prospect

Members' guide

email, internet and social media at work

Contents

Electronic communications

The use of email, the internet and social media at work is now mainstream. However, their use has raised new issues for workers and their trade union representatives. Prospect has seen an increase in disciplinary cases connected to the use of email, the internet and social media, so members need to be aware that inappropriate use of these facilities can lead to disciplinary action and even dismissal.

Many of the problems associated with abuse of email and internet facilities concern discrimination. Prospect is committed to equality for all members and cannot condone abusive or harassing conduct in the workplace or any behaviour which creates a hostile working environment for colleagues.

At the same time, concern about the extent of employer surveillance in the workplace is rising. This can take many forms – from monitoring phone calls (which can range from logging phone numbers called to recording calls) and monitoring keystokes, to the use of CCTV (closed circuit television). Prospect is opposed to indiscriminate surveillance because workers are entitled to privacy at in their work space, whether that is at home or on site. However, abuse of facilities gives employers reasons to extend surveillance. Therefore the extent to which employers can monitor email and internet use should be discussed, negotiated and agreed with union officials and representatives.

This guide aims to deal with some of the most common employment-related problems faced by members and representatives in this area, such as disciplinary matters, harassment and discrimination. It does not deal with technical or practical issues.

The law in this area is complex and developing rapidly through case law, statutes and regulations. This guide cannot cover every circumstance, so please contact your Prospect representative if you need further advice.

The law in the Channel Islands and the Isle of Man is quite different, so members should speak to their Prospect representative for more specific advice.

Decisions on whether to represent members, or offer legal advice or assistance, are taken on the merits of each case at the union's discretion.

1. Work-life balance

Full time employees in the UK work some of the longest hours in Europe. The provision of work mobile phones, laptops etc means that it can be difficult to switch off and members can be contacted at any time of the day or night. For more on this, please refer to *Prospect Guide on the right to disconnect* – https://library.prospect.org.uk/download/2020/01157

1.1 Some employers or clients expect an immediate response to emails and phone calls, but it is important to set boundaries because working excessive hours can lead to ill health, including stress. See our Members' guide to work-related stress for more information.

1.2 In some organisations members are responsible for the employer's social media sites. In others, employers encourage workers to use social media accounts to promote the business. This means that the lines between work and home life can be blurred and managers could place unreasonable expectations on workers to post or respond to issues outside the normal working day.

1.3 If you want a good work-life balance, you have to think about the impact of social media and email on your personal time.

1.4 Employers should have technology and social media policies that set out what is expected of staff (see section 9). Reps should negotiate with the employer to ensure these expectations are reasonable.

1.5 For more information see our Members' guide to working time and the law.

2. Equality at work

2.1 Under the Equality Act 2010, all workers have the right to be treated equally by their employer. It is unlawful to discriminate against anyone at work on the grounds of any of nine protected characteristics, which are:

- age
- disability
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation

2.2 In Northern Ireland, discrimination on the grounds of religion or political opinion is unlawful under the Fair Employment and Treatment (Northern Ireland) Order 1998.

Harassment

2.3 Unlawful discrimination at work includes harassment. The Equality Act defines harassment as "unwanted conduct, related to a protected characteristic, which has the purpose or effect of violating a person's dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment for them".

2.4 When employment tribunals look at harassment cases they must consider:

- the complainant's perception
- the circumstances of the case
- whether they believe it is reasonable for the conduct to be held to be harassment.

2.5 Where discrimination occurs in the course of employment, employers will be liable for their employees' acts unless they take all steps that are reasonably practical to prevent the discrimination occurring. Individual employees can also take another employee to an employment tribunal for harassment and discrimination.

2.6 Email and instant messaging at work means that messages can be circulated quickly and easily to a wide group of people. Because it is seen as an informal way of communicating, senders need to be sure that their communications are appropriate and avoid potentially offensive messages. Email is not a secure medium – even deleted emails can be retrieved and messages can easily be accessed by people they were not intended for. The same principles apply to posts on social media sites.

2.7 Accessing sexist or racist information by email or the internet is unacceptable. A group of people viewing or discussing such

information, or displaying material in an open plan area, is likely to create a hostile a working environment. This can constitute unlawful harassment even if it is not directly aimed at an individual.

