Labour Relations
AGENCY

Advice
on
Social Media and the
Employment Relationship

February 2016

Social Media and the Employment Relationship

Introduction

It's hard to think of a bigger change in the workplace over the last 10 years than the arrival of social media as a means of communication. Their rapid rise in prevalence and importance is changing the nature of work and how it balances with our private lives.

The use of social media at work presents new opportunities to employers, but also new responsibilities. One is how to manage the amount of time spent using the sites.

A report published in August 2010 by My Job Group ('Social media in the workplace') and based on a survey of 1,000 respondents, sought to paint a picture of the use of social networking sites in the UK and how it is affecting workplace productivity. In terms of time spent on social media sites, 55 per cent of respondents admitted accessing these sites while at work. A total of 16 per cent of respondents spent over 30 minutes and 6 per cent spent an hour or more per day.
http://www.acas.org.uk/media/pdf/d/6/1111_Workplaces_and_Social_Networking.pdf

The reaction of some employers might be to ban social network media from the workplace altogether. However many organisations are diverting big resources into social media, aware of the enormous potential for promotion and publicity. Many employees give direct benefits to businesses through enhanced communication, publicity and networking facilitated by social media. Platforms such as Twitter and Facebook have widely been found to be effective ways of building up strengthening relationships with clients or customers.

A common-sense approach whereby an organisation develops a coherent social media usage policy with employees may be the best line to take. As the speed of technological change is so great, employers need to regularly revisit policies to reflect the way people interact and work using social media.

Popular social networking sites

Current examples of social media tools include, but are not limited to, social networking sites such as:

Facebook – a social networking service where users have personal profiles, add other users as friends and exchange messages, including automatic notifications when they update their own profile. Additionally, users may join common-interest user groups, organised by common characteristics (e.g. their workplace). Users can choose their own privacy settings, such as allowing open access to their profile or limiting it to friends only. As of January 2013 Facebook active users have passed the one billion milestone.

Twitter – a microblogging service enabling its users to send and read publicly visible messages called tweets. Tweets are text-based posts of up to 140 characters displayed on the user's profile page. Users may subscribe to other users' tweets. Unregistered users can also read tweets. As of January 2013 there are 200 million active users.

LinkedIn – a business-related social networking site mainly used for professional networking. Users maintain a list of contact details of people with whom they have some level of relationship, called connections. This list of connections can then be used to build up a contact network, follow different companies and find jobs, people and business opportunities. As of January 2013 there are 200 million members.

YouTube – a video-sharing website on which users can upload, share, and view videos. A wide variety of user-generated video content is displayed, including film and TV clips as well as amateur content such as video blogging. Most videos enable users to leave and exchange comments. It is estimated that as of January 2013 there are four billion hours of video watched each month.

Blogs - A **blog** is a discussion or informational site published on the Web and consists of discrete entries ("posts") typically displayed in reverse chronological order (the most recent post appears first). As of January 2013 over 181 million blogs where indentified.

Legislation relevant to social media

The following legislative provisions should be considered by employers in relation to social media at work.

Computer Misuse Act 1990	This Act makes provision for securing computer material against unauthorised access or modification and for connected purposes.
The Human Rights Act 1998	This came into force in October 2000. It incorporates the European Convention for the Protection of Human Rights and allows individuals and organisations to go to court or to a tribunal to seek a remedy if they believe that the rights conferred on them by the European Convention have been violated by a public authority. The most relevant articles in relation to Social Media and the employment relationship are: • Article 8 – Right to respect for private and family life, home and correspondence • Article 9 – Right to freedom of thought, conscience and religion • Article 10 – Freedom of expression
The Data Protection Act 1998	This requires anyone (for example, an employer) who handles personal information to comply with a number of important principles. It also gives individuals rights over their personal information. Employers should comply with the **Data Protection Act 1998** when monitoring electronic communications.

Malicious Communications (NI) Order 1988	This Order makes provision for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety. A person guilty of an offence under section 127 of the Communications Act 2003 shall be liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine or to both.
Protection from Harassment (Northern Ireland) Order 1997	This Order was essentially enacted as Northern Ireland's anti-stalking law. However, as with other Orders such as the Malicious Communications (Northern Ireland) Order 1988, this Order could be applied in the employment context if the essential components of the offence are present. The Order deals with - pursuing a course of conduct which amounts to harassment, which the alleged perpetrator knows or ought to know amounts to harassment. The Order makes provision for the reasonable person's interpretation of harassment and details the relevant exemptions, the criminal offence, the civil remedy, what constitutes putting people in fear of violence (course of conduct on at least two occasions). The Order also covers aspects of: restraining orders, limitations and national security.
The Regulation of Investigatory Powers Act 2000 (RIPA)	Under RIPA it is against the law for a business to intercept an electronic communication on its, or anyone else's,

