**Bring Your Own Device (BYOD) Policy**

**About this policy**

We recognise that staff could use their personal mobile devices (such as tablets, smartphones and handheld computers) for business purposes. There can be benefits for both us and staff in permitting such use, but it also gives rise to increased risk in terms of the security of our IT resources and communications systems, the protection of confidential and proprietary information and reputation, and compliance with legal obligations.
The purpose of this policy is to set out our rules on the use of personal devices in order to:

- protect our systems and company data;
- prevent company data from being deliberately or inadvertently lost, disclosed or altered;
- set out the circumstances in which we may monitor your use of our systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy; More information about how we monitor, record and process your personal data is contained in our separate Privacy notice and Data Protection Policy.
- encourage our staff to consider carefully how and when you use your device, and maintain an effective balance between work and personal life.

Certain obligations under this policy are contractual and will form part of your contract of employment. These are clearly identified. The remaining sections of this policy do not form part of any contract of employment or other contract to provide services and we may amend it (including the contractual obligations that it places on staff) or remove the policy entirely, at any time.

**Who does this policy apply to?**

This policy covers all employees, officers, consultants, contractors, interns, casual workers and agency workers.

**Who is responsible for this policy?**

The Managing Director is responsible for this policy. Any questions you may have about the day-to-day application of this policy should be referred to your line manager in the first instance.
This policy is reviewed annually by the Managing Director.

**Scope of the policy**

This policy applies to any use by staff of a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) for business purposes. It applies to use of the device both during and outside office hours and whether or not use of the device takes place at your normal place of work.
This policy applies to all devices used to access our IT resources and communications systems (collectively referred to as **systems** in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, tablets, and laptop or notebook computers.
Anyone covered by this policy may use an approved personal mobile device for business purposes, provided that they sign the declaration at the end of this policy and adhere to its terms.
No one is required to use their personal mobile device for business purposes. It is a matter entirely for each person's discretion. We have chosen to implement this policy as we recognise that using personal mobile devices for business purposes can offer increased flexibility and autonomy for our staff. However, we also encourage our staff to consider carefully how and when you use your device, and maintain an effective balance between work and personal life.
This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our IT and communications systems policy, Privacy Notice and other IT related policies, which are available on the intranet**.**
When you access our systems you may be able to access data about us including information which is confidential, proprietary or private. The definition of data is very broad, and includes all written, spoken and electronic information held, used or transmitted by us or on our behalf, in whatever form (collectively referred to as **company data** in this policy).
When you access our systems using a device, we are exposed to a number of risks, including the loss or theft of the device (which could result in unauthorised access to our systems or company data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of company data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our systems, our business and our reputation.
Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal or, in the case of a breach of this policy by a contractor, consultant, casual or agency worker, the termination of the engagement. Disciplinary action may be taken whether the breach is committed during or outside office hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into

suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.
Some devices may not have the capability to connect to our systems. We are not under any obligation to modify our systems or otherwise assist staff in connecting to our systems.

**Monitoring**

The contents of our systems and company data are our property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as **content** in this policy) during the course of business or on our behalf is our property, regardless of who owns the device.
We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device [as well as keystroke capturing and other network monitoring technologies], whether or not the device is in your possession.
It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore you should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential. If you use your device to process personal data about third parties (for example your family and friends) you should be aware that this may be inadvertently monitored, intercepted, reviewed or erased. You should ensure that any third parties are aware that their personal data may be inadvertently monitored.
Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law in order for us to comply with a legal obligation or for our legitimate business purposes, including, without limitation, in order to:

- prevent misuse of the device and protect company data;
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);
- monitor performance at work; and
- ensure that staff members do not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.
You acknowledge that the company is entitled to conduct such monitoring where it has a legitimate basis to do so, and you confirm your agreement (without further notice or permission) to our right to copy, erase or remotely wipe the entire device (including any personal data stored on the device). You also agree that you use the device at your own risk

and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

**Security requirements**

You must comply with our IT Communications Systems Policy which is available from the intranet when using your device to connect to our systems.
In addition, you must:

- at all times, use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. You must secure the device whether or not it is in use and whether or not it is being carried by you. This includes, but is not limited to, passwords, encryption, and physical control of the device;
- protect the device with a PIN number or strong password, and keep that PIN number or password secure at all times. The PIN number or password should be changed regularly. If the confidentiality of a PIN number or password is compromised, you must change it immediately. The use of PIN numbers and passwords should not create an expectation of privacy by you in the device;
- not use a device to capture images, video, or audio, whether native to the device or through third-party applications, within the workplace;
- Not sell, replace or transfer the device to anyone else without our prior consent.