2.8 This is illustrated by the case of *Moonsar v Fiveways Express Transport Limited*. Ms Moonsar worked with men who downloaded pornography in the office. Although it was not directed at her, the employment appeal tribunal said that downloading pornographic material in the office where Ms Moonsar was working "would be regarded as degrading or offensive to an employee as a woman" and was unlawful harassment.

2.9 If you receive offensive messages by email, text, social media or any other form, or feel that the behaviour of colleagues at work is offensive, you should discuss this with your Prospect representative or full-time officer. You should keep records of what happened. You may need to make it clear to the perpetrators that you find their actions offensive, and you may need to raise the matter with your line manager, personnel section or equal opportunities adviser. Your Prospect representative should be able to offer advice on what to do.

2.10 Most incidents should be resolved without recourse to the law. But members should be aware of the strict time limits for pursuing an employment tribunal case. With discrimination, a case must be started within three months of the incident occurring, so seek advice as soon as possible, (see section 4).

2.11 In all cases of discrimination other than dismissal, the employee should present a grievance in writing to the employer before making the tribunal claim. Failure to raise a grievance could result in compensation being reduced by up to 25 per cent.

2.12 See Prospect's Members' guide to bullying and harassment for more information on what to do if you are harassed at work or accused of harassing someone else.

Protection from Harassment Act

2.13 As well as being outlawed under the Equality Act, harassment is also forbidden by the 1997 Protection from Harassment Act. The Act covers harassment on any grounds and makes it a civil and criminal offence. Individuals who have been harassed can seek court orders to restrain the harasser and claim damages.

2.14 Prospect is cautious about using this legislation in the workplace because the protection afforded is very limited and it should only be considered if there is no other

remedy. It usually applies when it can be shown that the harassment is severe and intentional.

Personal injury

2.15 You may be able to bring a claim for personal injury if you can show that your health suffered because of your employer's actions, or its failure to act, in a harassment situation. You would need to show that your employer's negligence caused the injury to health and that they could reasonably foresee that the injury would occur.

3. Disciplinary offences

3.1 Prospect representatives have had to deal with many cases of disciplinary action against members because of their use of email, internet and social media at work. Offences ranged from excessive personal use of email to downloading pornographic material from the internet.

3.2 Employers ought to make clear what constitutes an acceptable use of facilities and the standards expected of employees. For this reason Prospect representatives should try to ensure that their organisation has an agreed policy on the use of technology and social media (see section 9).

Disciplinary action

3.3 Issues which may give rise to an employer bringing disciplinary action and/or dismissal for internet or technology misuse include:

- unauthorised personal use of facilities
- excessive use of facilities
- using facilities for outside business purposes
- unauthorised access to company information
- loading software without authority
- disclosing confidential information
- using the internet for illegal or inappropriate purposes, eg accessing pornography or discriminatory material
- harassing other staff.

3.4 In all cases employees must be clear about what is acceptable use and what may be a disciplinary matter. Staff should check if their employer has a policy on social media, email and internet use, or if there are rules in a staff handbook, disciplinary code, equal opportunities policy or office or IT manual. Breach of such policies is likely to be misconduct. Even if the employer does not have a written policy, abuse of facilities could result in disciplinary proceedings.

Disciplinary procedures

3.5 Disciplinary procedures should be followed fairly in any form of disciplinary action. These will include rights to:

- a full and open investigation
- know the details of the allegation
- state the case in defence
- be represented by a union representative or colleague
- make personal representations to the person making the decision, and
- appeal to an impartial party.

3.6 The disciplinary process must also ensure that any sanction taken against the employee is consistent and proportionate. Employers should follow the ACAS (Advisory, Conciliation and Arbitration Service) Code of Practice

on disciplinary and grievance procedures (Labour Relations Agency's Code of Practice in Northern Ireland). Failure to follow the Code does not necessarily make a person or organisation liable to proceedings, but employment tribunals will take the Code into account. Tribunals have the power to adjust awards by up to 25% for unreasonable failure to comply with the Code (50% in Northern Ireland).

Representation

3.7 Members should seek advice from their Prospect representative if they are faced with disciplinary action. Employers must, by law, allow a worker to be accompanied at a disciplinary hearing by a union representative or colleague.

3.8 Decisions on whether to represent members, or to offer legal advice or assistance, are taken on the merits of each case, at the union's discretion.