	system. There are some exceptions. Most of the exceptions contained in RIPA itself are unlikely to apply to the monitoring of communications by employers, for example where an interception is authorised under a warrant. These exceptions will be particularly relevant to employers.
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000	These Regulations authorise certain interceptions of telecommunication communications which would otherwise be prohibited by section 1 of the Regulation of Investigatory Powers Act 2000. Interceptions are authorised for monitoring or recording communications.
Electronic Communications Act 2000	This Act makes provision to facilitate the use of electronic communications and electronic data storage; to make provision for the modification of licences granted under section 7 of the Telecommunications Act 1984; and for connected purposes.
Communications Act 2003	This Act confers functions on the Office of Communications; including making provision about the regulation of the provision of electronic communications networks and services. This Act makes it a criminal offence to send or cause to send "...by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character." It also makes it a criminal offence if, for the purpose

	of causing annoyance, inconvenience or needless anxiety to another, a person sends or causes to send by means of a public electronic communications network, a message that they know to be false, or persistently makes use of a public electronic communications network.
Employment Rights (NI) Order 1996 (Unfair Dismissal)	If an employee feels that their employer ended their employment unfairly, either because of the reason why they were dismissed, or the process they used, then the employee may have been unfairly dismissed and might be able to complain to an Industrial Tribunal. There are several ways the employee's dismissal could be unfair: • the employer does not have a fair reason for dismissing the employee • the employer did not follow the correct process when dismissing the employee (for example, if they did not followed their company dismissal processes or the statutory minimum dismissal procedure (if it applies) • the employee was dismissed for an automatically unfair reason (for example, because they wanted to take maternity leave)

Uses of social media within an employer's business

Communicating with employees - While we would not recommend that this is the only means by which you communicate with staff, it could serve as another potential medium for keeping staff informed about important events, etc.

Promoting your business - Advertising products/services and special promotions, e.g. beauty salon sending alerts for special offers. This could be done via email, Facebook, Twitter, etc.

News alerts - Keeping customers/followers updated about important news items, e.g. Invest NI – Twitter would commonly be used for this.

The Met Office has used a range of integrated social media channels and IT to create a social community to help keep people safe and well, informed and educated about the weather across the UK when it matters. It uses Twitter, Facebook, YouTube and its blog to help keep people up to date about the latest weather. The team of weather experts build engagement with followers, making sure that they know everything from whether or not they should hang their washing out, to whether or not they can go out walking on the moors or if severe weather is expected. They won an award for their work – best use of social media in the public sector http://www.metoffice.gov.uk/news/releases/archive/2011/social-media-award

Seek/use feedback – e.g. Trip Advisor reviews, Amazon, EBay. Users upload their feedback onto these sites and companies and other users can benefit from these blog type entries.

Discussion forums - Allows individual and organisations to benefit from knowledge/expertise and to debate common problems, e.g. CIPD website – small organisations without HR expertise can tap into experience and knowledge of others.

Blogs - Blogs can be used as an ongoing information reporting service to keep customers and others informed about developments.

Impact of social media on the employment relationship

Recruitment

Many employers use social media to advertise and recruit new employees: for example, posting job vacancies on websites or using smart phones to attract interest from specific target audiences. There are clearly huge savings for employers using free, electronic channels for recruitment. They can also reach more potential recruits quickly - social networking sites have huge audiences.

Employees are often unaware that their social networking pages are being used by employers as part of a screening process before offering employment interviews. They may be looking for evidence of what they consider 'inappropriate' behaviour or language. Laws protecting people from discrimination on the grounds of age, sex, disability, race, marriage/civil partnership, religion and belief, and sexual orientation start at the recruitment stage. Employers could face claims to an industrial tribunal if they refused to interview someone as a result of a judgement they made based on a social networking profile and, as such, we would not recommend the screening of social networking pages for recruitment purposes.

Recruiting or assessing potential recruits using social media exclusively can exclude people who do not have access to these facilities. In 2015, 22% of the population were not using the internet and around 7% of businesses with ten or more employees still had no internet access.

http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2015/stb-ia-2015.html

Employers should consider all the recruitment methods available to them.

These might include:

- internal recruitment (where justified): in the current economic climate many organisations are focusing on making the most of existing in-house skills;
- using Jobcentre on line NI, a professional recruitment service for employers, to advertise your vacancies and employees to browse for jobs;

- keeping in touch with local schools, colleges and the Careers service will help to promote your skills needs. It can also be useful to offer work experience or shadowing to students; and
- local newspapers and radio and specialist professionals journals can be useful but you should also consider broadening your search to include those communities less likely to use mainstream channels, such as ethnic minority groups.

