CPNI
Centre for the Protection of National Infrastructure

# PERSONNEL SECURITY IN REMOTE WORKING

## A GOOD PRACTICE GUIDE

**FEBRUARY 2012**

# Contents

# Introduction

### The aim of this guidance

This document provides guidance on good personnel security practice for remote working on a regular or permanent basis. The guidance is intended for employers (particularly managers, human resources and security departments) and employees in the national infrastructure.

Remote working can bring many benefits to both employers and employees in terms of flexible working patterns, higher commitment and retention of staff and overall cost savings. However, remote working does introduce additional personnel security risks which, if left unchecked, may lead to more serious consequences, such as an insider act[1]. These risks can be reduced by introducing effective policies and procedures.

This document aims to inform employers about the personnel security vulnerabilities of remote working and provide practical guidance on reducing these risks. It is not intended to replace an organisation's remote working policy but rather to provide information about good practice in this area.

In writing this guidance, CPNI has consulted a range of bodies from the private sector, from government departments and agencies, and legal experts. Those interviewed included managers of remote workers and of remote working policy, a number of whom were remote workers themselves. CPNI has also conducted open source research on this subject.

CPNI recommends that organisations seek professional advice, especially on employment law, when implementing or amending their personnel security measures.

This document should be read in conjunction with other guidance published by CPNI, in particular:

- *Risk Assessment for Personnel Security: a guide*
- *Ongoing Personnel Security: a good practice guide*
- *Personnel Security in Offshore Locations*

These guidance documents can be downloaded from www.cpni.gov.uk.

[1] An insider is someone (a permanent, temporary or contract worker) who exploits, or who has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes. A recent CPNI study of the insider threat found that a frequently recurring theme amongst identified insiders was unhappiness and frustration due to a combination of poor management relationships, unhealthy work/life balances and a perceived lack of recognition.

# What is remote working?


For the purposes of this document, '**remote working**' is used to describe employees who work away from an organisation's main site. This may be from home, from a remote office or it may be on the move. Other common terms include:

**homeworking** - where the employee works mainly in their own home, or in different places using their home as a base;

**mobile working** - working from any location including in hotels, work-hubs (see page 11), or in transit;

**agile working** – dividing time, working from a main site and another location other than a contracted place of work;

**teleworking** or **telecommuting** - working in a location that is separate from a central workplace, by using telecommunication technologies.

Statistics show that the number of remote workers in the UK has increased from 2.28 million in 1997 to 3.7 million (12.8 percent of the working population) in 2009. By 2012, it is estimated that over 6.5 million workers (over 20 percent of the working population) will be working in this way.[2]

[2] Office for National Statistics Labour Force Survey; www.workwiseuk.org; www.flexibility.co.uk

# Benefits of remote working

## For the organisation

- Remote working can raise morale, commitment and engagement with the organisation. Organisations may not lose skilled employees if their personal circumstances change.
- Remote working can be a positive factor in the recruitment and retention of a more diverse and experienced workforce. Employers can recruit talented employees from anywhere in the country instead of just around their local office. Remote working may also offer an attractive and popular non-monetary incentive to motivate and reward employees.
- Remote working can result in savings for organisations by consolidating desk and office space; reducing car parking space, and reducing other costs including electricity, heating, printing and catering. Organisations can become more environmentally friendly by reducing their carbon footprints; however, such savings might be offset by transferring the burden to the remote worker.
- Remote working can lead to lower rates of absenteeism as remote workers may be able to continue to work from home if not faced with having to make the journey to their work location.

## For the employee

- Remote working allows employees greater flexibility and they can be located where they are needed. They can work in their own environments at their own pace and at times which suit them best. This results in more effective time management (e.g. in respect of family commitments or health problems) and can improve their work-life balance.

- Remote working can also increase motivation, morale and job satisfaction. This can lead to greater loyalty and affinity with the employer organisation.
- Remote workers can be more productive when working away from the office environment. They can be more creative, with greater ‘thinking time’ than in the office. Remote workers can be more focused and less easily distracted than they might be if working in an open plan environment, for example. They do not have to contend with noise in the workplace, telephones ringing continually, or the daily commute. This not only reduces the stress of the commute, but also the pressure of working in an office environment.