4. Unfair dismissal

4.1 Employees who have been continuously employed for two years or more (one year in Northern Ireland) have the right not to be unfairly dismissed.

4.2 Exceptions to the two-year service requirement include dismissal on any of the following grounds:

- pregnancy
- childbirth
- asserting a statutory right
- trade union activities or membership
- health and safety activities
- making a protected disclosure (whistleblowing)
- being an employee representative or pension trustee
- campaigning for union recognition.

4.3 Under discrimination law, workers have the right not to be dismissed on the grounds of a protected characteristic (see section 2), regardless of the length of service.

Fairness

4.4 In unfair dismissal cases, an employment tribunal has to consider the fairness of each case on its own merits and decide whether dismissal was within the range of reasonable responses for an employer in the circumstances. The fairness of a decision to dismiss will depend on the seriousness of the offence, whether warnings had been given in less serious cases and whether a proper process was followed.

4.5 In cases of email, social media and internet abuse, a dismissal is much more likely to be fair if the employee had been advised about what was and was not acceptable. It is harder to mount a defence against dismissal where an employee had been warned about their use of facilities or had been given clear instructions not to access certain areas of the system.

4.6 This section looks at unfair dismissal generally and the following section will look at more serious cases concerning offensive material.

4.7 It is important to note that the law does not recognise breaches of social media policies as being a different type of disciplinary issue and therefore employment tribunals ask the same questions as for other forms of misconduct. The Employment Appeal Tribunal made this point explicitly and refused to lay down guidelines for social media breaches in *Game Retail v Laws (2014)*.

Examples

4.8 In the following cases, an employment tribunal had to consider whether a dismissal was unfair:

- Personal use. An employee was fairly dismissed when the company discovered that he had been spending between 10-15% of his daily working time on non-work related internet use *(McKinley v Secretary of State for Defence)*.
- Time wasting. Two employees were dismissed after a company investigated the circulation of private joke emails. The company said it had dismissed the employees because of the inappropriate nature of the emails and the amount of time wasted in the process. The employment tribunal found the dismissals were fair *(Pennington and Beverly v Holset Engineering Limited)*.
- Security. The employment appeal tribunal ruled that it was fair to dismiss a worker for accessing part of the computer system which was password protected and which he did not have authority to use *(Denco Ltd v Joinson)*.
- Legitimate access. On the other hand, a tribunal found it unfair to dismiss an employee who had accessed part of the system that he was not authorised to enter when he had a legitimate business reason to do so and he could have received the same information by telephone *(British Telecom v Rodrigues)*.
- Downloading. An employment tribunal found in favour of an employee who had been dismissed for loading inoffensive games software onto his PC. The company alleged that his actions had caused a serious computer virus. But the tribunal said there was no evidence that the virus had been caused by him and did not accept that his actions amounted to a breach of trust *(Gale v Parknotts Ltd)*.
- Harassment. An industrial tribunal in Northern Ireland found that an employee who had made accusations about the promiscuity of a female colleague on his Facebook page was fairly dismissed for harassment. The colleague who was targeted and other work colleagues reported the comments to the employer. In addition to unfair dismissal, the claimant argued that his right to a private life (Article 8 of the European Convention on Human Rights) had been violated. The tribunal said that the act of posting on Facebook removed any protection of privacy granted under Article 8 *(Teggart v Teletech)*.

4.9 Tribunal decisions can vary, but members need to be aware that misuse of technology and the internet can lead to disciplinary action and even dismissal. Members should understand what their employer says about acceptable use and keep within the limits laid down.

Remedy

4.10 Even when tribunals find that a dismissal is unfair, reinstatement is rare and compensation is likely to be significantly reduced to reflect the employee's contributory fault.

Employment tribunal claims

4.11 Claims for unfair dismissal must be started in an employment tribunal within three months of the date the employment was terminated. The first stage in bringing a tribunal claim is to apply to ACAS for 'early conciliation'. The conciliation period stops the clock for presenting the claim to the employment tribunal. These rules are complex so always seek advice from Prospect.

4.12 In Northern Ireland claims are made to an industrial tribunal. Early conciliation through the Labour Relations Agency is now mandatory (as of January 2020).

4.13 Members should seek advice from their Prospect representative as soon as possible. Decisions on whether to offer legal advice or assistance will be taken on the merits of the case, at the union's discretion.