Discipline and grievances

Employees can use social networking sites, emails or other forms of social media to air their grievances. For example, an employee may complain about how they are being treated by their line manager at work.

Employers have difficulty in knowing how to apply company disciplinary rules to social media activity. For example, what online behaviour constitutes 'gross misconduct'? Many employers have clear rules on defamation and breaches of confidentiality, but are often less sure about whether they should be making judgments about an employee's behaviour online.

Social networking can be an **excuse for avoiding face-to-face conversations.** Many of the issues that lead to disciplinary and grievance problems at work can often be dealt with by having a quiet word with an employee - which can prove hard if line managers have become over-reliant on communicating electronically.

Employers should:

- **set clear guidelines** on when employees are seen to be representing the company and what personal views they can express - for example, some employees are forbidden from expressing any political views. Also be clear about what is meant by defamation and how you expect employees to help protect the company or organisational brand;
- **include social networking in your discipline and grievance policy**, giving clear examples of what will be regarded as gross misconduct - for example, posting derogatory or offensive comments on the Internet about the company or a work colleague.
- **update bullying policies to include guidance on the use of social media** - for example, fellow employees at work being deliberately

ostracised because they did not accept an invitation to become someone's friend on a social networking site.
- **not forget direct forms of communication -** many of the causes of conflict at work can be resolved by face-to-face interaction.

Managing performance

Employers may be concerned that employees are spending too long using company computers for personal reasons: sending personal emails, updating social network accounts and shopping online. In some organisations productivity could be badly affected by employees spending too much time away from core work duties.

The use of social media often blurs the distinction between work and home life, with many employees accessible at home and while travelling. This has led some employers putting more emphasis on managing the tasks an employee performs rather than managing the time they work.

Use of social media is allowing many employees to work remotely. This offers unique challenges for performance management. Employees using tweets, smart phones, emails, internal message boards and professional networking sites to keep in touch can lead to improved communication between a line manager and their staff. However face to face communication is often required when sorting out work issues.

However there are health and safety considerations to be aware of. For example many employees are using personal social networking as a way of switching off from work rather than having regulated breaks away from IT equipment.

The use of social media can become **addictive** to varying degrees - from constantly checking work emails through to deeper personal problems, such as on-line gambling. Where there is a serious problem, employees may need to be encouraged to seek specialist help.

Electronic communication can reduce face to face communication and line managers may not be able to get to the root of problems relating to sickness absence, for example, if communication is via email.

Inappropriate conduct:

This could include

- **Negative comments about employees, employer or customers.**

In the case of **Preece v JD Wetherspoons plc** (ET/2104806/10) an Employment Tribunal found the dismissal of Miss Preece to be fair for posting negative comments about customers on her Facebook page. She was aware of the company's policies regarding "blogging", which expressly referred to sites such as MySpace and Facebook. The policies stated that employees should not write or contribute to a blog, including Facebook, where the content lowers the reputation of the company or its customers, and the company reserved the right to take disciplinary action where this occurred. Miss Preece was also aware that, if an emergency situation arose when she was acting manager, she could ring a hotline number and access the support of a pub manager at any time.

Following an unpleasant incident with 2 customers (who were asked to leave the pub) Miss Preece received a number of abusive phone calls. Following this she posted comments on her Facebook page regarding the incident. These comments were viewed by the customer's daughter who made a complaint to the company. The company began an investigation, during which Miss Preece admitted that her actions were in breach of company policy. However, she argued that her privacy settings meant that her Facebook messages would have been seen only by between a maximum of 40 to 50 close friends, rather than all her friends, which numbered 646 in total.

Following a disciplinary hearing Miss Preece was dismissed. She made a claim for unfair dismissal to the Employment Tribunal. The tribunal found that the company genuinely believed that Miss Preece had committed an act of gross misconduct, and that it had reasonable grounds on which to do so. It also found that the company had carried out as much investigation into the matter as was reasonable in all the circumstances.

However in the case of **Whitham v Club 24 t/a Ventura ET/18/0462/10** an employment tribunal found the dismissal of an employee for posting comments on a Facebook site arising out of work frustrations to be unfair. Mrs Whitham worked as a team leader for an outsourcing company working on an account for Skoda/Volkswagen. She posted comments on her Facebook site including 'I think I work in a nursery and I do not mean working with plants'. When the Company was made aware of the comments they suspended Mrs Whitham and launched an investigation and subsequent disciplinary procedure. Following this Mrs Whitham was dismissed for gross misconduct on the grounds that her comments could have damaged the relationship between the Company and its customer and also because of a breach of confidence. Mrs Whitham claimed Unfair Dismissal and the Employment Tribunal found her dismissal to be unfair on the basis that dismissal for what were 'relatively minor' comments was an overreaction and not within the band of reasonable responses open to the employer. The employer also did not have a social media policy.

