USE OF IT EQUIPMENT, INFORMATION SYSTEMS AND DATA POLICY

TABLE OF CONTENTS

1. POLICY STATEMENT

1.1 Our IT Equipment and Information Systems are intended to promote effective communication and safe and secure working practices within our organisation. This policy outlines the standards you must observe when using them, and in particular when dealing with Confidential Information and Personal Data.

1.2 We also explain acceptable use of personal IT Equipment, including mobile phones, and personal use of Information Systems, including use of the internet, both at work and elsewhere, when that use may have an impact on our business operations or reputation.

1.3 Use of Social Media is dealt with separately in our Social Media Policy.

1.4 This policy also outlines:

a) acceptable standards of communication in writing and in video meetings,

b) the circumstances in which we will monitor use, and

c) the action we will take in respect of breaches of these standards.

1.5 We also have a commitment to ensuring that Personal Data is processed in line with UK GDPR and relevant UK law and that all members of staff, and people who have access to Personal Data, conduct themselves in line with this and other related policies. We have strict obligations to process Personal Data securely and to adopt sufficient procedural and technological safeguards.

1.6 This policy does not form part of any employee's contract of employment and may be amended at any time. We may also vary this policy, including any time limits, as appropriate in any case.

2. WHO IS COVERED BY THE POLICY?

2.1 This policy covers all employees, directors and other officers, workers and agency workers, volunteers and interns.

2.2 We also require in any contracts with third parties who have access to our IT Equipment and Information Systems, such as consultants, contractors or suppliers, that they comply with this policy. We will ensure they are given access to a copy.

2.3 All individuals covered in sections 2.1 and 2.2 are referred to as 'staff' in this policy.

3. THE SCOPE OF THE POLICY

3.1 This policy applies to your use of:

a) **IT Equipment**, meaning any hardware, including all computers, laptops, other mobile devices, USB flashdrives, telephones, (including android and smartphones), fax machines, copiers, scanners, CCTV, and electronic key fobs and cards.

b) **Information Systems**, meaning anything we use to store, process or communicate any information or data, including the internet, Wi-Fi systems, email, telephone, voicemail and any cloud-based systems or other networks.

c) **Personal Data**, meaning any personal information about an individual,

where the individual can be identified, whether directly or indirectly if combined with other information.

d) **Confidential Information**, meaning information that is marked as confidential or information that you are required to keep confidential under your contract of employment or in any third-party agreements with us. This includes Personal Data, and in particular any sensitive Special Category Data under data protection laws.

3.2 We have a separate Social Media Policy which you should also read and understand.

4. WHO IS RESPONSIBLE FOR THIS POLICY?

4.1 While we ask all managers to take responsibility for making sure this policy is complied with, its successful operation also depends on you. Please take the time to read and understand it, and to go back to your manager with any questions you may have. References to Directors in this policy mean the most senior people within our organisation.

4.2 If you feel you need training or guidance on any of the elements of this policy, or on any related instructions or guidance we give you, it is your responsibility to speak to your manager.

5. IT EQUIPMENT SECURITY RULES

5.1 You are responsible for the security of the IT Equipment allocated to or used by you for work. To do that effectively you will need to comply with the rules in this section.

5.2 You should always do the following:

a) use passwords, and any other security measures required by us, on all IT Equipment in accordance with section 12 below,

b) set all IT Equipment to ‘sleep’ after a short period of non-use, or log off when leaving it unattended, to prevent unauthorised users accessing our Information Systems in your absence,

c) only move static IT Equipment or any of its cabling if you have prior approval from your manager,

d) keep any mobile IT Equipment secure when travelling or working remotely, for example, by not leaving it unattended in vehicles or public places,

e) make sure that any IT Equipment used away from our premises is used securely so that no Confidential Information or Personal Data can be seen by unauthorised people, such as passengers on public transport or other household members if working from home, and

f) let us know immediately if any IT Equipment is lost or stolen.

5.3 You must ensure that you:

a) do not allow your IT Equipment to be used by anyone else, except as allowed under this policy,

b) do not allow anyone not authorised to access our Information Systems to use IT Equipment except under supervision,

c) do not allow anyone not authorised to access our Information Systems to use our internal Wi-Fi system (they can instead access our external or

guest Wi-Fi system),

d) do not use portable storage devices, such as USB flashdrives, UNLESS there is an exceptional temporary reason for which your manager has given you prior approval, and you agree to:

e) encrypt and password protect any Personal Data and Confidential Information, and

f) delete any files as soon as you no longer need to store them there, and

g) do not attach or connect remotely any external device or equipment to our Information Systems, including any USB flashdrive, MP3, tablet or smartphone or other similar device whether connected via bluetooth, USB port, infra-red connection port, Wi-Fi or in any other way. (There may be exceptions to this, but only ever with the prior approval of your manager).