# Remote working: personnel security issues

While there are many advantages to remote working, it brings with it a number of personnel security issues for both the organisation and the individual:

## For the organisation

- Direct supervision of remote workers is not possible: managers cannot physically observe their employees' performance. Also, providing timely, reliable and constructive feedback is more challenging for managers of remote workers. There is a perception amongst some managers that remote workers will not work unless under close supervision. It may also take longer for issues to emerge and be discussed and dealt with.

- Remote working can erode company culture and departmental or individual morale. If employees with a positive impact on the team environment enter into a remote working agreement, their absence is often felt by the team members left behind, either through missed contact, disruption of the team's activities, or through resentment if they do not have their own remote working agreement. Change to a group's dynamics can unsettle it, and the group's activities may have to change significantly to accommodate this new practice.

- Remote working can incur a variety of increased security risks, e.g. loss of IT equipment or sensitive company data. Employees may not realise the risks of having sensitive data in their possession outside the workplace, nor adopt policies and standards appropriate for their personal data. Organisations should stress the importance of document and IT security including storage and transportation, and outline possible sanctions if an organisation's security policies are breached. Organisations might wish to consider establishing registers for documents/sensitive data and equipment which are removed from their sites, particularly if held for significant periods of time by remote workers.

- Remote workers may live in shared accommodation with other people not employed by the organisation. Organisations have little or no control over these environments. There is a risk that remote workers might divulge commercially sensitive or operational information with house-mates or family members, however inadvertently. There may also be security issues surrounding the storage of sensitive data and IT equipment. Organisations should provide security advice on what may or may not be discussed with house-mates/family members, and consider policies relating to the use of company IT equipment or working on company documents in the company of house-mates, and the use of company IT equipment by house-mates/family members (see also page 12).

- Organisations may have insufficient welfare or support systems in place for remote workers. Welfare issues may not be identified or acted on until they develop into more serious problems. This is discussed further in the chapter on *Welfare considerations*.

## For the employee

- Whilst remote working can lead to greater flexibility and autonomy, there is a perception that remote workers can become more lonely, isolated or ineffective. They may have little or no contact with management or colleagues, and can develop feelings of being ‘left out of the loop’. They may not be fully informed of important information, organisational or procedural changes, or considered for promotion or other development opportunities. The ‘water cooler’ moments of general chit chat and bonding are missing. Networking opportunities with colleagues and clients may also diminish. Those who feel alienated from an organisation are less likely to engage with its values and culture and this may have an adverse impact on the loyalty of the employees to the organisation.

- Some employees may be unsuited to working from home. Their productivity could drop, either because of family distractions or their own limited capacity to focus on tasks. Work/family life may become blurred; family and friends might not appreciate that working from home does not mean that remote workers are available to do household chores, school runs etc (although prioritising the working day and tasks efficiently may allow remote workers to do this). If remote workers cannot adjust to their new working environment, job satisfaction can decline.

- Whilst remote workers can be more productive, they may have a tendency to overwork. They may consciously work long hours, including at evenings and weekends, to dispel misconceptions by management and colleagues that they are not pulling their weight. Working long hours from home risks contravening the European Working Time Directive 1998, which applies equally to remote workers as it does to office-based staff. Overworking may increase the risk of home workers suffering from burnout. Colleagues and clients who are office-based can forget that those who work from home are not available round the clock.

- Organisations are increasingly introducing open-plan office spaces, hot desks, and ratios of desk to staff numbers. This may reduce the incentive to work in the office. Employees may become disaffected, believing that they have no other choice but to work at home. They may also incur increased financial burdens of heating, electricity, telephone and broadband use, for example, offsetting the savings made by organisations. These factors could lead to resentment and increase the likelihood of employee disaffection, an important precursor to more serious problems such as counter-productive work behaviours and malicious activity.

# Policy and legal considerations for remote workers

## Remote working policies


Organisations should ensure that they have robust but flexible remote working policies. Such policies should be defined clearly to avoid ambiguity or confusion, particularly in any contract between the employer and the remote worker. If appropriate, a new contract should be entered into if it is likely to be significantly different from an existing contract. Policies should be flexible enough to respond to changing priorities and circumstances within the organisation.