5. Offensive material

5.1 A common disciplinary issue referred to Prospect is accessing offensive or pornographic material. This can be via the internet, Twitter, WhatsApp or any other social media.

5.2 Most companies and organisations will have an equality and diversity policy covering discrimination on the grounds of a protected characteristic *(see section 2)*. Accessing or circulating offensive information (whether obscene or not) contrary to such a policy would be a disciplinary matter, and would breach Prospect's policy on equality and diversity.

Unfair dismissal

5.3 Section 4 explained the general points about unfair dismissal law that apply here. Use of the internet or email to deliberately access, download or forward offensive material, particularly pornographic material, is much more likely to be gross misconduct and to warrant instant dismissal.

5.4 Under the Obscene Publications Act, it is a criminal offence to download or distribute obscene material. There are also criminal offences concerning paedophile material. Deliberately committing any criminal offence at work is likely to lead to instant dismissal.

5.5 Accessing pornographic or offensive material is likely to be regarded as gross misconduct and a fair reason to dismiss.

Examples

5.6 Two examples of dismissals that employment tribunals said were fair:

- An employee who was dismissed for using the internet at work to access sexually explicit pictures was held to have been fairly dismissed. He claimed he got into a site by mistake and then revisited it because he was disturbed that it was so easy to do. The tribunal said he had been fairly dismissed because the employer had investigated events thoroughly and objectively and concluded that the employee was guilty of violating established codes of conduct and of breaching trust and confidence *(Parr v Derwentside District Council)*.
- A tribunal ruled that, in the absence of terms detailing the categories of conduct that constitute gross misconduct, the mere use of the internet for unauthorised purposes would not normally justify summary dismissal. But the employee had downloaded pornography that was so objectionable, it amounted to gross misconduct *(Humphries v VH Barnett & Co)*.

5.7 But in another case a tribunal found a dismissal unfair:

- An employee dismissed for accessing pornography and other non-work related material was found to have been unfairly dismissed. The tribunal said there was no clear breach of company policy and the disciplinary procedure was fundamentally flawed. However the tribunal reduced his compensation by 50% in recognition of his contributory fault in the dismissal *(Dunn v IBM United Kingdom Ltd).*

Degree of offence

5.8 Tribunals have to consider the nature of the material and distinguish between cases where it is distasteful and where it is significantly more offensive. The penalty will be greater in cases where the material would fall under the Obscene Publications Act, but less extreme cases can still result in fair dismissal.

5.9 As with other types of misuse cases, an important (though not conclusive) factor will be whether the employee had been advised that such action was forbidden. The matter will be more serious if the material was forwarded or brought to the attention of others *(see section 2).*

6. Other legal issues

6.1 Many legal issues that are not related to employment can arise as a consequence of using email, the internet and social media at work.

6.2 These are largely outside the scope of this guide but this section briefly outlines some of the most common areas.

Defamation

6.3 Defamation is the publication of an untrue statement tending to lower the subject in the estimation of others. The informality of instant messaging apps, direct messages in social media apps and to a lesser extent email may make employees less cautious about what they say, but comments made by any of these means including blogs or any other method can be as defamatory as any other written communication. An employer could be liable for comments made by employees in an email or on social media.

6.4 Members can seek initial legal advice through the Prospect's legal advice scheme. Please contact your full-time officer or the union's member contact centre to begin with for more information about the service.

Variation of contract

6.5 Employment contracts can be varied by email. For example an email to all staff about new arrangements for working hours could amount to an attempt to impose a variation of contractual terms. Although a contract cannot be lawfully varied without the agreement of both parties, the legal remedies against employers who do impose changes are often inadequate.

6.6 If an employer notifies a change to terms and conditions and employees do not respond, they may be deemed to have accepted the new terms and waived any right to stand on their existing terms or to sue for financial loss. The law in this area is complicated and members should contact their Prospect representative as soon as possible if their employer tries to change their terms and conditions. Please note that any delay in objecting to the new terms could work against the employee, so it is important that advice is sought promptly.

6.7 See Prospect's Members' guide to individual contracts of employment for more information.

Formation of contract

6.8 Members can enter into legally binding contracts through email (or even through social media, for example on LinkedIn) either on their own account or on behalf of their employer.

