# Staff working from home? How do you keep data secure?

Data protection law requires every business that deals with personal data to ensure that they have “Technical and Organisational Measures ” in place to keep that data secure. Losing that data could seriously damage the company’s reputation and potentially land it with a fine from the ICO and with claims for compensation.

14 April 2020

**Please note: the information contained in our legal updates are correct as of the original date of publication**

Data protection law requires every business that deals with personal data to ensure that they have “Technical and Organisational Measures ” in place to keep that data secure. In addition to personal data, business owners and employees are also likely to be dealing with data that is confidential (either relating to the business itself or to third parties).

Losing that data could seriously damage the company’s reputation and potentially land it with a fine from the ICO and with claims for compensation.

But with everyone working from home right now – how do you ensure that data is kept safe?

Here are a few points to bear in mind:

1. **If you don’t have a “Working from home” policy now might be the time to put one together.**

   **Why?** In the event of a data breach being investigated by the Information Commissioner’s Office (ICO), the ICO are likely to want to see the precautions that your business had in place to avoid and minimise the effects of that breach.

   As a business you want to have an answer to the question “What did you do to try to prevent this?” This policy should as a minimum deal with all of the points below and be required reading for all staff.

2. **Ensure data is regularly (and securely) backed up**

   Having regular back-ups should be part of any decent IT security policy – to mitigate the risk of a ransomware attack (where access to data is blocked and requires the use of a key (typically in return for payment a ransom) to recover it.

   **Why?** Regularly and securely backing up data means that the risk of an individual device or individual user being compromised is considerably reduced, since data can be recovered up to the point of the last back up.

   Where employees are working offline for any length of time it is worth reminding them that personal data needs to be kept secure and that an individual laptop’s own hard drive (or free storage such as Google Drive or Dropbox) is unlikely to have the same level of security.

3. **Software updates and patches**

   Of course you’re regularly installing the latest versions of your own business software, making sure that vulnerabilities are dealt with aren't you? This should be an integral part of any IT security policy – but is something to particularly consider when staff are working from home.

**Why?** Because unlike workers commuting to work on a regular basis, there is no requirement for someone working from home to switch off their computer at night. As far as you know it may still be whirring away in some back room, meaning the usual installation of updates to software may not be triggered. You need to ensure that these updates are installed.

4. **Agree communication channels with employees**

   Hopefully your workers have access to an email server controlled and secured by the business. In times like these however you might want to be clear about the channels employees should use to communicate.

   **Why?** Discussions between employees scattered to their various homes might well carry on across a multiplicity of platforms – from Zoom, Whatsapp, Google hangouts, Skype, Facebook Messenger and on apps like Houseparty or Dropbox. Some of these apps have well- known security flaws and can be easily hacked or discovered by those outside the company.

   Communicating in advance the software that is acceptable can help avoid sensitive data from being exposed.

5. **Have a way of dealing with suspected Phishing emails**

   Having a policy agreed in advance means that employees are less likely to be susceptible to emails that appear to be from the boss, or which request financial or other information.

   **Why?** Any good policy should give a point of contact to whom suspicious emails can be sent and verified. If your staff receive an email that appears to have a suspicious link then a central point of contact (who has the tools to check the email in a secure, isolated environment) can considerably reduce the cost of having to deal with the consequences.

6. **Other people in the household**

   We all remember the BBC News interview where the interviewee's young children bounded into shot to great comic effect (in stark contrast to the serious nature of the discussion). Children, partners and other people will be around the house and no one can seriously object to their occasional interruption – but what about discussions about particularly sensitive or confidential information? These should also be covered in your policy.

   **Why?** Clients and employees are likely to expect and deserve confidentiality to be maintained, including from other members of a household. Discussions about sensitive or involving confidential information should be afforded the same level of privacy that would be maintained in an office – so if a discussion would typically involve you leaving an open plan environment for a discussion (e.g. performance reviews, confidential new projects, discussion of a client's personal circumstances) then common sense would suggest leaving the room that you're sharing with other members of your family.

Ultimately these points might seem like (and are) little more than common sense, however in the imposed informality of working from home some of the normal precautions around security can be missed. It is therefore critical that every business remains vigilant to the risks of a lack of security and takes appropriate measures to keep data secure. Taking the steps above, capturing them in a policy and ensuring that all employees are aware of that policy are sensible steps to (hopefully) avoid a data breach or (at worst) minimise the consequences of a breach.

# Contact

## Richard Nicholas

Partner

richard.nicholas@brownejacobson.com

+44 (0)121 237 3992

## Related expertise

Data protection and privacy