An organisation's remote working policies should include:

- whether any jobs or activities within an organisation are not permitted under remote or mobile working e.g. financial transactions, processing of sensitive or personal data, some IT roles;
- security and storage of documents, sensitive data and IT equipment (including password protection); the sending of documents or sensitive data either in hard copy or electronically; disposal of data; sanctions/disciplinary procedures for breaching security policies, loss of data or equipment;
- financial obligations, i.e. payment for the use of telephone, broadband, stationery, heating and lighting and travel expenses, either by the organisation or the employee;
- attendance in the workplace, frequency of meetings with management and colleagues.

Mandatory Requirements 9 and 10 of the HMG Security Policy Framework (version 7, October 2011) require government departments and agencies or organisations handling HMG assets to put in place appropriate policies and procedures to support mobile and remote working, and the security of all portable and electronic devices used for these purposes.

Organisations also need to consider the financial and tax liabilities inherent with remote working, e.g. tax on equipment, council tax, mortgage/tenancy agreements, and insurance. If not met by the organisation, these may incur a significant financial burden for remote workers, who should demonstrate that they are able to meet any additional financial obligations. Her Majesty's Revenue and Customs (HMRC) provides guidance to employers and employees on tax rules.[3]

Organisations should ensure that their existing business insurance covers remote workers. They should undertake regular visits to the home to ensure that the work station complies with both relevant legislation and the terms of their insurance.

[3] www.hmrc.gov.uk/incometax/relief-household.htm; www.hmrc.gov.uk/paye/exb/a-z/h/homeworking.htm

## Legislation

The legal responsibilities of the employer in the workplace apply equally to the home working environment. Legislation applicable includes:

**Data Protection Act (1998)**: concerns the processing and storage of personal information, irrespective of where this is carried out. Is the data secured against theft and from viewing by family members and visitors?

**Health and Safety at Work Act (1974)**: ensures the welfare, health and safety of employees wherever they work. Under section 2(4) of the Act safety representatives, appointed by a recognised Trade Union, can represent home workers in any consultations with employers concerning health and safety and welfare matters.

**Working Time Regulations (1998)**: stipulate that, unless opted out of, workers should work no more than 48 hours per week. They also provide directives on breaks taken, and paid annual leave.[4]

**Display Screen Equipment Regulations (1992) (amended by the Health and Safety (Miscellaneous Amendments) Regulations 2002)**: anyone, including remote workers, who uses computers on a regular basis (i.e. for a third or more of their working time for a continuous period of one month), is entitled to an eye test paid for by their employer.

**Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995**: employers have a duty to report and record work-related accidents, injuries and other occurrences arising from work-related activities, including home working.

**Employment Act (2002)**: an employer may reject an application to commence remote working if the desired working pattern cannot be accommodated by the needs of the business.

This list is not exhaustive. CPNI strongly recommends that employers consult employment lawyers when implementing or updating their policies on remote working.

[4] www.hse.gov.uk/contact/faqs/workingtimedirective.htm

# Commencing remote working: protective security advice

Undertaking a Personnel Security Risk Assessment may identify concerns before an employee undertakes remote working. Appropriate measures can then be identified to reduce the risk of malicious activity taking place. A risk assessment could also identify posts with a heightened security risk (with potentially significant impacts on the organisation in terms of loss of assets, business or reputation), which are therefore not suitable for remote working.

Before remote working is undertaken, employees must decide whether remote working is right for them. They should consider, with their employer, how their role could work effectively in a remote location and how work requirements, tasks and meetings can be organised. Employees should speak to existing and previous remote workers about their own experiences, both positive and negative. These may have a bearing on the employee's final decision to commence remote working. The following should be considered:

- **Agree a contract**

If required by the organisation, the employee should state their proposals to work remotely in a business case, which should be authorised by line management and HR. A contract covering remote working arrangements and its provisions should be agreed by the organisation and the employee. (See the previous chapter on *Policy and legal considerations*.)

