GLAISYERS ETL GLOBAL

BRING YOUR OWN DEVICE TO WORK (BYOD) POLICY

Document Name	Bring your own device policy
Current Version	1.0
Plan Owner	Sean Edwards or Risk Committee
Plan Approver	Risk Committee
Date of Last Review	July 14th 2024

1. About this policy

1.1 We recognise that colleagues would either like or may need to use their personal mobile devices (such as tablets, smartphones and handheld computers) for business purposes. There can be benefits for both the business and our colleagues 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 and regulatory obligations.

1.2 The purpose of this policy is to set out our rules on the use of personal devices in the workplace and as part of your duties in order to:

(a) protect our systems and business and client data;

(b) prevent business and client data from being deliberately or inadvertently lost, disclosed or altered;

(c) 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.

(d) encourage our colleagues to consider carefully how and when you use your device, and maintain an effective balance between work and personal life.

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

2. Who does this policy apply to?

2.1 This policy covers all employees, officers, consultants, contractors, volunteers, interns, vacation students, casual workers and agency workers.

3. Who is responsible for this policy?

3.1 The Risk Committee has overall responsibility for the effective operation of this policy, and has delegated responsibility for overseeing its implementation to Sean Edwards, the Projects & Business Solutions Manager. Questions about the content of this policy or suggestions for change should be reported to the Projects & Business Solutions Manager.

3.2 Any questions you may have about the day-to-day application of this policy should be referred to the Projects & Business Solutions Manager in the first instance.

3.3 This policy is reviewed annually by the Risk Committee in conjunction with the Projects & Business Solutions Manager.

4. Scope of the policy

4.1 This policy applies to any use by colleagues 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.

4.2 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.

4.3 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 and comply with any further requirements or conditions relating to such use (including, where requested, downloading software and/or VPN or other profiles) which we may introduce from time to time.

4.4 No one is required to use their personal mobile device for business purposes and whether they choose to do so is a matter entirely for each colleague'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 colleagues. However, we also encourage our colleagues to consider carefully how and when you use your device, and maintain an effective balance between work and personal life

4.5 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 Computer Protection Policy, Data Protection Policy, and other IT related policies, which are available in the Staff Handbook or via the Intranet.

4.6 When you access our systems you may be able to access data about us or other ETL Group member, our clients, referrers, suppliers (including, without limitation, Counsel) and other business connections, including information which is confidential, proprietary or private in nature. 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 business and client data in this policy) to ensure that it aligns and complies with applicable data protection, privacy and cybersecurity regulation and best practice.

4.7 When you access our systems using any 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 business and client data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via any device) and the loss or unauthorised alteration of business and client 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 and lead to both civil claims and regulatory action being taken by the Solicitors Regulation Authority.

4.8 Any breach of this policy may lead to us revoking your access to our systems, whether through any 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 vacation student contractor, consultant, casual or agency worker, the termination of their further engagement with us. 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.

4.9 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 colleagues in connecting to our systems.

5. Connecting devices to our systems

5.1 Connectivity of all devices is centrally managed by the Projects & Business Solutions Manager and the IT Department, who must approve any device before it can be connected to our systems. Devices must comply with our Computer Protection Policy. Devices must be on the approved list of devices, available from the Projects & Business Solutions Manager or ETL IT. You may apply for any device to be added to the approved list by submitting it to the Projects & Business Solutions Manager who will have full discretion to approve or reject the device.

5.2 Before using your device to connect to our systems, or to access business and client data, in accordance with this policy, you must:

(a) register your device with the Projects & Business Solutions Manager or ETL IT; and

(b) present your device to the Projects & Business Solutions Manager or ETL IT for approval and configuration; and

(c) implement such technical security measures as the Projects & Business Solutions Manager or ETL IT may reasonably require, including ensuring the device is up to date in terms of its supported software lifecycle for example.

5.3 You are not permitted to use any device to connect to our systems other than the device that has been registered and approved by us. We reserve the right to refuse or remove permission for your device to connect at any time and for any reason, or (and may take all steps reasonably necessary to do so) where in our reasonable opinion any device is being or could be used in a way that puts, or could put, us, our colleagues, our business connections, our systems, or our business and client data at risk or that may otherwise breach this policy.