- **Bringing the organisation into disrepute**

  Whilst an employer should treat any sort of inappropriate conduct the same regardless of where it occurs, the bigger issue with the use of social media sites is that a much wider audience will be privy to any inappropriate conduct as for example a video uploaded to Youtube could have thousands of viewings within a short period of time. An employer's response to such inappropriate conduct will be dependent on the extent the conduct can be linked to the employers business and also to what extent it could or potentially could damage an employer's/reputation or business.

In **Taylor v Summerfield (Aberdeen Employment Tribunal)** (ET S/ 107487/07) 2007, Taylor was dismissed after posting a video on YouTube of himself hitting a colleague with a plastic bag stuffed with other plastic bags whilst at the warehouse of his employer and whilst wearing his work uniform. The tribunal held that the dismissal was unfair because the company could not show that it had suffered any damage to its reputation and the video had only been viewed eight times.

- **Behaviour incompatible with role**

In the case of **Pay v Lancashire Probation Service 2004 (**UKEAT 1224_02_2910**),** Mr Pay was a probation officer who specialised in the treatment of sex offenders. He was well regarded both by his employers and by the courts for the work which he did with sex offenders.

In his spare time, Mr Pay ran a company selling bondage, domination and sado-masochism merchandise through a website. He also had involvement with a club called 'Club Lash'. The probation service took the view that this was an unsuitable activity for a Probation Officer and dismissed him. On his complaint of unfair dismissal the Manchester employment tribunal held that the dismissal fell within the range of responses of a reasonable employer and that proper procedures had been followed in effecting the dismissal. Accordingly the tribunal dismissed Mr Pay's case. He appealed to the EAT.

Mr Pay lost. The EAT accepted the employer's argument in reply to the effect that "..... it was simply unacceptable for a probation officer engaged in the supervision of sex offenders, with a duty to the victims of such offences, to be engaged in BDSM pursuits in a public way". The EAT held that Article 8 of the Human Rights Act (right to respect for private and family life) - was not engaged because Mr Pay had brought his activities into the public domain through his website. However, Article 10 was engaged but the probation service's right to uphold its reputation, when balanced against Mr Pay's right to freedom of expression, meant that dismissal was justified in the circumstances of this case.

Pay also pursued the matter with the European Court of Human Rights who found that his dismissal did not breach his right to respect for his private life under Article 8 of the Human Rights Act.

In Gosden v Lifeline Projects Ltd 2010 (ET/2802731/2009**),** Gosden was employed by Lifeline, an organisation which provides support for vulnerable people including women, people from black and minority ethnic communities, refugee and asylum seekers, sex workers and the homeless. Godsen sent an email to a friend outside working hours which had sexist and racist content. The friend worked for HM Prison Service, a client of Lifeline and the email made its way into HM Prison Service email system. The Prison Service complained and Godsen was subsequently dismissed for misconduct on the grounds that the fact of sending on the email created an impression that Godsen held the views expressed in the email (sexist and racist) and that such views were incompatible with the work he was required to do. The tribunal upheld the decision to dismiss. Although this case concerned email and not a social media site – the same principles can apply to such comments or postings on social media sites.

- **Bullying and Harassment**

Employers need to be aware of the potential for social media to be used for cyber bullying and harassment purposes. Bullying and harassment can be defined as - *Unwanted conduct which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment. The above shall be regarded as having that effect if having regard to all the circumstances, including in particular the complainant's perception, it should reasonably be considered as having that effect.*

Online bullying and harassment could include:

- Social exclusion – limiting interaction to cliques/groups
- Posting offensive or threatening comments
- Posting photographs or videos
- Online bullying may breach an employer's bullying/harassment policy and so should be treated in the same way as if it had occurred in the workplace. If the harassment is related to a particular characteristic of the individual, e.g. race, sex, etc it is prohibited under anti-discrimination legislation.

The following cases illustrate examples of cyber bullying/harassment:

In Teggart v TeleTech UK Ltd 2011 (IT 704/11), Mr Teggart worked for TeleTech UK Ltd, which provides call-centre services for a number of clients. Mr Teggart's "friends" on Facebook included some work colleagues. While on his computer at home, Mr Teggart posted offensive messages on his Facebook page about A, a female employee at TeleTech.

A, who was known to Mr Teggart but was not a friend, was told about the comments by a work colleague. She asked that the comments be removed. Mr Teggart refused.

At an investigatory meeting, Mr Teggart, who accepted he was the author of the comments on Facebook, was suspended. Mr Teggart was invited to a disciplinary hearing to take place a few days later, with the invitation letter accusing him of gross misconduct.