- **Define work space**

A suitable area at home must be identified to carry out remote working. This may be a spare room or even an area which is not in the main house, e.g. in a suitably appointed garage or shed conversion. This helps separate work/home life. All furniture and IT equipment should be installed and full health and safety/ergonomic assessments carried out. Appropriate physical security measures should also be taken to ensure the home working space is secure. Organisations should provide secure storage containers for the storage of sensitive data and portable devices when not in use.

Remote workers should educate family, friends and neighbours about home working. Because they will often be at home, this does not mean that remote workers are available for domestic or other personal concerns (home working does not equate to child care, for example). Remote workers should consider using a system whereby family understand when they can and cannot be disturbed.

- **IT equipment**

Organisations and remote workers should ensure that all IT equipment (including portable devices) functions properly. Organisations should also ensure that all IT equipment is installed with adequate encryption and security software to reduce the threat of electronic attack or theft of information. Remote workers should receive appropriate training in the use of all IT equipment allocated to them.

- **Induction**

Some organisations have a formal induction process for remote working which new and existing remote workers must complete. This includes the organisation's policies, security considerations and mobile working. Remote working will only commence and equipment be installed following the successful completion of the induction process. An effective induction might include scenario-based exercises based on security and/or health and safety issues surrounding remote working, and how to resolve them. If an organisation requires its employees to undertake such training, this must be included in its remote working policies.

- **Trial period**

Prior to working from home on a permanent basis, employees should undergo a trial period. This could range from anything between one and three months, for example. Employees and management can then assess whether the new working arrangements are a success, or whether they need refining. Employees and management should document the trial period, including the results of all assessments completed, meetings held, and feedback from management, colleagues and clients. If the remote worker finds that reality does not match expectations or if it does not suit them, the remote worker should have the right to request that the remote working arrangement be terminated.

## Mobile working

A common form of remote working is mobile working. This can include working on public or private transport, staying in hotels, working in work hubs, and taking telephone conversations in the street or public places.

Mobile working provides an opportunity to plan the working day, prioritise tasks, read documents or catch up on e-mails. Security awareness is paramount when working in this way, and it should be included in remote working policies (including what tasks may or may not be done when mobile working, and where) and any training prior to the commencement of the remote working arrangement. Policies and training should include the following considerations:

- Mobile workers must consider what they are working on when in transit. Company logos are often emblazoned on laptops or pop up as screensavers/wallpaper. Inconspicuous screensavers should be used as this will reduce the risk of fellow travellers taking an interest in what the remote worker is doing, of connecting the remote worker to an organisation, or eliciting information from the remote worker about their employer, job or company data.

- Mobile telephone conversations in the street or public places should be discreet. Mobile telephone users often talk loudly without being aware of the information they are sharing openly with others, which might include sensitive commercial or organisational data. This may attract unwanted attention or interest about where the mobile worker is employed, or what they do.

- When in transit, it is recommended that mobile workers should not leave any IT equipment or sensitive information (whether hardcopy or electronic) unattended at any time. Such items should be transported in secure document cases or containers. If travelling by vehicle, IT equipment and sensitive information should be stored securely, and removed whenever the mobile worker leaves the vehicle.

- Within government, assets with a protective marking of CONFIDENTIAL or above should not be removed from government premises. Mobile workers should not work on official documents while travelling on public transport, or communicate their contents by telephone or unsecure e-mail. Official documents worked on at home should be kept in secure document containers.

- Working within a ‘work hub’ may reduce the above risks. Work hubs provide low-cost desks and meeting spaces if working from home is not practical. However, as the space is rented, the remote worker will have no control over who will be working adjacently or nearby. Consideration should therefore be given to what can be worked on securely and the means of storing information.

# Personnel security considerations for staff working overseas

Having staff working overseas brings a number of challenges for organisations, not least the logistical difficulty of being separated geographically. UK-based organisations may not be familiar with local customs, security practice and legislation. Managers are increasingly responsible for employees based abroad, and will have little or no knowledge of them.

