



PERSONNEL SECURITY GUIDANCE ON REMOTE WORKING

December 2020

Introduction

Who?

The guidance is intended for employers, particularly line managers, human resource professionals and security teams, in the UK national infrastructure.

What?

This document provides guidance on good personnel security practice for remote working on a regular or permanent basis. For the purpose of this guidance, remote working is defined as working beyond your organisation's own site or premises.

Why?

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 act¹. These risks can be reduced by introducing effective policies and procedures.

How?

This document aims to inform employers about the personnel security vulnerabilities of remote working and provide practical guidance on reducing these risks, which can help provide solutions to wider security risks across the organisation.



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 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.

KEY POINTS

- **Understand the benefits and security risks of remote working to your organisation and employees.**

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. Some of these benefits and risks have been summarised in the table at Annex A.

- **Conduct a Personnel Risk Assessment for remote working in your organisation.**

Undertaking a Personnel Security Risk Assessment may identify concerns before the organisation embraces remote working. Appropriate measures can then be developed to reduce the risk of malicious activity taking place. A Per Sec Risk Assessment could also identify specific 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. Further advice on Personal Security Risk Assessment can be found at www.cpni.gov.uk/insider-risk-assessment.

- **Consider the relevant legal issues for remote workers in your organisation**

The law, as it applies to remote working in your organisation, should be considered by your own legal advisors at an early stage and factored into any future policy. Some relevant pieces of legislation are listed at Annex B.

- **Create an appropriate Remote Working policy and communicate it effectively to both line managers and staff across your organisation.**

An organisation should ensure that it has robust, but flexible, remote working policy. It should be defined clearly to avoid ambiguity or confusion, particularly in any contractual matters between the employer and the remote worker. The policy should be flexible enough to respond to changing priorities and circumstances within your organisation. A suggested list of topics that should be included in a remote working policy is at Annex C

- **Consider welfare issues for remote workers in your organisation.**

Managers have the same duty of care towards remote workers as they have for all other workers. However, there are some additional challenges for the manager to identify and resolve welfare issues quickly. Some of these challenges are discussed in more detail in Annex D.

- **Provide Line Managers with guidance and training for managing remote workers.**

- **Provide remote working employees with appropriate guidance and training.**

1. Action for employers and employees before commencing remote working:

Before remote working is undertaken, both employer and employees should consider and agree how their role could work effectively in a remote location and how work requirements, tasks and meetings can be organised. The following should be considered:

- **Remote working 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.

- **Define workspace**

Ideally an employer or the remote worker should identify a suitably defined and secure area to carry out remote working. For the employer this may be an agreed shared working hub, and for the worker this might be a dedicated room at home, which will separate work/home life. The physical security of a remote working area should be assessed, especially where there is uncontrolled shared access. If necessary, organisations should provide secure storage containers for the storage of sensitive data and portable devices when not in use. Remote workers should be provided with a reporting mechanism for lost or stolen material or devices

Appropriate working furniture should be made available and, if possible, a health and safety/ergonomic assessment carried out as soon as remote working commences. Secure IT should be provided with training and technical support available.

Remote workers should educate family, friends and neighbours about home working. Just 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 childcare, 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 provided 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.

Remote workers should consider personal Smart Devices within their household and seek technical advice about their proximity to working areas.

2. Actions for Employers and Employees Commencing Remote Working

- **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. Ideally remote working will only begin, 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. This should include recognising a range of security concerns and how to report 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. 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 they are unable to work effectively in this way, the remote worker should have the right to request that the remote working arrangement be terminated.

3. Ongoing 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 as it does to those based on site. The manager should provide vision, coaching, support, and sufficient tools and information for the remote worker to complete tasks effectively. Guidance is provided in CPNI's '*Ongoing Personnel Security: a good practice guide*' available on this webpage:

<https://www.cpni.gov.uk/ongoing-personnel-security>

- **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. CPNI's 'Preserving Organisational Trust' provides advice and guidance how to do this, especially in times of change.

<https://www.cpni.gov.uk/system/files/documents/93/4c/Organisation%20Trust%20factsheet%20v3.2.pdf>.

Relationships between management and remote workers develop over time. 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 SMART job 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 recorded.

- **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. For example, this could be achieved by conducting 360-degree appraisals.

- **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.

- **Working Remotely Overseas**

Organisations should have security policies and procedures in place for staff working remotely overseas. These policies should cover both when an employee is required to work, at the request of the organisation, remotely overseas for short periods such as when travelling on business (CPNI advice and guidance can be found in Smart Traveller) and also requests from the employee to base themselves outside of the UK.

Requests from staff to work remotely overseas on a temporary or permanent basis should be individually risk assessed on an exceptional basis. Organisations will wish to consider the role of the individual and sensitivity of the materials being accessed overseas, the security of IT systems and devices, the future security of hard copy materials, local employment laws that might be at odds with your security policies and procedures, particularly relating to: protective monitoring, dual nationality issues, and an inability to recall staff at short notice if circumstances change.

4. 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.

Organisational communications on security must be clear and consistent across the whole workforce to avoid confusion and disgruntlement.

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).

5. 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 organisational 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).

Useful websites and further guidance

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

Centre for Protection of National Infrastructure (CPNI) – Physical and Personnel Security advice for the Critical National Infrastructure. – <https://www.cpni.gov.uk>.