The company dismissed Mr Teggart for gross misconduct on the basis that "he [had] made multiple postings on a social media site regarding a fellow employee, one of which made reference to TeleTech". The company stressed that it considered that Mr Teggart had harassed A and, in mentioning TeleTech, had brought the company into disrepute.

The tribunal dismissed Mr Teggart's claim for unfair dismissal.

Otomewo v Carphone Warehouse Ltd 2011 (ET 2330554/11)- Two members of O's staff used his iPhone without his permission and changed his Facebook status update to read, 'Finally came out of the closet. I am gay and proud.' O is not gay and did not believe that his colleagues thought that he was. O made a claim for sexual orientation harassment which was upheld by the ET. The employer was held to be vicariously liable for the actions of the employees.

- **Breach of confidentiality**

The duty to preserve confidentiality is part of the duty of fidelity which all employees owe to their employer. Employers may also have express terms, e.g. confidentiality clauses which set out clear rules about the use of company/employee information.

Unauthorised disclosure of company information via social media sites could include details relating to:

- Profit/loss accounts
- Potential redundancies
- Employee personal information
- Client details
- Details of grievances/internal complaints
- Trade secrets

In Pennwell Publishing (UK) Ltd v Ornstien & ors QBD 2007 EWHC 1570 (QB),Mr Isles, publisher and editorial director, and two others worked for Pennwell Publishing (UK) Ltd (Pennwell) for a number of years and apart from Mr Isles all were the subject of restrictive covenants against competition contained in their contracts of employment.

At some point during 2005 Mr Isles and the other two decided that they would set up their own company and in 2006 resigned with that in view. It emerged that they had, during their employment, removed substantial quantities of confidential information including a list of business contacts.

Penwell brought an action against them for breach of contract and to prevent them using the information removed from Penwell.

The High Court found that a list of contacts created by an employee which were stored on an employer's email system (Outlook) belonged to the employer and could not therefore be used by an employee. However, the Court also stated that in the absence of any clearly laid down guidance it was reasonable to imply a term into the contract of employment that an employee will be entitled (at the end of their employment) to take copies of their own personal and confidential information that they had held on the employer's computer system. They referred to such information as doctor, banker, legal advisor details.

Managing the use of social media in the workplace

Develop and introduce a social media policy

ACAS has produced information about social media and social media policies - see at http://www.acas.org.uk/index.aspx?articleid=3375

ACAS states that having a written policy on 'the acceptable use of social networking' at work an organisation can:

- help protect itself against liability for the actions of its workers.
- give clear guidelines for employees on what they can and cannot say about the company
- help line managers to manage performance effectively.
- help employees draw a line between their private and professional lives.
- comply with the law on discrimination, data protection and protecting the health of employees.
- set standards for good housekeeping - for example, for the use and storage of emails.
- be clear about sensitive issues like monitoring and explain how disciplinary rules and sanctions will be applied.

Content of a Social Media Policy

- **Definition and purpose of policy** – e.g. outline what policy is for and what it applies to, e.g. appropriate use of Company equipment, risk management, minimising reputational damage, loss of productivity, etc).
- **Who it applies to** – outline who policy applies to, e.g. all staff, contractors, third parties, etc.
- **Responsibilities** – outline what responsibilities the organisation (e.g. implementation of policy), managerial (e.g. management of policy)

and individual (appropriate use and adherence to policy) have in relation to the policy.

- **Reference and links to other policies** - you may wish to make reference to how this policy links with other organisational policies and procedures, e.g. Disciplinary procedure for dealing with improper use, internet and email policy for appropriate use of equipment, confidentiality policy relating to disclosure of company information, etc. To help a reasonable response, consider the nature of the comments made and their likely impact on the organisation. Provide examples of what might be classed as misconduct and the sanctions you will impose. Also, be clear about confidentiality and what constitutes intellectual property.

- **Responsible use of social media** – define what is seen as acceptable and 'normal' use and acceptable behaviour.

    - Internet and emails: what limits are there on personal use of internet and email?

    - Smart phones: employers need to update their policies to cover new and evolving ways for accessing social networking tools and to reflect changing employee behaviour and attitudes.

    - Social network sites**:** remind employees of privacy settings. Research has shown that the majority of employees would change what they have written on their social networking sites if they thought their employer could read them. Also cross reference to your bullying and harassment policy.

    - Blogging and tweeting**:** if an employee is representing the company, set appropriate rules for what information they may disclose, the range of opinions they may express and reference relevant legislation on copyright and public interest disclosure.

- **Business objectives**: As well as setting clear rules on behaviour, many employers are integrating the use of social media tools into their business strategy. Social networking can be used internally to promote levels of employee engagement and externally to help promote the organisational brand and reputation.