CPNI's '*Personnel Security in Offshore Locations*' highlights policies and procedures which organisations could implement for staff working overseas. The following should be considered when formulating remote working policies:

- Organisations may wish to locate some UK employees in overseas locations; ideally such staff should be those fluent in the local language. They can oversee the work and any security issues which arise, and increase the flow of information between offices. Organisations can also assign a UK-based mentor to overseas staff, allowing for increased communication and engagement.

- Organisations should consider exchanging staff between locations for training, development and work opportunities. This may increase awareness of cultural diversity. Longer-term UK postings for overseas staff, including Intra Company Transfers under the UK immigration rules[5], may also be an option for organisations.

- Managers and senior staff members should visit overseas staff on a regular basis and maintain frequent contact with them. This helps management to have a good understanding of local issues and establishes a better degree of oversight to ensure security and compliance. In some organisations, new management delay visiting overseas staff for a considerable time or have infrequent contact with overseas staff.

- When managing performance, particularly if working in different areas or time zones, it is advisable to avoid having the manager and the counter-signing officer at a considerable distance, or based in the same place. Rather, it might be practical for at least one of them to be located as close to the remote worker as possible, or to consider having more local management arrangements.

- Some countries and cultures have different expectations regarding working hours. Some may have different work patterns, for example Friday and Saturday may form the weekend instead of Saturday and Sunday. UK-based organisations must take this into consideration when arranging meetings or identifying suitable times to contact overseas staff. In some cultures, it is common practice and even expected that overseas staff residing in remote villages, for example, make IT equipment available for general use by family and neighbours. Organisations should bear this in mind when deciding policies on appropriate incidental usage of IT equipment by overseas staff.

[5] www.ukba.homeoffice.gov.uk/business-sponsors/

- Managers and staff working overseas should agree protocols on the frequency and means of communication (i.e. telephone, e-mail, videoconferencing etc). UK-based workers should not just hold meetings during regular UK working hours, but should also plan meetings which fit in with local working hours.

- For UK-based staff travelling or working overseas, organisations should provide training and guidance on countries visited. This can include culture, customs, advising on places to visit or stay, communicating with and managing staff of different nationalities, and even on issues such as the exchanging of appropriate gifts.

- Overseas-based staff should also receive guidance on the risk of approaches by foreign nationals who may befriend overseas-based staff to elicit information about the organisation's operations, or blackmail staff into providing commercially sensitive data or information of an intelligence value (e.g. by the use of the established and highly effective 'honeytrap'). If left to escalate, such activity could, for example, lead to the removal of the employee's security clearance if the organisation is governed by National Security Vetting regulations. Staff should report any approaches they consider unusual to the organisation's security department at the earliest opportunity.

- Organisations should provide staff with travel advice, particularly on areas with difficult or dangerous working environments. This could be provided by an independent supplier, who will have locally-based staff who can advise on particular issues, and who can meet and accompany staff if required. Staff should be encouraged to 'check in' at regular intervals to confirm that they are safe and well, and that there are no issues of concern. Staff visiting overseas should also be advised to avoid drawing attention to themselves, either through their behaviour or their overt affiliation to the parent organisation if there are security concerns in that particular country. Foreign and Commonwealth Office travel advice can be found at www.fco.gov.uk/en/travel-and-living-abroad/travel-advice-by-country/.

# Managing remote working: personnel security considerations

Good management is key to reducing the risk of employee disaffection and the potential for an insider act occurring, and the same high standards must apply to managing remote workers. The manager should provide vision, coaching, support, and sufficient tools and information for the remote worker to complete tasks effectively. See also CPNI's '*Ongoing Personnel Security: a good practice guide*'.

## The manager/remote worker relationship

Managers must be accessible and should ensure that remote workers know when they can be contacted and for what purpose. It may be the case that, like members of their team, the manager will also be a remote worker. This allows the manager to have a greater understanding of the issues and requirements of team members working remotely, as they will often be similar to those of the manager. Issues can be identified at an early stage, and discussed and resolved as appropriate.

Managers must be able to trust their remote workers to complete their work without the need for constant supervision or micro-management. Being too controlling may cause resentment amongst staff, and will erode trust in the manager. There is also a risk that, as a result, remote workers become too compliant and dependent on the manager, or become apathetic[6], with the risk of team performance suffering as a result.