6.9 Members need to be careful not to enter a contract inadvertently. The fact that emails are not signed documents (in the traditional sense) does not affect the ability to make a contractual arrangement.

Copyright

6.10 Copyright infringement can occur if members copy and paste images, text etc from the internet and distribute it to others. Members should be mindful of this and include any relevant copyright notices where appropriate.

6.11 Laws on copyright apply to information on the internet (including music) just as they do to books and other publications. Copyright law also protects computer software.

Computer Misuse Act 1990

6.12 The Computer Misuse Act 1990 makes it an offence for an unauthorised person to knowingly access a programme or data, or to modify the contents of a computer. This is the legislation that outlaws 'hacking'.

7. Employer monitoring

7.1 The extent to which an employer should be allowed to monitor electronic communications such as emails and phone calls is highly controversial. Prospect maintains that employers should respect the privacy of staff.

7.2 Monitoring should be limited and only carried out after consultation with trade unions and after giving adequate notice to workers.

7.3 It is generally held that employers can monitor emails and phone calls made at work where there is good reason for doing so and where the employees have been notified that this may happen.

Data protection

7.4 The Data Protection Act applies to any personal information that is processed or stored, including information that is recorded as a result of monitoring. Such information should therefore comply with the principles of data protection for fair and lawful processing of data. These principles include:

- personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- personal data shall be accurate and, where necessary, kept up to date
- personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Employment Practices Code

7.5 The Information Commissioner's Employment Practices Data Protection Code deals with employer monitoring of workers by use of email or telephone screening, CCTV, video surveillance etc. The code says that the Data Protection Act does not prevent monitoring, but that the adverse impact of monitoring on individuals must be justified by the benefits to the employer and others. This involves balancing the infringement of privacy against the employer's legitimate aims.

Core principles

7.6 The code sets out five core principles for employers to follow:

- it will usually be intrusive to monitor your workers

- workers have legitimate expectations that they can keep their personal lives private and that they are 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 the 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
- in any event, workers' awareness will influence their expectations.

7.7 The code recommends that employers carry out an impact assessment to establish whether the monitoring is justified. The assessment should consider alternatives that would meet their requirements and whether the monitoring can be limited or targeted as necessary.

7.8 The code also says that trade unions should be consulted about developing and implementing practices that involve processing personal information about workers.

Monitoring e-communications

7.9 A section of the code deals specifically with monitoring telephone, fax, email, voicemail, internet access and other forms of electronic communication.

7.10 The code recommends a policy for use of such communications. The policy should:

- set out the circumstances in which workers may or may not use the employer's telephone systems (including mobile phones), email system and internet access for private communications
- make clear the extent and type of private use that is allowed, for example restrictions on overseas phone calls or limits on the size and/or type of email attachments that they can send or receive
- in the case of internet access, specify clearly any restrictions on material that can be viewed or copied. A simple ban on 'offensive material' is unlikely to be clear enough for people to know what is and is not allowed. Employers may wish to consider giving examples of the sort of material that is considered offensive, for example material containing racist terminology or nudity
- advise workers about the general need to exercise care; any relevant rules and what personal information they are

allowed to include in particular types of communication

- make clear what alternatives can be used, for instance the confidentiality of communications with the company doctor can only be ensured if they are sent by internal post, rather than email, and are suitably marked
- lay down clear rules for private use of the employer's communication equipment when used from home or away from the workplace, for instance the use of facilities that enable external dialling into company networks
- explain the purposes for which monitoring is conducted, the extent of the monitoring and the means used
- outline how the policy is enforced and the penalties for breaching it.

Other sections

7.11 The code also has sections dealing specifically with video and audio monitoring, in-vehicle monitoring and monitoring information from third parties.

7.12 As set out in the core principles, covert monitoring of workers should be exceptional. The code suggests this should only happen where senior management is satisfied that there are grounds for suspecting criminal activity or 'equivalent malpractice' and where they consider that notifying individuals would prejudice its prevention or detection. It also stresses that this should not be used in areas where workers would genuinely and reasonably expect to be private.

7.13 There is a separate code for small businesses, where the expectation is that the same principles should apply, though monitoring is likely to be on a different scale.

