Working from Home Policy Checklist

By Daniel Pollard - 16 October 2020

With many employees having worked from home for the past few months, employers are now reassessing the long-term feasibility of remote working. As homeworking was first adopted as an emergency measure out of necessity, not all of the implications were fully considered and we set out below a checklist of the issues to take into account.

Where employers encourage or permit homeworking, it is important to remember that their duties to provide a safe system of work and to safeguard third parties personal data and confidential information apply equally to employees who work remotely. The lack of uniformity in the facilities that employees have at home also presents practical difficulties.

Once employees no longer need to attend a place of work regularly it may be attractive for employees to relocate to or work from abroad or a significant distance from the office. However working overseas presents some unique challenges and risks to the employer.

As a firm, we have offered unlimited homeworking for a number of years as a part of the way that we have attracted and retained talented lawyers to our team. Based on that experience, we set out below some of the "soft" issues which are as important as, if not more important than, the legal issues.

Healthy and Safety

- [ ] Do employees have adequate facilities to work *safely* including a suitable desk, chair, monitor, keyboard and mouse which are suitable for all-day long-term use?

- [ ] Consider remote desk-based assessments and/or workstation training.

- [ ] Consider heightened psychological risks arising from remote working including how to maintain regulator contact, monitor workload and how to deal with the challenges of recognising stress in remote workers (see the Health & Safety Executive guidance here).

- [ ] Carry out risk assessments, update your health and safety policy statement and (if applicable) consult with health and safety representatives about homeworking arrangements.

Physical Security

- [ ] Do employees have adequate facilities to work securely?

- [ ] Do employees have a private workspace or is their workspace shared with housemates or family members? If so, how can the risks of inadvertent disclosure of confidential information be managed?

- [ ] Require lockable cupboard(s) for documents.

- [ ] Provide facilities to dispose of documents securely (i.e. shredder).

- [ ] Should you mandate a minimum standard of home security, encourage employees to complete a home security self-assessment or subject them to security audits?

- [ ] Consider prohibiting work from public places (such as cafes) especially where sensitive information may be viewed onscreen and there is a heightened risk of documents being lost.

Technology and Information Security

Even where employees work using the employer's devices which are fully encrypted and have appropriate security protocols, there are a number of issues to consider:

- [ ] Where possible laptops should be connected to the network with a cable (for both speed, resilience and security).

- [ ] If Wi-Fi is enabled in the home network, the wireless network should be protected using a WPA2 or WPA3 security mode. The Wi-Fi password should have at least 10 characters, a capital letter, lower case letter, number and a special character. The password should not be easy to guess (such as address or surname) and the wireless network name (SSID) should not include any personal information that makes it easy for people to identify the network.

- [ ] A modern router with routinely updated firmware must be used. The built-in firewall function on the router should be enabled, denying all external traffic by default.

- [ ] Default admin login details for home network devices (routers, Wi-Fi, network storage devices) should be changed to something complex and unique.

- [ ] Multi-factor authentication should be enabled on all company and personal cloud-based systems. It should also be enabled where VPN is used to connect to the company network.

- [ ] Consider technology that can leverage advanced office-based unified threat management (UTM) even while working remotely. Most businesses should have UTM through their office firewall, but this only protects employees whilst they are working in the office leaving them vulnerable to issues like zero-day threats (unknown malware or vulnerabilities) which are often not picked up by anti-malware software.

- [ ] Implement web filtering to protect users from malicious content wherever they work. Typically, office networks have web filtering in place through a virtual or physical appliance such as a firewall, but this only filters web traffic for employees whilst they are in the office.

- [ ] Consider prohibiting working on public Wi-Fi networks.

- [ ] Ensure members of the same household are aware of these data security best practices to help prevent home networks becoming compromised (for example, by someone who has improperly configured an inbound firewall policy for online gaming).

- [ ] Consider audit of home IT networks and arrangements.

Whilst the above recommendations comply with latest remote working security requirements from the National Cyber Security Centre's (NCSC) Cyber Essentials framework and would allow for ISO 27001 accreditation employers should also consider other vulnerabilities. For example, with the proliferation of devices attached to the home network (often dubbed the internet of things or "IoT") employers may also consider policies that seek to control risks arising from vulnerabilities introduced by such devices. In an ideal world, employers would provide a dedicated home broadband connection to eliminate this risk, although the risk/impact and cost of this measure means that this would be unusual. Other less invasive measures might include rules, recommendations or education around the risks introduced by such devices. The risks can be reduced if all home devices are produced or accredited by well-known trusted brands, are routinely updated (and disposed of if the manufacturer stops providing updates) and if usernames/passwords are changed from default settings. The risks associated with remote working are further mitigated for organisations that use VPN to route all traffic for remote workers through the secure office network.