Relationships between management and remote workers develop over time. Inevitably, staff turnaround means that managers will be replaced, and new manager/ remote worker relations have to start again from scratch. New managers and remote workers should meet each other as soon as possible, and invest sufficient time and effort in building these new relationships by getting to know each other, holding regular meetings, and defining the requirements and expectations of both parties.

## Managing the performance of remote workers

- **Set objectives**

Prior to the start of a remote working arrangement, managers and remote workers are advised to meet to set and record SMART job and development objectives (this should include agreement on the collation of evidence of work completed). This will reduce the risk of remote workers over- or under-working. If duties or responsibilities change, this must be reflected in the job and development objectives as soon as is practical.

**S**pecific
**M**easureable
**A**greed
**R**ealistic
**T**ime-framed

[6] The Distance Manager (Kimball Fisher and Mareen Duncan Fisher, 2004)

- **Agree schedule for meetings**

Agreement should also be reached on the number and frequency of meetings to be held throughout the year to discuss matters such as objectives and target setting, performance reviews, organisational and welfare matters. These meetings can be a mixture of the formal and informal. Consideration should also be given to the means of communication, i.e. regular face-to-face contact (particularly if discussing sensitive issues), e-mails, instant messaging or video-conferencing.

- **Feedback**

Managers and remote workers should actively seek and offer feedback on their respective performances. Feedback must be fair, consistent and proportionate to be of value to both the manager and the remote worker. Feedback should be sought from a variety of sources including management, colleagues and clients on subjects including performance and behaviour. This could be achieved by conducting 360 degree appraisals, for example.

- **Training and development**

Personal and career development for the remote worker should be no different from that of other workers. The manager should assess the needs of the remote worker and of the team to determine the most appropriate form of training, be it face-to-face, web-based or by video-conferencing.

Depending on the structure of the organisation, remote workers could be allocated specific roles within the team in addition to their core duties. These would depend on the size and work of the team but might include policy, IT, training or technical disciplines, mentoring new staff to remote working, or planning and organising meetings or conferences. They would be the first point of contact for issues concerning their particular role and be responsible for communicating with, and coaching, other team members.

- **Rewards**

Where organisations operate a reward system for meeting and exceeding job objectives and targets, remote workers should be treated in the same way as other employees. Rewards may include financial bonuses or instant recognition awards. Rewards could be decided by management, or by a committee of employees, for example.

- **Disciplinary issues**

Managers also need to consider appropriate action to take should remote workers fail to meet job objectives or targets; not work contracted hours, or behave inappropriately (e.g. misuse IT equipment, lose company equipment or information). Appropriate action may include addressing performance issues at appraisal interviews, informal/formal warning, security awareness training or, in extreme cases, the removal of remote working status. One solution might be to change the hours worked remotely and increase the number of hours undertaken in the workplace. This may reduce the isolation of the remote worker; improve performance and increase communication and engagement with management and colleagues.

## Communicating with remote workers

Communication is a two-way process: managers and remote workers have a duty to maintain effective means of communication. They should decide before the remote working arrangement begins how often they will be in contact and by what means. Managers should contact their staff regularly, even if it is just to provide assurance that the remote worker is not encountering any problems.

A number of organisations run company intranets or internal social networking sites. Staff can keep up to date with company news or changes, and development opportunities. Cyber cafes and chat rooms allow day-to-day interaction with colleagues, corporate networking and socialising. Company intranet sites can be used to provide practical help and advice on remote working issues; staff can share experiences of remote working by writing blogs on the subject.

Team engagement can be difficult, particularly if staff work in a variety of locations. However, it is important that this is encouraged as it allows colleagues to get to know each other, reduces feelings of isolation, promotes a common purpose within the team, and provides an opportunity for social activities. As with managers, remote workers should keep in contact with colleagues by sharing diaries, e-mails or instant messaging (which is handy for small talk - the ‘water cooler’ moments).

## Terminating the remote working arrangement

If the arrangement is successful for the organisation, management and the employee, remote working can continue for years. However, there will be instances when the remote working arrangement should be terminated. These should be reflected in company policy and all contracts.