7.14 The code can be found at https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Human Rights Act

7.15 The Human Rights Act 1998 incorporates the European Convention on Human Rights directly into UK law. Article 8 of the Convention provides workers with the right to respect for their private and family life, their home and correspondence. This is not an absolute right and interference with privacy can be justified in some circumstances. However, routine monitoring of all calls and emails may violate human rights.

7.16 In the case of *Halford v UK*, the European Court of Human Rights held that there had been a breach of the right to privacy under

the Convention. In this case the employer intercepted phone calls on Ms Halford's private line at work, when she had not been warned of any monitoring and therefore had reasonable grounds to expect privacy. However if employees have been told that there is no privacy, employers may not be in breach of the Act.

8. Social media pitfalls

8.1 With the increased use of social networking sites like Facebook, Instagram and Twitter, many employers are checking employees', or prospective employees', social media posts.

8.2 Even if social media profiles are private, many people have 'friends' or 'followers' who are also work colleagues. There is therefore a risk that these colleagues could inform the employer of things that are posted online. Screenshots of posts can be taken and forwarded on, so be mindful of what you post before doing so. Examples of what to watch out for are set out in this section.

8.3 During the recruitment process, prospective employers will often look at a candidate's social media profile before deciding whether to offer them the job. It is therefore important to consider whether you would be happy for your employer, or a potential employer, to see the things you post online.

8.4 Employers have been known to check the social media accounts of employees who are absent due to sickness for evidence that they are not unwell. In several Prospect cases, employers have produced screen shots from employees' social media accounts as 'evidence' that they were not as unwell as they said they were and even to question whether a member really was disabled.

8.5 Civil servants are bound by the Civil Service Code, which sets out behavioural standards, including objectivity and impartiality. Posting content online that could be considered to breach the Civil Service Code (eg making statements of a political nature) may result in disciplinary action. All members, not just those who work in the civil service, should be aware of this.

8.6 Disciplinary measures may be a legitimate course of action if comments made on social media, on a blog or in any other form could damage the employer's reputation and/or bring the organisation into disrepute. Such comments could also breach an employee's duty of confidentiality towards their employer. In the case of *Zaver v Dorchester Hotel Ltd*, a tribunal found that an employee who had set up a public blog where he listed specific and general workplace concerns was dismissed fairly because the blog breached the employee's duty of confidentiality.

8.7 Disciplinary action can also be taken against workers who make personal remarks about other colleagues online . In the case of *Young v Argos Ltd*, an employee was dismissed for gross misconduct after they 'liked' a Facebook comment that described their

manager as being 'as much use as a chocolate teapot'. The tribunal found the dismissal unfair because no reasonable employer could have concluded that the comment amounted to gross misconduct. However, some form of disciplinary action would be likely to be considered fair.

9. Policies on acceptable use of technology and social media

9.1 Many employers have email, internet and social media policies which provide rules on the use of computer facilities.

9.2 Representatives in Prospect areas have been actively involved in negotiating these policies with employers to ensure that staff are clear about what is acceptable. These policies are often called 'acceptable use' policies.

9.3 Acceptable use policies should have input from human resources and IT departments and be negotiated with trade unions. Such policies can vary enormously depending on the company or organisation and workers' use and access to the systems.

9.4 Prospect encourages the introduction of such policies so that everyone is clear about what is acceptable. They are also an important way of identifying discrimination and harassment issues.

9.5 Representatives should ensure that their policies refer to, and comply with, the Information Commissioner's Code (see section 7).

9.6 The checklist below covers the topics that Prospect recommends should be included in a policy for appropriate use of social media, technology and internet facilities. It highlights issues that impact on the employment relationship rather than technical, legal or housekeeping issues which should also be included in such policies, but are outside the scope of this guide.

Application

9.7 The policy should:

- be subject to full consultation with trade unions before it is introduced
- apply to all workers, including freelancers, temporary and agency workers and contractors
- be widely disseminated to all workers (eg by email, displayed on the staff intranet or in induction training to new starters)
- be incorporated into the staff handbook and contracts of employment
- provide for regular review in consultation with the trade union.

Use

9.8 The policy should:

- not be unduly punitive
- be clear on what is acceptable use
- allow workers reasonable personal use
- identify restricted areas of the system
- provide for rules on confidentiality

- provide information about email, blog and social media etiquette to avoid offence
- be clear about any political or other restrictions placed on staff, particularly in relation to their use of social media
- provide rules to prevent the organisation being brought into disrepute
- be clear on whether loading or downloading software is prohibited
- clearly identify potential disciplinary offences
- cross-refer to the disciplinary procedure to ensure that procedures are fairly applied
- agree the trade union's use of technology facilities.