5.4 In order to access our systems, it may be necessary for the Projects & Business Solutions Manager or ETL IT to install software applications on your device. If you remove any such software, your access to our systems will be disabled.

6. Monitoring

6.1 The contents of our systems and business and client data are our property or the property of our clients. All materials, data, communications and information, including but not limited to email (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 any device (collectively referred to as content in this policy) during the course of business or on our behalf is our or our clients' property, regardless of who owns the device.

6.2 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 or on behalf of our clients. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, 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.

6.3 It is possible that your personal data may be inadvertently monitored, intercepted, reviewed or erased after you connect your device to our systems. Therefore, you should have no expectation of privacy in any data or content on the device. Colleagues 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 other than our clients are aware that their personal data may be inadvertently monitored.

6.4 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:

(a) prevent misuse of the device and protect business and client data;

(b) ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);

(c) monitor performance at work; and

(d) ensure that colleagues do not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

6.5 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 the purposes litigation or investigations (whether internal or external).

6.6 By signing the declaration at the end of this policy, you acknowledge that we are entitled to conduct such monitoring where we have 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) which you connect to our systems. You also agree that you use the device and connect it to our systems 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.

7. Security requirements

7.1 In addition, you must:

(a) 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, biometric security measures (such as FaceID) encryption, and physical control of the device;

(b) install any anti-virus or anti-malware software at our request before connecting to our systems and consent to our efforts to manage the device and secure its data, including providing us with any necessary passwords;

(c) comply with our device configuration requirements;

(d) 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 any expectation of privacy by you in the device;

(e) maintain the device's original operating system and keep it current with security patches and updates. Rooted (Android) or jailbroken (iOS) devices are forbidden from accessing our systems or business or client data;

(f) not download and install software to the device unless explicitly authorised by us. A list of applications that are already authorised and those that are expressly forbidden is available from the Projects & Business Solutions Manager or IT Department;

(g) not alter the security settings of the device without our consent

(h) prohibit use of the device by anyone not authorised by us, including your family, friends and contacts;

(i) not download or transfer any business and client data to the device, for example via email attachments, unless specifically authorised to do so. Colleagues must immediately erase any such information that is inadvertently downloaded to the device;

(j) not backup the device locally or to cloud-based storage or services where that might result in the backup or storage of business and client data. Any such backups inadvertently created must be deleted immediately;

(k) not use any device to capture images, video, or audio, whether native to the device or through third-party applications, within the workplace

(l) where we have permitted you to store business or client data on the device, ensure that any business or client data is encrypted using appropriate encryption technologies approved by the Projects & Business Solutions Manager or IT department.

(m) not use the device as a mobile hot-spot without our prior consent.

(n) not use public unsecured Wi-Fi to access our systems without our prior consent.

(o) Not sell, replace or transfer the device to anyone else without our prior consent.

7.2 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 business and client data on it for legitimate business purposes, which include (without limitation) enabling us to:

(a) inspect the device for use of unauthorised applications or software;

(b) inspect any business and client data stored on the device or on backup or cloud-based storage applications and prevent misuse of the device and protect business and client data;

(c) investigate or resolve any security incident or unauthorised use of our systems;

(d) conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and

(e) 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. **This paragraph 7.3 of the policy is contractual.**

7.3 If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we will immediately remove access to our systems and, where appropriate and available, remove any business and client data from the device. Although we do not intend to wipe other data or content that is personal in nature (such as photographs or personal files or emails), it may not be possible to distinguish all such information from business and client data in all circumstances. You should therefore regularly backup any personal data or content contained on the device.

7.4 By signing the declaration at the end of this policy, you consent to us, without further notice or permission, inspecting any device and applications used on it, and remotely reviewing, copying, disclosing, wiping or otherwise using some or all of the data on or from any device for the legitimate business purposes set out above.

8. Lost or stolen devices and unauthorised access

8.1 In the event of a lost or stolen device, or where a colleague believes that any device may have been accessed by an unauthorised person or otherwise compromised, the colleague must report the incident to the Project & Business Solutions Manager immediately.

