standards of service are maintained
- to prevent or detect crime
- to protect the communications system
- to determine the relevance of the communication to the employer's business (i.e. picking up messages when someone is away from work)

Clearly this does give the employer a wide scope to justify monitoring of employee e-mails. However, these conditions do show that employers need to be extremely careful in applying monitoring, particularly when they attempt to do this in a covert manner.

PERSUADING THE EMPLOYER: AVOIDING PERSONAL E-MAIL AND INTERNET BANS

Good employers are able to move with the times. They can adapt to social and technological changes that affect the lives of their staff.

Though it might be tempting for an employer to introduce a ban on certain websites or even to ban personal e-mail and internet use altogether, this is almost always counter productive. A balanced and well publicised internet and e-mail use agreement is the best way to promote responsible use of work facilities. But how do you persuade an employer that balanced agreements rather than draconian bans are the sensible route to take? The following points may prove helpful:

1. **Work-life balance.** Personal e-mail and social networking sites are simply a new form of communication at work. Whereas people once made personal phone calls or chatted in the break room, workers are now increasingly using online communication. This communication helps people balance busy working and personal lives without necessarily affecting their performance at work.

2. **Recruitment and retention.** Draconian internet and e-mail policies can damage recruitment and retention. Workers do not want to work for an organisation that stops them from engaging in legitimate communication that does not affect their work. As James Lynas, a HR professional for a city law firm states: "… a total ban on using Facebook will make your organisation look like it's run by clueless monsters which is perhaps not the best staff retention strategy."

3. **Restricting personal use is rare.** Most companies simply do not ban personal use. In a survey of 51 employers carried out by Xpert HR in 2005, only 13% had implemented an outright ban on personal e-mail and internet use. In contrast, 49% had a formal policy which did not restrict the use of work facilities for personal e-mail and internet use.

4. **Work networking.** Social networking sites such as Facebook can also be "work networking" sites. Facebook is full of "groups" that have been set up to co-ordinate work related issues. There are numerous groups dedicated to workers with particular areas of expertise in local government, healthcare and education. These groups help workers share ideas and best practice. It would be counter-productive for an employer to restrict access to this kind of information.

5. **Reducing disciplinary and dismissal proceedings**. If an employer has a balanced and well communicated internet and e-mail agreement with the trade union the policy is more likely to be adhered to by the workforce. When managers and union officials are active in communicating the agreement workers will be more aware of acceptable levels of personal use. This in turn will reduce the number of disciplinary and dismissal proceedings which need to be carried out – in the same way good sickness absence agreements reduce the need for disciplinary hearings on the grounds of excessive absence.

6. **Security issues**: Some companies have raised concerns about the security risks posed by social networking. For example, if staff identify themselves as working for a particular employer, it may help fraudsters to gather information to use against a company. Whilst this could be true, it is part of a wider issue and unfair to just single out sites like Facebook as the culprits. As recent guidance from the TUC states: "If employers help staff with training on IT security and identity theft, those staff will also have a better idea of how to minimise security risks to themselves and their company on social networking."

7. **Don't panic!** Facebook is a new phenomenon that is currently very popular, but this may not always be the case. Past experience shows us that particular sites enjoy an initial flurry of activity which then settles down with time. News stories about wide-spread "time wasting" are wide of the mark for two reasons. Firstly people aren't necessarily wasting time (see above) and secondly people are no more likely to be "addicted" to using social networking sites than e-mail or other websites. Facebook isn't a reason to crackdown on internet use, but it should give an employer impetus to have an effective internet and e-mail agreement with their trade union, particularly if they don't have an agreement already.

PERSUADING THE EMPLOYER: AVOIDING EXCESSIVE MONITORING

Monitoring of internet and e-mail use at work is a sensible and necessary policy for any employer. For reasons of system security and legality employers have a responsibility to ensure that their online services are not being misused. However, there is a balance to be struck between monitoring for these reasons and simply snooping on employee's private communications.