The use of personally owned computer equipment should be prohibited unless the company has authorised it and implemented the same security standards on the device that are used on company devices as part of a proper BYOD program.

With thanks to Labyrinth Technology who can provide a full information security audit for your office or homeworking arrangements.

Expenses and Tax

- [ ] What is the company's policy on the provision of computer equipment and peripherals for home use?

- [ ] Until the end of the 2020-21 tax year, there is a temporary exemption from income tax and NICs for expenses reimbursed by an employer to an employee where the expenses are incurred on the purchase of equipment obtained for the "sole purpose" of enabling the employee to work from home due to COVID-19. For the reimbursement to be exempt, it must be the case that the provision of the equipment directly by the employer would have been exempt from income tax under the usual homeworking tax provisions.

- [ ] In cases where the employer does not reimburse the employee for the cost of office equipment, the employee may be able to claim an income tax deduction provided the expenditure is incurred "wholly, exclusively, and necessarily" in the performance of their employment duties.

- [ ] Employers can provide one mobile phone and SIM card to each employee, with no restriction on private use, without the phone, line rental, or call charges giving rise to a taxable benefit in kind. However, if employees arrange the phone and contract and

the employer reimburses the cost, this is likely to give rise to income tax and Class 1 NICs.

- [ ] Landline phone expenses may be exempt from tax if it can be demonstrated that the installation is only for business purposes (for example, a second line). In all other cases, tax and NICs may be due depending (broadly in the same way as for mobile phones) on how the service is arranged and paid for. The reimbursement of specific business calls on the employee's landline can, if correctly documented, be exempt from undesirable NICs treatment.

- [ ] Employers can also pay or reimburse certain additional costs incurred by employees who regularly work at home (for example, heating, lighting, water, increased charges for Internet access or home contents insurance). Up to £26 a month can be reimbursed without tax and NICs, including by way of a flat rate allowance.

- [ ] Employers occasionally reimburse substantial home office costs for senior staff, including in some cases paying part of the rent or mortgage on their property. Specific advice should be taken on substantial reimbursements, not only because income tax and NICs consequences are likely to follow but also because there is a risk of employees being exposed to business rates and losing part of the capital gains tax exemption on their main home.

Further advice on these issues can be obtained from our employment tax specialist Dan Pipe.

Housing Issues

- [ ] Home insurance providers should be notified of business use (clerical only) and any changes to the pattern of occupancy.

- [ ] Employees may wish to check the terms of their lease or mortgages to ensure that they are not in breach of their obligations (unlikely for clerical use).

Business Protection

- [ ] Where an employee does not have exclusive use of a private office consider imposing a duty to disclose potential conflicts of interest with other members of the household which may arise from inadvertent sharing of confidential information.

- [ ] Consider enhanced systems to detect and prevent misappropriation of confidential information. For example, disabling USB drives, data loss prevention tools, enabling audit logs (including for systems like Microsoft 365 where the audit log is not enabled by default) and reviewing audit logs to monitor access to commercially sensitive information. Where appropriate consider using advanced log management and analysis tools to centrally manage logs and automatically flag high risk activity. However increased monitoring should be balanced against the privacy issues discussed below.

- [ ] Revisit how confidential information is identified and protected within the business. Many employees do not appreciate that information is confidential and confidential information should be identified as such in confidentiality agreements and also with an appropriate header in the relevant documents. Access should also ideally be limited.

- [ ] Consider prohibiting the use of private communication systems (such as WhatsApp and personal text messages) between employees and third parties for work purposes to ensure that all work-related communications are retained in line with document retention policies.

- [ ] Consider prohibiting the recording of work-related conversations using private equipment without consent of both parties. This is already recommended but it is much easier to record telephone conversations covertly than in person conversations.

Working Time

- [ ] Consider whether you need to reassess normal working hours including whether measures are required to enforce "down time" and the policy on "errands" or childcare responsibilities during what would traditionally be seen as working time.