8.2 Appropriate steps will be taken to ensure that business and client data on or accessible from the device is secured, including remote wiping of the device where appropriate and available. The remote wipe will destroy all business and client data on the device (including information contained in a work email account, even if such emails are personal in nature). Although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or emails), it may not be possible to distinguish all such information from business and client data in all circumstances. You should therefore regularly backup all personal data stored on the device.

9. Procedure on termination of employment and selling, transferrring or replacing the device.

On your last day of work, or your last day before commencing a period of garden leave, or when you intend to sell or transfer your device to anyone else, or to sell it, all business and client data (including work emails), and any software applications provided by us for business purposes, will be removed from the device, using software applied by the Project & Business Solutions Manager or the IT Department. If this cannot be achieved remotely, the device must be submitted to the Project & Business Solutions Manager or ETL IT for wiping and software removal. You must provide all necessary co-operation and assistance to the Project & Business Services Manager or ETL IT in relation to this process. This paragraph 9 of the policy is contractual.

10. Personal data

10.1 We have a legitimate basis on which to access and protect business and client 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:

(a) consider whether the action is proportionate in light of the potential damage to the business, our customers or other people impacted by business and client data;

(b) consider if there is an alternative method of dealing with the potential risks to the business's interests (recognising that such decisions often require urgent action);

(c) take reasonable steps to minimise loss of your personal data on your device, although we will not be responsible for any such loss that may occur; and

(d) 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 business and client data, including all personal emails sent or received using our email system).

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

(a) organise files within the device specifically into designated folders that clearly distinguish between business and client data and personal data (for example, marking your own folders as "PERSONAL");

(b) do not use work email for personal purposes

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

(d) regularly backup all personal data stored on the device.

11. Appropriate use

11.1 You must be aware of our and your obligations under the relevant data protection legislation when processing business and client data. You must ensure that business and client 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 business and client 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.

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

(a) breach our obligations with respect to the rules of relevant regulatory bodies;

(b) breach any obligations that relevant regulatory bodies may have relating to confidentiality and privacy;

(c) breach our Disciplinary Rules;

(d) defame or criticise us or our affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;

(e) harass or bully other colleagues in any way

(f) unlawfully discriminate against other colleagues or third parties

(g) breach our Data Protection Policy;

(h) [breach any other laws or ethical standards (for example, by breaching copyright or licensing restrictions by unlawfully downloading software on to any device).

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

11.4 You must not talk, text, email or otherwise use any device while operating a business 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.

11.5 Before using your device under this policy for the first time you must erase all information and software related to any previous employment. You must confirm to us that this has been done if asked to do so.

12. Technical support

The Projects & Business Solutions Manager or ETL IT will provide initial support to assist in determining if an issue with the device is software or hardware related. If the issue is hardware related or relates to software which you have installed, then you will be responsible for resolving it, including any repairs, maintenance or replacements costs and services. If it relates to software we have provided, then we will provide any necessary support.

13. 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 unless otherwise agreed in writing with the business. 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.

Declaration and Agreement

I ..... wish to use my personal mobile device for business purposes and explicitly confirm my understanding and agreement to the following:

- I have read, understood and agree to all of the terms contained in the Bring Your Own Device to Work Policy.

- I understand that the terms of this policy will always apply to me, during or outside office hours and whether or not I am at my normal place of work.

- I acknowledge and agree that authorised personnel of Glaisyers ETL will have the rights set out in this policy, including but not limited to the right to access, monitor, review, record and wipe (as the case may be) data contained on my personal device (which I acknowledge may result in inadvertent access to or destruction of my personal data).

- I understand and agree that Glaisyers ETL in its discretion may amend, or remove this policy at any time and that I will be bound by the terms of the policy as amended.

SIGNED .....

PRINTED NAME .....

DATE .....

GLAISYERS ETL GLOBAL

Manchester Office:
3 Hardman Street
Manchester M3 3HF
T: 0161 832 4666

Liverpool Office:
The Plaza
100 Old Hall St
Liverpool L3 9QJ
T: 0151 332 3555

hello@glaisyers.com
www.glaisyers.com