6. RULES ON USING PERSONAL IT EQUIPMENT FOR WORK (BYOD)

6.1 This section covers our rules on using personal IT Equipment or Bring Your Own Device (BYOD) for work purposes. Personal use of mobile phones and tablets or other devices is dealt with under section 7 below.

6.2 You can only access our Information Systems via your smartphones, other mobile devices or home computers for work purposes with prior written approval from your manager, which will be regularly reviewed. We are unlikely to agree to the viewing or processing of Personal Data or Confidential Information, unless as an agreed part of any hybrid working arrangements.

6.3 Any approval will be given on the basis that you agree to the following conditions:

a) you will delete any files containing Personal Data or Confidential Information as soon as you no longer need to have them there,

b) you will install appropriate security and anti-malware software,

c) you will comply with all other provisions of this policy in relation to the viewing or processing of any Personal Data or Confidential information set out in section 11 below,

d) you will give us access to your personal IT Equipment in the event of any security issues arising,

e) we can monitor your personal IT Equipment, and

f) we can wipe data from your IT Equipment in certain high-risk situations.

6.4 your manager may also require you to encrypt any files containing Personal Data or Confidential Information stored on your own device or sent over the internet or other network, where it is considered necessary for security.

6.5 In the event that we need access to your personal IT Equipment, we will not actively seek to access any personal files, but eliminating identified security issues may result in such access. If you are concerned about this, we recommend that you do not use personal IT Equipment for work.

6.6 Always back up any work you do on your personal IT Equipment onto our Information Systems as soon as possible, and as directed by your manager.

6.7 If you intend to lend, sell or give away your personal IT Equipment, and there is any risk that the recipient could gain access to the work you were doing on it

for us, please inform your manager before doing so. We will then assess the risk involved, and may require you to wipe its data in high-risk situations.

6.8 If you are using personal IT Equipment for work, the responsibility for its upkeep and any liability for its use remain yours.

7. PERSONAL USE OF PERSONAL IT EQUIPMENT SUCH AS MOBILE PHONES DURING WORKING HOURS OR AT OUR PREMISES.

7.1 We permit the incidental use of personal mobile phones for sending personal messages or making personal calls subject to the conditions set out in this section.

7.2 Personal use of mobile phones is a privilege and not a right. We reserve the right to withdraw permission or restrict access if you abuse this privilege.

7.3 The following conditions must be met for personal use to continue:

a) use must be minimal and take place substantially outside normal working hours (that is, during break times, before or after work),

b) use must not interfere with business or operational commitments, and in particular mobile phone notifications should be silenced during working hours,

c) use must not commit us to any extra costs, and

d) personal use must comply with this policy and our other related policies, including our Social Media Policy, and our policies on equality and diversity, anti-harassment and bullying, and data protection.

7.4 For details of acceptable internet use, please refer to section 9 below.

8. INFORMATION SYSTEMS SECURITY RULES

8.1 All staff should access and use our Information Systems responsibly and in a safe and secure way, whether on our work premises or elsewhere. To do that effectively you will need to comply with the rules in this section.

8.2 You should always do the following:

a) use passwords, and any other security measures required by us, to access all Information Systems, in accordance with section 12 below,

b) carry out a virus and malware check before downloading any incoming files and data, and if in any doubt about how to do this, please ask your manager,

c) exercise particular caution when opening unsolicited emails from unknown sources because of the malware risk,

d) tell your manager immediately if you suspect your IT Equipment may have a malware problem, and

e) only attempt to gain access to areas of our Information Systems that you have been authorised to access.

8.3 You must ensure that you:

a) never delete, destroy or modify existing systems, programs, information or data that could have the effect of harming our business or operations, or exposing us to risk, and

b) never download or install any software from external sources, including instant messaging, screensavers, photos, video clips and music files, without prior authorisation from a Director.

8.4 We monitor all emails passing through our Information Systems for malware problems. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

8.5 Employees should not use personal email or instant messenger accounts to send or receive email, or any Personal Data or Confidential Information, for the purposes of our business. Only use the email account we have provided for you. Use of personal email accounts by staff other than employees will be covered by their contractual arrangements with us, where we will require normal business precautions as a minimum.

9. ACCEPTABLE INTERNET USE

9.1 We need to ensure that any use of the internet involving our IT Equipment or our Information Systems is done in a way that minimises the risk of any harm to our staff, our visitors, our customers or our reputation, and which protects the security of our Personal Data and Confidential Information.

9.2 Internet use is therefore restricted in the ways described in this section, and there are different rules for work and personal internet use. This section does not cover the use of social media, which is covered separately in our Social Media Policy.