- **Policy on monitoring use** – give details of organisational policy towards monitoring. Be sure that you ensure any monitoring is carried out in compliance with relevant legislation. See Employment Practices Code on Information Commissioners website for guidance on monitoring and data protection issues –https://ico.org.uk/
- Have alternatives to monitoring been considered and can it be justified in terms of the negative impact it will have on the business? Make sure that thorough consultation takes place with employees and their representatives.

- **How breaches will be dealt with/complaints procedure -** make reference to disciplinary and grievance procedures.

- **Ongoing review and update** – who will be responsible for reviewing and how often it will be done, staff comments etc.

Who should be involved?

- **Consultation**: consultation with staff on the policy will help to ensure the policy is fair. It will also help to make the policy relevant to organisational needs - for example, if employees handle sensitive, confidential information on members of the public the policy will have to reflect this.

- **Communication**: a high proportion of employees may not know if their employer has a policy on internet use. Technology is evolving so quickly that many policies soon get out-of-date, so they need to be reviewed regularly.

- **Induction programmes** are a good way to set clear boundaries about the use of the internet. Each organisation will have its own culture and standards of 'acceptable behaviour' but it is best to be as clear as possible about these from the start.

Review other policies and procedures to include use of social media

Some policies and procedures that an employer may wish to review to include references to use of social media are:

- **Statement of terms and conditions** – many small employers may not have detailed policies and procedures so they may wish to include a clause in the statement to refer to social media use.

- **Discipline and grievance** – this can include reference to how inappropriate use of social media will be dealt with as misconduct and also provide employees with an avenue for raising complaints about inappropriate use e.g. Cyber bullying/harassment

- **Communication** – some organisations may have a general communication policy or a code of conduct. This may set out guidelines on how internal and external communications are carried out. Guidance for using social media for communication purposes should be included and should also set out rules on confidentiality.

- **Internet and email** –The policy should provide guidelines on appropriate use of the internet and email facilities.

- **Mobile phone** – organisations may wish to specify what is deemed to be appropriate use during working hours – whether these are provided by the company or not. A lot of smart phones now have internet capability and there is a danger that unless appropriate usage is specified employees could spend considerable amounts of time accessing social media sites. Organisations may also wish to stipulate that employees are not permitted to take photos/videos in work.

- **Recruitment and Selection** – employers should be careful about being influenced in relation to the recruitment of employees by information on social media sites.

Training, induction and supervision

Induction is a perfect opportunity to make new staff aware of company rules, policies and procedures, including Social Media policy. Ensure existing staff are well briefed on the Social Media policy and also appropriate use of IT equipment, internet use, mobile phones etc.

It is not enough to simply have a Social Media policy – managers must ensure that employees are adhering to it also. This involves the manager being aware of use in the workplace, reminding employees of appropriate use, identifying any potential breaches and dealing with them as early as possible.

Many employers may fail in defending claims of unfair dismissal cases related to inappropriate use of Social Media for failing to either provide clear guidelines on use or not having a consistent policy for managing such issues.

Monitoring

Monitoring must be undertaken appropriately and in accordance with relevant legislation, e.g. Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, etc.

In **Copland v United Kingdom 2007 (European Court of Justice)** ECHR Case No. 62617/00, Copland worked for a further education government maintained college – Carmarthenshire College since 1991. In 1995 she was appointed to the position of Personal Assistant to the college principal. During her employment, and at the deputy principal's request, her telephone, e-mail and internet usage were monitored to establish whether she was making excessive use of the college's facilities for personal purposes. The College had no policy regarding such monitoring.

When she became aware of this Copland lodged a case against the UK Government with the European Court of Human Rights, arguing that the college had violated her right to respect for private life and correspondence by monitoring, collecting and storing personal information relating to her telephone, e-mail and internet usage at work. As this case arose before the implementation of the Human Rights Act 1998 (implemented in October 2000) the employee took a claim against the UK Government (on the basis that the college was an emanation of the State) to the European Court of Justice under Article 8 of the European Convention on Human Rights. The ECJ found that the employer's monitoring without her knowledge did amount to a breach of Article 8 – Right to respect for private life and correspondence. As the employee had not been given any notification that her calls etc. would be monitored, she had a reasonable expectation of privacy.

Core principles of monitoring

The Employment Practices Code produced by the Information Commissioner states that:

- It will usually be intrusive to monitor your workers
- Workers have legitimate expectations that they can keep their personal lives private and they are also entitled to a degree of privacy in the work environment
- If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered
- Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified

The Employment Practices Code can be accessed by clicking on the following link:
https://search.ico.org.uk/ico/search?q=%27employment+practices+code%27

Covert Monitoring

Covert Monitoring should be authorised by Senior Management. They should satisfy themselves that there are grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals about the monitoring would prejudice its prevention or detection.