We reserve the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the company data on it for legitimate business purposes, which include (without limitation) enabling us to:

- inspect the device for use of unauthorised applications or software;
- inspect any company data stored on the device or on backup or cloud-based storage applications and prevent misuse of the device and protect company data;
- investigate or resolve any security incident or unauthorised use of our systems;
- conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).

You must co-operate with us to enable such inspection, access and review, including providing any passwords or PIN numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken, up to and including dismissal.
If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we shall immediately remove access to our systems

and, where appropriate, remove any company data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from company data in all circumstances. You should therefore regularly backup any personal data contained on the device.
You consent to us, without further notice or permission, inspecting a device and applications used on it, and remotely reviewing, copying, disclosing, wiping or otherwise using some or all of the data on or from a device for the legitimate business purposes set out above.

**Lost or stolen devices and unauthorised access**

In the event of a lost or stolen device, or where a staff member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to their line manager immediately.

**Personal data**

We have a legitimate basis on which to access and protect company data stored or processed on your device, including the content of any communications sent or received from the device. However, we recognise the need to balance our obligation to process data for legitimate purposes, with your expectations of privacy in respect of your personal data. Therefore, when taking (or considering taking) action to access your device or delete data on your device (remotely or otherwise) in accordance with this policy, we will, where practicable:

- consider whether the action is proportionate in light of the potential damage to the company, our customers or other people impacted by company data;
- consider if there is an alternative method of dealing with the potential risks to the company's interests (recognising that such decisions often require urgent action);
- take reasonable steps to minimise loss of your personal data on your device, although we shall not be responsible for any such loss that may occur; and
- delete any such personal data that has been copied as soon as it comes to our attention (provided it is not personal data which is also company data, including all personal emails sent or received using our email system).

To reduce the likelihood of the company inadvertently accessing your personal data, or the personal data of third parties, you must comply with the following steps to separate company data from your personal data on the device:

- organise files within the device specifically into designated folders that clearly distinguish between company data and personal data (for example, marking your own folders as "PERSONAL");
- do not use work e-mail for personal purposes, but if you do ensure that it is labelled appropriately in the subject line;

- keep the amount of third party personal data (e.g. in relation to family and friends) stored on the device to a minimum;
- regularly backup all personal data stored on the device.

**Appropriate use**

You must be aware of our and your obligations under the relevant data protection legislation when processing company data. You must ensure that company data is used only for the business purposes for which it was intended, and that you do not use it for a purpose different from that for which it was originally intended. For example, you should not use contact information gathered for business purposes for your own personal purposes. You should also minimise the amount of company data you retain on the device by accessing information remotely where possible, and deleting any data saved locally on your device as soon as it is no longer required. Your obligations as a processor of personal data are explained in more detail in our Data protection policy.

You should never access or use our systems or company data through a device in a way that breaches any of our other policies. For example, you must not use a device to:

- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations that relevant regulatory bodies may have relating to confidentiality and privacy
- breach our Disciplinary Rules;
- defame or criticise us or our affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;
- harass or bully other staff in any way**;**
- unlawfully discriminate against other staff or third parties**;**
- breach our Data protection policy;
- breach any other laws or ethical standards (for example, by breaching copyright or licensing restrictions by unlawfully downloading software on to a device).

If you breach any of the above policies you may be subject to disciplinary action up to and including dismissal.

You must not talk, text, e-mail or otherwise use a device while operating a company vehicle or while operating a personal vehicle for business purposes. You must comply with any applicable law concerning the use of devices in vehicles. For your own safety and the safety of others, we recommend you should not use your device while operating vehicles of any kind.

**Technical support**

We do not provide technical support for devices.

**Costs and reimbursements**

You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs. By signing the declaration at the end of this policy you acknowledge that you alone are responsible for all costs associated with the device and that you understand that your business usage of the device may increase your voice and data usage charges.