

COVID-19 Legal Response Team

Our lawyers are working across the UK alongside BPA members and authorities to provide regular updates and assistance through this period of uncertainty.

Most if not all businesses will not or cannot have planned for what we are experiencing. The key to any business is to get timely and meaningful advice.

At JMW, BPA Lawline have a team of senior lawyers who are on hand to provide advice and assistance to you or any of your clients.

- **struggling to meet contractual obligations or understanding your rights under certain contracts;**
- **employers obligations and questions in relation to employees;**
- **privacy and data protection;**
- **property;**
- **insolvency;**
- **dispute resolution;**
- **competition and EU law;**
- **funding/cash flow;**
- **regulatory compliance;**
- **issues in relation to IP;**
- **understanding the help available from the government and whether or not the business qualifies.**

We advise clients across a wide range of sectors.

We have now launched a dedicated COVID-19 resource hub on our website. It contains numerous blogs and articles from a range of our departments, which all businesses will benefit from reading.

A number of our departments are now also producing downloadable updates, which can also be sourced from the hub.

The hub can be found at

www.jmw.co.uk/covid-19-hub

You can also contact

**Derek Millard-Smith and the
BPA Lawline team directly on:
0345 241 3024, bpa@jmw.co.uk**

Across all our departments and teams we are able to offer 'virtual meetings' via video conferencing software.

Tips On Safe Remote Working



Only use work approved PCs & laptops. If you connect via Citrix or VPN ensure your device has the latest anti-virus software and firewall.



Minimise printing and dispose of material carefully preferably shredding it (using a P4 shredder or the office confidential waste bins).



Inform the police and your IT department asap if your laptop, mobile phone or any storage device etc. is lost or stolen.



Avoid removable media (USB sticks or CDs), public computers or public WIFI (e.g. coffee shops) and use a privacy screen.



Do not use social media, personal email accounts, e.g. Yahoo, Gmail or Hotmail & cloud storage, e.g. Dropbox, iCloud, OneDrive or local drives for work data.



Change your home WIFI password often (every 60 days) and avoid default passwords set by network providers – use guest accounts for visitors.



Switch off smart speakers, smart TVs and mobile apps such as Siri and avoid discussing confidential matters where you can be



Lock your device when you are away from it (hold windows key and press 'L').



When using video conferencing such as Zoom or Skype change default settings to improve security (e.g. require passwords).