9.3 **Internet use for work purposes**: You may use the internet for work reasons, using our IT Equipment, personal IT Equipment you have been authorised to use for work purposes, and using any of our Information Systems, subject to the following conditions:

a) you must not create, view, access, transmit or download any prohibited material, which means any material which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral, or material on websites where cookies, tags or other markers from those websites could cause us embarrassment, including:

b) pornographic or similarly offensive, obscene or criminal material,

c) a false and defamatory statement about any person or organisation,

d) material that is discriminatory, offensive, derogatory or may cause embarrassment to others (including material that breaches our policy on equality and diversity, or our Anti-harassment and Bullying Policy),

e) Confidential Information, except as authorised in the proper performance of your role,

f) any statement that is likely to create any criminal or civil liability (for you or us),

g) music or video files or other material in breach of copyright, and

h) any material from the Dark Web or accessed using the 'Tor' internet browser.

9.4 **Personal internet use:** We ask you to limit your access to the internet for personal use to your non-working times only, when it will not interfere with your work. Access to the internet at these times is a privilege not a right, and we reserve the right to withdraw permission or restrict access if you abuse this

privilege. Personal internet use is also subject to the following conditions.

a) You must not do anything that would breach the other provisions of this section or this policy, our Social Media Policy, or our other policies on data protection, equality and diversity, or anti-harassment and bullying.

b) You must never access the Dark Web or use the 'Tor' internet browser.

c) You may access the internet on your own IT Equipment without making use of any of our Information Systems, such as our Wi-Fi.

d) If you wish to access the internet for personal use using our IT Equipment or via any of our Information Systems, then you must never use our internet, internal or external Wi-Fi to download or stream music, other audio, films or other video, as this may affect the quality and speed of our internet use for work purposes.

e) Accessing the internet using our IT Equipment or via our Information Systems may be subject to monitoring by us as outlined in section 13 below.

f) We also reserve the right to block access to certain websites using our Information Systems.

10. PERSONAL USE OF INFORMATION SYSTEMS OTHER THAN INTERNET USE

10.1 We permit the incidental use of our email and telephone systems to send personal email or messages, and make personal telephone calls subject to certain conditions set out below.

10.2 Personal use is a privilege and not a right. We reserve the right to withdraw permission or restrict access if you abuse this privilege.

10.3 The following conditions must be met for personal use to continue:

a) use must be minimal and take place substantially outside normal working hours (that is, during break times, before or after work),

b) use must not interfere with business or operational commitments,

c) use must not commit us to any extra costs, and

d) personal use must comply with this policy and our other related policies, including our Social Media Policy, and our policies on equality and diversity, anti-harassment and bullying, and data protection.

10.4 We reserve the right to require you to label personal emails as 'personal' in the subject header, or to otherwise distinguish them as personal messages and not from our organisation.

10.5 Personal use of our Information Systems may be monitored (see section 13 below).

11. RULES FOR SECURITY OF PERSONAL DATA AND CONFIDENTIAL INFORMATION

11.1 You are expected to safeguard all Personal Data and Confidential Information, and take steps to ensure it does not fall into the wrong hands.

11.2 You are required to consider and assess the security risks involved when working with Personal Data and Confidential Information. In cases of Special Category Data you will need to be even more vigilant.

11.3 Do not view or process Personal Data or any other Confidential Information unless we have authorised you to do so.

11.4 Ensure that any Personal Data or other Confidential Information is not on display on your desk, workstation or screen when not being used

11.5 Comply with any requirements in our Remote Working Policy for handling Personal Data or other Confidential Information outside our work premises.

11.6 Lock away any paper copies of Personal Data or other Confidential Information when not being used.

11.7 Securely dispose of paper copies of Personal Data or other Confidential Information, for example, by shredding them.

11.8 Unless it is absolutely necessary, and we have given you permission to do so, do not save Personal Data or any other Confidential Information on the local drive of any IT Equipment, external storage devices or on external 'cloud' storage (for example, Dropbox or icloud). Use our systems so that it can be securely held and backed up.

11.9 Think carefully before sending any Personal Data or other Confidential Information in the post. Consider using special delivery options or using a courier. Always follow up to ensure that Personal Data or other Confidential Information has reached the intended recipient. Special Category Data should not be sent in the post unless it is absolutely necessary and we have given you permission to do so.

11.10 If sending Personal Data or other Confidential Information via email, check carefully that you have the correct email address, that the recipient is authorised to process the information, and consider encrypting and password protecting any files.

11.11 Do not use social media to process any Personal Data or Confidential Information, even if you think it is safe. For further information, please refer to our Social Media Policy.

11.12 Always report any breaches of security or suspicions of breaches to us without any delay and comply with any further guidance we may introduce in this regard.

12. PASSWORDS

12.1 Passwords must be used on all IT Equipment and to access all Information Systems, particularly in order to keep all Personal Data and Confidential Information secure.