- [ ] Consider, for example, if employees should be asked to complete timesheets or if other technical solutions can be adopted to monitor output (but see below regarding privacy).

- [ ] Those with compulsory holiday policies may need to consider taking steps to enforce these policies for example with an IT lock out.

Super Remote Working

- [ ] Consider whether there should be a maximum distance from the office at which employees may reside, so employees are able to attend the place of work at short or reasonable notice. A time and distance requirement may be appropriate.

- [ ] Consider if there should be an express requirement to attend the office on request and any advance notice that may be required.

Employee Privacy

- [ ] Ensure that the use of monitoring applications or features are appropriately disclosed to employees facing fair processing notices. This does not just apply to employers who install applications specifically designed to monitor workplace behaviours (such as keystroke loggers, web browser monitoring, camera tracking, tracking, screenshot monitoring and the like) but also to features within standard business applications. Examples include Team's presence monitoring and Zoom's (recently withdrawn) attention tracking. But disclosure is not enough: monitoring must also be for a specific legitimate purpose, information processed must be minimised to achieve that purpose and the lawful basis documented – an impact assessment is prudent and likely to be required when adopting the most invasive tech. (Update: YouGov Polling conducted by Prospect (the Trade Union) found that 66% of workers would be uncomfortable with the use of keystroke monitoring and only 32% were even aware of these technologies).

- [ ] Where employers do use online tools to monitor productivity their use in the home rather than the workplace is likely to be far more invasive. This will require greater scrutiny, consultation and care in deployment.

- [ ] As employers seek to monitor employee's productivity we have started to see employees (especially the tech savvy) start to formulate what might be termed "defeat strategies". For examples of the weird and wonderful devices that can prevent Teams showing that you are away from your desk trying googling "mouse jiggler". Should your policies prevent the use of such devices?

Overseas Working

- [ ] Employees who base themselves overseas may expose their employers to local employment, immigration and health and safety laws. Employees are likely to be subject to local taxation and employers may also be subject to local tax withholding requirements. This means that local advice should always be sought. The cost of obtaining this advice and the additional administrative burden means that many employers choose to impose an outright ban on overseas working. Alternatively, employers may allow overseas working via professional employer organisations or may allow overseas working from designated countries.

- [ ] Employees may even be at risk of creating a taxable presence for their employer overseas and exposing it to corporate taxes in the other jurisdiction. Homeworking policies should contain guidance on how this can be avoided.

- [ ] Providing employees with access to your information systems from locations outside the UK (and especially also if outside the EU) may create data sovereignty issues which should be considered and may need to be addressed. Working outside the EU (or countries with an EU approved adequacy determination) is likely to be especially problematic.

- [ ] Pursuing employees for breach of confidentiality or non-compete obligations is likely to be significantly more complex and time consuming. Where key talent are based overseas, local law advice should be obtained from the outset especially if they are unlikely to return to the UK.

We have offices all over the world with employment lawyers qualified to practice in nearly all jurisdictions. Please contact your usual GQ|Littler lawyer for support.

Practicalities

Based on our experience the following principles emerged:

- **Choice** - Not all employees want to or are able to work from home. It is especially difficult for those who do not have a dedicated workspace.
- **Equipment** - Office quality IT is essential - that means dual monitors, office quality printers, full size keyboards, VOIP phones, fast broadband and the like.
- **Exercise** - Commuting to the office is often one of the main sources of daily exercise. If this is removed from the daily routine it is important to get out of the house on a daily basis and employers may wish to offer "healthy living" advice/sessions.
- **Team** - Some way of replicating watercooler moments, team dynamics and mentoring of work are vitally important.

The significant advantages of homeworking in terms of the reduction of real estate cost and commuting expenses also beg the question who should benefit from those savings? We have yet to see employers reduce salaries for those who do not face commuting costs or who are able to benefit from reduced living costs away from the main urban centres but we envisage that that these tensions will drive many of the disputes of tomorrow.

Homeworking may not be a long-term sustainable solution for some employers, teams and individuals. There is certainly some empirical evidence that early adopters of homeworking have rolled back on their approach. Employers should ideally adopt a formal homeworking policy to set out their approach to the issues set out above.

If you require assistance forumalting your homeworking policy please contact your usual GQ|Littler lawyer or get in touch with either Daniel Pollard or Dan Pipe.