National Cyber Security Centre (NCSC) - <https://www.ncsc.gov.uk/guidance/home-working>
Cyber security advice for organisations with staff working from home.

Chartered Institute of Personnel and Development (CIPD) – www.cipd.co.uk
Information for HR professionals on remote working.

Health and Safety Executive (HSE) – www.hse.gov.uk
Guidance for employers and employees on health and safety when working remotely.

British Security Industry Association (BSIA) – www.bsia.co.uk
Guidance for Lone Workers and Mobile Workers in the security industry.

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

WorkWise UK – www.workwiseuk.org
Not-for-profit organisation which encourages smarter working practices including flexible, remote and home working

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstance.

Benefits of remote working

For the Organisation	For the Employee
Remote working can raise morale, commitment and engagement with the organisation.	Remote working can increase motivation, morale and job satisfaction. This can lead to greater loyalty and affinity with the employer organisation.
Organisations may not lose skilled employees if their personal circumstances change.	Allows employees greater flexibility and can improve their work-life balance. They can work in their own environment, at their own pace and at times which suit them best.
Remote working can be a positive factor in the recruitment and retention of a more diverse and experienced workforce from anywhere in the UK.	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.
Remote working can result in savings for organisations by consolidating desk and office space; reducing costs including electricity, heating, printing and catering. Organisations can become more environmentally friendly by reducing their carbon footprint.	Remote workers can save money for example by not needing to commute and by needing less childcare provision.
Remote working can lead to lower rates of absenteeism as remote workers may be able to continue to work from home if not needing to commute.	Remote workers can lead healthier and stress-free lives by having a better work-life balance.

Security risks associated with Remote Working

For the Organisation	For the Employee
<p>Direct supervision of remote workers is not possible: managers cannot physically observe their employees' performance. Providing timely, reliable and constructive feedback is more challenging for managers of remote workers. It may also take longer for performance issues to emerge and be discussed and dealt with.</p>	<p>Remote workers can become lonely, isolated or less effective. If they 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.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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. Overworking may increase the risk of home workers suffering from burnout.</p>

<p>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.</p>	<p>Organisations are increasingly introducing hot desking or shared hubs and decreasing corporate space. 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. 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.</p>
<p>Remote workers may live in shared accommodation with other people not employed by the organisation. Organisations will have little or no control over these environments. There is a risk that remote workers might inadvertently divulge commercially sensitive or operational information to family members or house-sharers. 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 and consider policies relating to the use of company IT equipment or working on company documents in the company of others.</p>	<p>Remote workers may feel anxious if they do not have the right space or privacy at home or in shared spaces to work securely and safely, especially on sensitive material. They may not have appropriate desk, chair, IT peripherals to support long term remote working and develop physical and mental health conditions related to this situation.</p>
<p>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.</p>	<p>Remote workers may not be able to quickly access on-site support systems such as welfare and occupational health professionals.</p>

Legislation

Legal obligations on the employer apply equally to remote workers as they do to employees in the workplace. Applicable legislation includes:

Data Protection Act 2018: concerns the processing and storage of personal information, irrespective of where this is carried out. Issues to consider include whether data is secured against theft, intrusion or from viewing by family members and visitors; whether staff have been adequately trained on the risks of remote working (e.g. secure password, appropriate use of corporate devices, the risk of malware); and/or whether the corporate system is secured to the necessary standards (e.g. system back-ups, use of VPNs, encryption standards).

Health and Safety at Work Act 1974: sets out the general duties of employers and imposes a positive obligation to ensure 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: impose limits on workers' hours of work and stipulate that workers should work no more than 48 hours per week unless they agree to opt out or do a job not covered by the Regulations. They also set out requirements for breaks from work and paid annual leave.⁴

Health and Safety (Display Screen Equipment) Regulations 1992 set out requirements for assessing workstations with display screen equipment and anyone, including remote workers, who uses computers on a regular basis, is entitled to an eye test paid for by their employer.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013: 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 1996: established the statutory right to request a contract variation, including a change to place of work. It sets out the employer's duty in relation to such an application and 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 intended to be exhaustive. CPNI strongly recommends that employers seek independent legal advice when implementing or updating their policies on remote working.

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

Key Per Sec considerations in Remote Working Policies

An organisation's remote working security policies should consider:

- whether any jobs or activities within an organisation are not permitted under remote 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, ie payment for the use of telephone, broadband, stationery, heating and lighting and travel expenses, either by the organisation or the employee and any tax liabilities.
- prohibited locations for remote working, including outside of the UK.
- attendance in the workplace, frequency of meetings with management and colleagues.

Welfare considerations for remote workers

For many people remote working is an enjoyable experience, but some people do report feelings of social isolation and disconnection with the organisation. Managers should be able to identify the signs and symptoms of employees with personal issues, in particular isolation or lack of contact with colleagues, by having regular one to one online meetings. 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. Remote workers should have access to an organisation's Welfare Support and Occupational Health Team.

Working hours should be monitored by both the remote worker and the manager to identify instances of under or over-working. Remote workers should be encouraged to 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. Managers should ensure that remote workers aware of the need to take regular breaks. 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 (eg 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 because they do not need to commute; 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.