Equality

9.9 The policy should:

- state that all workers are entitled to be treated with dignity and respect at work, regardless of any protected characteristic
- refer to the organisation's equality and diversity policy
- forbid the use of facilities for accessing or circulating racist, sexist or other offensive material
- forbid accessing pornographic or obscene material
- make harassment or bullying by email, social media or any other form a disciplinary offence
- provide advice for employees who are harassed, bullied or intimidated by other people's use of facilities.

Monitoring

9.10 The policy should:

- exclude routine monitoring of email or internet use
- advise workers that the employer does not guarantee absolute privacy
- state whether emails will be accessed in the worker's absence
- provide for unions to be alerted before monitoring happens
- require any monitoring which is undertaken to be open (known to users)
- obtain employees' consent before monitoring
- ensure that all forms of surveillance or monitoring are proportionate
- forbid monitoring of union communications
- entitle employees to privacy through access to phones and email for personal use which will not be subject to monitoring.

Trade union use

9.11 Just as trade unions negotiate for the use of phones, photocopying and office equipment, it is equally important to ensure that union representatives have access to computer facilities in the workplace. This will include their use for communicating with management, representatives and members.

9.12 It is important to ensure that management does not monitor emails sent or received in the course of trade union activities, for example communications between representatives or with members over personal cases. Official policy should include a guarantee of privacy in respect of such emails. Representatives and members should always be cautious about using work email for potentially sensitive information.

9.13 Reps who use social media for union purposes, such as campaigns or communications with members etc, should be mindful of what they post. Make sure that you:

- do not post any comments or information about confidential matters such as personal cases
- respect the union's policies and negotiating objectives
- avoid negative comments about other unions and take care that any comment you make about employers are in line with legitimate industrial relations practice

9.14 Many Prospect branches and sections have developed their own websites or have pages on the employing organisation's intranet. Where there is an agreement about use of the intranet, representatives need to be clear about the scope, content or use of such material. Disagreements with the employer over this should be referred to your full time-officer. This guide cannot cover best practice on this, but Prospect's communications team can provide advice on content and presentation.

10. Dos and don'ts

10.1 Guidance on the use of email, social media and the internet at work:

Do:

- find out if your employer has a policy on acceptable use
- familiarise yourself with the policy
- encourage your Prospect representative to negotiate a policy if one does not exist
- ensure that you stay within the terms of the policy
- respect other colleagues at work
- remember that emails and internet access can be traced
- remember that social media sites are public so anything you write may be brought to the employer's attention
- remember that posting on social media, even in a personal capacity, may lead to disciplinary action against you.

Don't:

- use email or internet facilities for personal use if this is not allowed
- use the facilities excessively for personal use
- access pornographic or offensive materials
- send or forward offensive or harassing messages
- load unauthorised software
- access parts of the computer to which you do not have official permission.

11. Resources and addresses

Prospect guides

Guide on the Right to Disconnect: https://library.prospect.org.uk/download/2021/00381

Members' guide to preventing work-related stress: https://library.prospect.org.uk/download/2020/00393

Members' Guide to Working Time: https://library.prospect.org.uk/download/2011/00537

Members' guide to equality at work: https://library.prospect.org.uk/download/2008/00092

Members' guide to bullying and harassment: https://library.prospect.org.uk/download/2007/00549

All Prospect guides are available by logging on at https://prospect.org.uk/

Other publications

Employment Practices Data Protection Code – Information Commissioner (www.ico.gov.uk): https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

TUC report – I'll be watching you: https://www.tuc.org.uk/i'll-be-watching-you-what-workplace-monitoring

TUC report - The future of flexible work: addressing the risks of increased homeworking: https://www.tuc.org.uk/research-analysis/reports/future-flexible-work?page=5

Contact

Prospect member contact centre: **0300 600 1878** if you need further information or advice.

New Prospect House
8 Leake Street
London SE1 7NN
0300 600 1878
enquiries@prospect.org.uk

22-0115/FEB23/PDF

prospect.org.uk

ProspectUnion