Senior Management should ensure that Covert Monitoring is strictly targeted at obtaining evidence within a set timeframe and that the covert monitoring does not continue after the investigation is complete.

Covert audio or video monitoring should not be used in areas which workers would genuinely and reasonably expect to be private, e.g. toilets, etc.

If a private investigator is employed to collect information on workers covertly employers should ensure there is a contract in place that requires

the private investigator to only collect information in a way that satisfies the employer's obligations under relevant legislation.

Senior Management should ensure that information obtained through covert monitoring is used only for the prevention or detection of criminal activity or equivalent malpractice. They should disregard and, where feasible, delete other information collected in the course of monitoring unless it reveals information that no employer could reasonably be expected to ignore.

In **McGowan V Scottish Water 2004 Employment Appeal Tribunal (**EAT/0007/04), McGowan was employed by Scottish Water at a water treatment plant near Stranraer and lived in a tied house close to the plant. Scottish Water suspected McGowan of falsifying timesheets in relation to call-outs and periods when it was necessary for him to attend the plant. It considered installing cameras within the plant but decided against this because it was not possible to do so without McGowan realising what was going on. Instead, Scottish Water employed a firm of private investigators to secrete themselves for a week opposite McGowan's home and film his comings and goings. Videos of McGowan were produced and were used as evidence against him during a disciplinary hearing. McGowan was subsequently dismissed and brought proceedings against Scottish Water claiming that he had been unfairly dismissed. McGowan's claim was based on the Human Rights Act 1998, which makes it unlawful for public sector employers to act in a way that is incompatible with the European Convention on Human Rights. McGowan argued that the employer's covert surveillance had breached his right under Article 8(1) of the Convention `to respect for his private and family life, his home and his correspondence', and that his dismissal was unfair as a result.
The tribunal held that McGowan's rights under Article 8(1) had not been interfered with because the surveillance was carried out on a public road and any member of the public could have observed what the investigators observed. The tribunal went on to hold that the employer's actions were in any event justified within the meaning of Article 8(2), which provides that interference by a public authority with the exercise of an Article 8(1) right is justified provided it `is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the

rights and freedoms of others'. Stating that it was necessary to strike a balance between the gravity of the offence and the measures taken to investigate it, the tribunal decided that the employer had acted reasonably. McGowan appealed to the EAT who upheld the tribunal decision.

Network Security

The following are examples of ways in which employers can help control usage of social media sites or the impact of any inappropriate emails.

- Firewalls are used to prevent inappropriate content coming in or out of the organisation.
- Web security tools such as websense which can be used to monitor or restrict usage and to prevent access to specific websites.
- Spam prevention tools can block emails containing certain terms
- Antivirus software to detect, prevent, and take action to disarm or remove malicious software programs, such as viruses and worms. Computer viruses are software programs that are deliberately designed to interfere with computer operation; record, corrupt, or delete data; or spread themselves to other computers and throughout the Internet.

The main advantages of such tools are:

- to restrict/block access to certain sites, e.g. Facebook at work

- to ensure that emails containing inappropriate content do not reach employee's inboxes nor can they be sent onwards from employees email systems

- to use such tools for monitoring internet usage – including which sites are being visited.

Dealing with improper use through disciplinary action

An employer's awareness of improper use could come from a number of sources:

- Grievance/complaint – from another employee
- Customer complaint
- Observation – where the employer/line manager observes inappropriate use for themselves
- Monitoring – as a result of appropriate monitoring behaviour in line with Data Protection Act principles
- Police – inappropriate use that is noticed by the police could be notified to the employer
- Newspaper articles/other media – an employer may only be aware of an issue from reading a newspaper article or other media article

Taking disciplinary action

Employers should treat improper use of social media as they would any other type of alleged misconduct. This would involve an investigation and consideration of suspension or other precautionary action followed by disciplinary action if appropriate.

Investigation

In certain cases, for example in cases involving alleged gross misconduct, consideration should be given to a brief period of suspension with full pay whilst an unhindered investigation is conducted. Such a suspension should be imposed only after careful consideration of the necessity for this. Employers should also consider alternative actions which would be more acceptable to the employee yet serve the same purpose as a suspension. An alternative to suspension might be the agreeing of a temporary transfer to other duties or another work station without loss of pay. Any action taken, including suspension on full pay, should be reviewed frequently to ensure it is not unnecessarily protracted. It should be made clear that any action taken is neither considered as disciplinary action nor an indication of blame or guilt.