12.2 You must create strong and secure passwords. This means:

a) at least eight characters long,

b) containing at least one numeral, one capital and one symbol,

c) creating different, memorable passwords for each piece of IT Equipment and for each access to any of our Information Systems,

d) not duplicating any passwords for work with any other work or personal passwords,

e) changing any default installation passwords immediately after set up,

f) changing every password at least every 12 months, or more frequently if we require it, and

g) not using previously used passwords without altering them.

12.3 You must keep your passwords confidential and secure. This means:

a) not telling colleagues any of your passwords,

b) not writing your passwords down anywhere accessible by others,

c) only storing them electronically if it is encrypted and password protected, and

d) not allowing any passwords used in relation to work to be automatically remembered.

12.4 If you are accessing any of our Information Systems via programs or apps, ensure that, wherever possible, those programs or apps are not accessible without a password. For example, if you are accessing work files stored in the cloud on your iPhone, ensure that you have one password or equivalent strong secure method to access your iPhone and a different password or method to access the files in the cloud from your iPhone.

12.5 You must not use another person's username or password unless authorised by your manager.

12.6 On the termination of your employment (for any reason) you must provide details of your passwords for all Information Systems to your manager and return any equipment, key fobs or cards with password details.

12.7 If you become aware of any password issues or if you suspect a password may have been compromised, please report it immediately to either your manager or a Director, and immediately take steps to change the password or otherwise remedy the situation as instructed.

12.8 We may also issue separate written guidance on additional security measures to use on our IT Equipment or Information Systems, such as Two-Factor Authentication or Single Sign On, which will be attached as Appendices to this policy.

13. MONITORING OF USE

13.1 We may monitor telephone, email, voicemail, internet and other communications.

13.2 Monitoring may include, without limitation, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of our Information Systems as well as keystroke capturing and other network monitoring technologies. We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

13.3 For business or operational reasons, and in order to carry out legal obligations in our role as an employer, use of our Information Systems, including the telephone and computer systems, and any personal use of them, is continually monitored. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business or operational purposes.

13.4 We reserve the right to retrieve the contents of messages, posts or details of activity or check searches that have been made on the internet for the following purposes (this list is not exhaustive):

a) to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy,

b) to find lost messages or to retrieve messages lost due to computer failure,

c) to assist in the investigation of wrongful acts, or

d) to comply with any legal obligation.

13.5 We cannot guarantee that personal use of our Information Systems will not be caught in our monitoring systems. Do not use our IT Equipment and Information Systems for any matter you wish to be kept private or confidential from us.

14. STANDARDS OF COMMUNICATION

14.1 When communicating with anyone on our behalf, or in situations where your association with us is used or implied, make sure you act responsibly and are professional, accurate, courteous and appropriate at all times.

14.2 This applies to any form of communication, including email, social media messages, instant messaging, and video meetings using tools such as Zoom or Microsoft Teams.

14.3 Email and written messages:

a) Where we have provided a standard email signature and disclaimer, always include these when emailing outside our organisation.

b) Take care with the content of all messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

c) Do not send or forward private emails at work that you would not want a third party to read.

d) Remember that you have no control over where your message may be forwarded by the recipient. Do not say anything that would cause offence or embarrassment if it was forwarded to colleagues or third parties, or found its way into the public domain.

e) Remember that emails and other messages can be used as evidence in legal proceedings and that even deleted messages can remain potentially retrievable.

f) Avoid contributing to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them.

g) Do not agree to terms, enter into contractual commitments or make representations in writing unless you have obtained appropriate authority to do so. Be aware, for example, that a name typed at the end of an email is a signature in the same way as a name written at the end of a letter, and could create a legal obligation for us.

h) If you receive a wrongly delivered email or other message, you should return it to the sender.

14.4 Video meetings:

a) Consider the suitability of your location when organising a video meeting away from our work premises, including, for example, levels of background noise or the strength of your internet signal.

b) Minimise the risks of being overheard or interrupted, especially when using Personal Data or Confidential Information.

c) Consider your background on screen and take steps to change or blur it if

it would be inappropriate to see it in a work meeting.

d) Wear appropriate clothing for the meeting you are participating in.

15. BREACHES OF THIS POLICY

15.1 Misuse of our IT Equipment and Information Systems can damage our business and our reputation.

15.2 You must comply with this policy at all times to protect our IT Equipment and Information Systems from unauthorised access, misuse and harm.

15.3 Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

15.4 If you become aware of any misuse of our IT Equipment or Information Systems, you should report it to your manager or a Director.

15.5 If you consider that this policy has not been followed in respect of Personal Data or other Confidential Information, you should raise the matter with either your manager or a Director.

15.6 If you are suspected of committing a breach of this policy, you will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details of accounts used in the course of work, such as a professional Twitter or LinkedIn account, and also any relevant personal accounts, subject to compliance with data protection laws and the provisions of our Social Media Policy.

16. MONITORING AND REVIEW OF THE POLICY

16.1 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.