Remote working must be reversible if business requirements change or if it is no longer in the organisation’s interest. This may include changes in the organisational structure or business, or financial or regulatory reasons. It should also apply if the remote worker’s personal circumstances change, or if they take up a new job which is office-based.

The organisation may decide to cancel a remote working arrangement if the remote worker is not meeting job objectives or targets, or for a breach of organisational policy or conduct (this might include inappropriate use of IT equipment, a poor security record or other disciplinary offences).

# Welfare considerations for remote workers

Managers have the same duty of care towards remote workers as they have for other workers. However, there are some additional challenges for the manager and the remote worker to identify and resolve welfare issues as soon as they arise. The chapter on *Policy and legislation* outlines the legislation to which organisations must adhere.

Managers should be able to identify the signs and symptoms of employees with personal issues, in particular isolation or lack of contact with colleagues. Remote workers who believe that isolation is having a negative impact on their well-being should discuss with their manager how to overcome their difficulties; this could include more frequent visits to the workplace, for example. Sensitive handling of such cases will go a long way in ensuring that such problems do not escalate unnecessarily.

Working hours should be monitored by both the remote worker and the manager to identify instances of under- or over-working. Remote workers should report any concerns about excessive working hours to their manager. Managers have a duty to ensure that remote workers do not contravene the Working Time Regulations and Health and Safety Directives for display screen users[7]. Managers should ensure that remote workers aware to the need to take regular breaks when working for more than one hour with IT equipment. Managers should also ensure that remote workers take sufficient leave or time off in lieu for extra time worked.

Remote workers should inform their managers of absence from work due to sickness or other reasons as appropriate (e.g. compassionate leave) in accordance with the organisation's sickness and absence policies. Remote workers should also report any change in circumstances to their manager (e.g. change of address or working environment). Health and safety and ergonomic assessments should be undertaken as required. Remote workers can be more inclined to work through their illnesses;[8] nevertheless employers should ensure that their remote workers take sufficient time off to recover from sickness.

Organisations might provide an independent counselling service to support remote workers. Remote workers and their families can contact a service hotline and receive independent and impartial advice and counselling.

Company intranet sites can be used to address welfare issues through cyber cafes, chat rooms and blogs, and can offer practical help and advice on welfare issues. They can also outline legislation and regulations relevant to remote working conditions.

[7] www.hse.gov.uk/msd/dse/guidance.htm

[8] Homeworking: psychological implications and practical solutions. Mendas white paper November 2009

# Useful websites and further guidance

The following organisations provide useful and practical guidance on their websites on remote working:

**Chartered Institute of Personnel and Development (CIPD)** – www.cipd.co.uk.
Factsheets on health and well being at work, including work-life balance (revised September 2011) and flexible working (revised August 2011).

**Health and Safety Executive (HSE)** – www.hse.gov.uk.
Publications INDG73 (rev2) working alone – health and safety guidance on the risks of lone working (September 2009) and INDG226 home working – guidance for employers and employees in health and safety.

**British Security Industry Association (BSIA)** – www.bsia.co.uk.
Forms 248: health and safety for lone workers – a guide and 288: lone workers – an employers guide (February 2010).

**Information Commissioner's Office (ICO)** - www.ico.gov.uk.
Information on data handling, and the responsibilities of employers and employees under the Data Protection Act (1998).

**Directgov** – www.direct.gov.uk.
Search for working from home. Government website providing advice to employers and employees on remote working.

**Business Link** – www.businesslink.gov.uk.
Search for working from home. Government website providing advice to employers and employees on remote working.

**Flexibility** – www.flexibility.co.uk.
Not-for-profit venture which raises awareness on the impact and benefits of flexible working.

**WorkWise UK** – www.workwiseuk.org.
Not-for-profit organisation which encourages smarter working practices including flexible, remote and home working. Runs an annual week of activities including National Work From Home Day, Mobile Working Day and Virtual Meeting Day.

**Telework Association** – www.telework.org.uk.
Not-for-profit organisation promoting the benefits of teleworking and providing support to individuals and organisations.