The employer should decide who will carry out the investigation – the aim to add as much objectivity to the process as possible, so it is desirable to have a different person conduct the investigation than will carry out any disciplinary action. It could be another manager within the company or an external consultant. This may involve taking witness statements, making a report and referring to other relevant organisational policies and procedures.

The employer should be mindful that the investigation should be conducted promptly to adhere to organisation timescales, but also to gather evidence while the incident is fresh.

Further information on carrying out investigations can be found in the LRA Advisory Guide - Advice on Conducting Employment Investigations

The employer should then determine, on the basis of the investigation, whether it is necessary or appropriate to carry out any formal (or informal) action.

After the investigation

The employer can then decide the necessary action to take i.e.

- No case to answer so no further action required.
- Informal action is used to try and nip problems in the bud.
- Formal action i.e. Warnings are taken when informal action has not brought about the improvement needed or a more serious offence has been committed where informal action is not appropriate.
- For a gross misconduct offence you could go straight to the dismissal stage, or if the procedure permits use action short of dismissal as an alternative penalty. This may include demotion or suspension without pay if allowed for in the contract of employment.

Disciplinary procedure

Formal disciplinary action should be in line with statutory dismissal/disciplinary procedure as set out in the Labour Relations Agency Code of Practice on disciplinary and grievance procedures.

This involves three steps:

Step 1- Statement of grounds for action and invitation to meeting

- The employer must set out in writing the employee's alleged conduct which lead them to contemplate dismissing or taking disciplinary action against the employee.
- The employer must send the statement or a copy of it to the employee and invite the employee to attend a meeting to discuss the matter.

Step 2 - The meeting

- The meeting must take place before action is taken, except in the case where the disciplinary action consists of suspension.
- The meeting must not take place unless: the employer has informed the employee what the basis was for including in the statement under Step 1 the ground or grounds given in it; and the employee has had a reasonable opportunity to consider their response to that information.
- The employee must take all reasonable steps to attend the meeting.
- After the meeting, the employer must inform the employee of his/her decision and notify them of the right to appeal against the decision if they are not satisfied with it.

Step 3 - Appeal

- If the employee wishes to appeal, they must inform the employer.
- If the employee informs the employer of their wish to appeal, the employer must invite them to attend a further meeting.
- The employee must take all reasonable steps to attend the meeting.
- The appeal meeting need not take place before the dismissal or disciplinary action takes effect.
- After the appeal meeting, the employer must inform the employee of the final decision.

An employee has the right to be accompanied at disciplinary and appeal hearings.

Read about disciplinary procedures in the LRA Code of practice on disciplinary and grievance procedures and the LRA Advisory Guide - Advice on handling discipline and grievances at work.

Learning points

Case law in relation to social media highlights some important points for employers.

- **Employers** must have a clear policy setting out what is acceptable usage of social media and provide training about the policy and its importance. This policy must be communicated to all employees. If comments are made on a social media site the employer must consider the impact of these comments. If the comments are not directly about customers, products or the organisation, it might not be reasonable to dismiss.

- **Employees** must be made aware that having privacy settings on Facebook does not mean that they can post whatever they want about the organisation. It must be clearly set out in the organisation's policy that postings could be copied by people entitled to access them, and sent on to others beyond the control of the original poster. Hence merely having privacy settings does not mean that comments will be kept out of the public domain. The TUC has issued guidance about blogging. It says: "As you probably spend more time working than doing anything else, you may want to blog about work, but first stop and think about it. Blogging about existentialism or football may be harmless, but discussing your boss, your colleagues or any aspect of your work could lose you friends, cost you your job and even land you in court facing a defamation suit." And even if you change jobs, given the developing recruiting practices described elsewhere in this booklet the blight of a negative internet footprint has the potential to come back and haunt you for many years, even if you bring a claim in the employment tribunal and win.

Further Advice

The Labour Relations Agency runs a series of good practice seminars covering many aspects of employment relations matters. These events will be held in the Agency's headquarters in Belfast and in the Regional Office in Londonderry **and t**here is no charge for attendance at any of these events.

The seminars relevant to this publication are:

- Handling Discipline and Grievance
- Conducting Employment Investigations
- Social Media and the Employment Relationship

For details of these seminars and online booking click on the following link http://www.lra.org.uk/index/workshops_and_seminars/seminars.htm

Head Office

Labour Relations Agency

2-16 Gordon Street
Belfast, BT1 2LG
Tel: 028 9032 1442
Fax: 038 9033 0827
Email: info@lra.org.uk
Website: www.lra.org.uk

Regional Office

Labour Relations Agency

1-3 Guildhall Street
Londonderry, BT48 6BB
Tel: 028 7126 9639
Fax: 038 7126 7729
Email: info@lra.org.uk
Website: www.lra.org.uk