As stated above, a balanced and well publicised internet and e-mail use agreement is the best way to promote responsible use of work facilities – not excessive or personalised monitoring of communications. So how do you persuade an employer to avoid this kind of snooping? The following points may be of use:

1. **Privacy.** As shown in the "legal context" section above, there are very tight restrictions on how and when an employer can legitimately monitor employee's communications. Excessive monitoring, particularly when it is covert and directed at an individual, could lead to an employer breaching privacy law.

2. **Recruitment and retention.** Workers don't want to work at an organisation where they feel their every e-mail or Facebook visit is being watched. There is a general acceptance that personal online communication is a part of everyday life – not something to be spied on.

3. **Bullying and victimisation.** Employers will be on very shaky ground if they focus monitoring on particular individuals without showing that they have good reason. Employers who begin to apply heavy handed individual monitoring for no good reason could leave themselves open to claims of bullying or victimisation.

AN EFFECTIVE INTERNET AND E-MAIL USEAGE AGREEMENT

So what should be in a balanced and effective internet and e-mail usage agreement? An agreement could cover a multitude of issues, but there are certain red lines that negotiators should make their objectives. A good agreement should:

Privacy and Monitoring

1. Include a commitment by the employer not to intercept or otherwise monitor emails and internet use, other than when it is suspected that abuse of the system is taking place; as defined in accordance with other elements of an agreed policy.

2. Make clear what monitoring activity is taking place as a matter of routine, including it's extent and the manner in which it will be carried out.

3. Include a commitment from the employer that when abuse of the system is suspected then explanations from the individuals involved will always be sought as a first-step.

4. Include a commitment from the employer to monitor e-mail traffic only by random checks on the volume of email traffic emanating from specific system users. There would be no need to read the contents of e-mails in order to do this.

5. Guarantee privacy of emails sent to and from designated trade union addresses

Restrictions on internet and e-mail use

6. Many employers' IT firewalls and filters have very basic screening which blocks e-mails containing the words lesbian, gay or bisexual, automatically quarantining them as offensive, adult or unprofessional. This is not acceptable. There have even been cases of union activists hauled in under disciplinary procedures for receiving UNISON emails about LGBT workers equality. It can be hard for an individual to raise this so branches should make sure their employers do not block such e-mails.

7. Make it clear what type of private e-mail and internet use is allowed – for example limits on the size or type of email attachments.

8. Specify any restrictions on websites that can be viewed. A simple ban on "offensive material" is unlikely to be clear enough for workers to know exactly what is and is not allowed. Employers should give examples of the kind of material that should not be viewed, for example racist, homophobic or sexist material.

9. Make it clear what kind of e-mails should not be sent; for example sending sexually explicit material and offensive e-mails based on race, sex, sexuality, disability, age, or religion.

10. Make it clear that personal use of e-mail and the internet *is* permitted, provided that it is used responsibly and does not affect staff's work.

11. Avoid banning social networking sites such as Facebook. They are a legitimate form of communication which if used at work in the context of a balanced and well-communicated internet policy will cause no more problems than any other website.

ORGANISNG

Getting a new agreement is always an opportunity to organise and recruit. One good way of doing this is by circulating a questionnaire or survey to employees asking what they would like to see in their organisations internet and e-mail agreement. If you work somewhere where most people have e-mail facilities, you could circulate the survey electronically. This process of consultation can get people involved in the work of the union who might otherwise think that UNISON isn't relevant to them. This opens up the opportunity to recruit new members and show existing members that their branch cares about their views.

WORKING TOGETHER

By sharing information your branch can help the union to spread best practice, identify obstructive employers and monitor the implementation of employment rights.

The way to do this is to send your internet or e-mail agreement to UNISON Bargaining Support via email to bsg@unison.co.uk or by post to Bargaining Support Group UNISON Centre, 130 Euston Road, London NW1 2AY.

FURTHER SOURCES OF INFORMATION

1. ACAS Leaflet, Internet and e-mail policies
   http://www.acas.org.uk/index.aspx?articleid=808

2. Homepage of the Information Commissioner, the public body set up to promote access to official information and protect personal information:
   http://www.ico.gov.uk/about_us.aspx

3. Chartered Institute of Personnel and Development information on internet and e-mail policies http://www.cipd.co.uk/subjects/hrpract/general/webepolicy.htm