24 Computers, Email and Internet Policy

1. Introduction
   1. IT and communications systems are of key importance to our business. These systems must be used appropriately. There is a significant risk of damage to our business and its reputation if you misuse them.
   2. In this Policy, we set out the standards we require you to follow when using these systems and equipment. We also explain when we will monitor your usage, and for what purpose, and set out the sanctions for breaches of this Policy.
   3. Please note that this Policy does not form part of your contract with us. We reserve the right to amend or remove this Policy.
   4. This Policy applies to all employees and workers in our business and anyone who has access to our IT and communications systems. This may include contractors, agency workers, casual workers, interns and volunteers.
2. Computers
   1. You are responsible for the security of any IT equipment issued by us to you. You must not let any of your IT equipment be used by anyone else, whether at work or at home.
   2. When working, either in the office or remotely, you are responsible for the security of your computer terminal. The screen should always be locked if the computer is left unattended.
   3. You must shut down your computer at the end of each working day. We often schedule updates overnight and it is important that your computer is shut down for these updates to take effect.
   4. You must not remove or tamper with any software systems installed on our computers. If you have an issue in relation to any software installed on your work computer, then you should contact our IT Department for advice.
   5. You should use unique passwords for each electronic device we issue to you. They should ideally include a random string of capital and lowercase letters, symbols and numbers. You should keep all passwords confidential and should not share them with anyone else (save as outlined below). You should change your passwords regularly.
   6. You must provide us with details of all passwords on request and, in any event, on termination of employment.
   7. You must report any loss of IT equipment to our IT Department immediately.
   8. If you are issued with portable IT equipment by us, then you must make sure that it is stored safely and securely when being transported. If you are using our IT equipment whilst in a public place, then others may be able to view your screen. Please make sure that you do not display any confidential information when using IT equipment in public.
   9. If you are issued with any IT equipment (such as computers, monitors, keyboards or printers) for use when working remotely, then you must agree to return it to us on demand and, in any event, on termination of your employment. You are responsible for maintaining any IT equipment issued for remote use in a good condition. You are responsible for damage to any issued IT equipment, other than that caused by reasonable wear and tear and we will deduct the cost of any repairs from your pay where your contract authorises us to do so.
3. Systems and data security
   1. You must not download or install any software from external sources without the prior approval of our IT Department.
   2. You must not attach any devices (including USB sticks) to your work computer without the prior approval of our IT Department. This includes attaching any Bluetooth devices.
   3. You must not use any device on public unsecured Wi-Fi unless we have installed a Virtual Private Network on the device and you have activated it.
   4. We have a virus detection system installed on all our computers. You must not tamper with it or disable it. You can assist us in cyber security by making sure that you review all emails you receive from unknown sources. If you suspect that an email is not genuine, then you should contact our IT Department as soon as possible. Do not open the email or any attachments to it.
4. Email
   1. The following rules should be followed when using email:

* You should avoid the use of slang, emojis and ‘text speak’ when sending work emails.
* Always consider the relevant recipients when sending an email – do not copy messages unnecessarily widely.
* You should not forward chain emails or send jokes.
* You should not forward emails from your work account to your private email address.
* Do not send emails which are or might be considered abusive, obscene, discriminatory, harassing or otherwise inappropriate in nature. If you receive such an email, then you should inform your line manager or our HR Department immediately. We have a zero-tolerance policy in relation to bullying and harassment in the workplace. Please see our Bullying & Harassment Policy for more details.
* Email correspondence is disclosable in legal proceedings. All messages should be treated as being potentially disclosable in a court of law.
* It is possible to enter into a legally binding contract via email. If your job role involves the negotiation of terms which could form a contract, then you should ensure that all correspondence is headed “Subject to contract”.
* You must not use your personal email address for work purposes.

1. Internet
   1. We provide internet access in our workplace primarily for work. Personal use is only permitted on the basis set out in section 6.
   2. When using the internet, do not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive or immoral. As a general rule, if any person might be offended by the contents of a page or if the fact that our software has accessed a page might be a source of embarrassment or reputational damage, then viewing it will be regarded as a breach of this Policy.
   3. You must not use our systems to post on chat rooms or social media sites unless you are doing so as part of your job. For more guidance in this area, please refer to our Social Media Policy.
2. Personal use of email and the internet
   1. Our business provides email and internet access for work-related purposes. We acknowledge that some personal use will occur. However, excessive personal use of these resources during working hours may result in disciplinary action under our Disciplinary Policy.
   2. The following guidance should be followed:

* Personal use should be minimal.
* Personal use should not interfere with your work commitments.
* Personal use must not commit the business to any costs.
* Personal use must always comply with our Bullying & Harassment, Equal Opportunities, Data Protection and Disciplinary Policies.

1. Monitoring
   1. Your use of our IT and communications systems (including computer, internet, email and telephone) may be monitored by us. Any such monitoring will only be carried out to the extent permitted by law and in accordance with our Data Protection Policy.
   2. We may monitor and check emails and internet usage for reasons including the following:

* To assess compliance with our rules and policies
* To investigate alleged wrongdoing by you or others
* To monitor performance, particularly if you are undergoing a performance management process and have been told that we will be monitoring your email and internet usage
* To retrieve lost messages
* To access messages and information if you are unable to do so directly (for example due to illness or other absence)
* To comply with our legal obligations

1. Use of personal devices for work purposes
   1. Our general rule is that personal devices are not allowed to be used for business purposes. However, there may be circumstances where you need to use certain personal devices (such as smartphones, laptops and tablets) for work. Any use must be in accordance with the following rules:

* Any personal device (Device) must be approved by our IT Department before it can be connected to our systems and be used for work purposes. We may require you at our cost to implement additional security measures prior to approving your Device for work use.
* Any software systems installed by us to allow your Device to be used for work must not be tampered with or removed by you.
* We reserve the right to monitor, intercept and remove any content on your Device which has been created by us or on our behalf to the extent permitted by law or for our legitimate business purposes. Please see our Data Protection Policy for details.
* As your Device is a personal one, we are aware that inadvertent monitoring, interception, review and removal of personal data may occur. You should have no expectation of privacy in relation to any data on the device if you are using it for work purposes.
* You must delete any data relating to our business which is stored locally on your Device as soon as it is no longer required.
* You must pay all costs associated with your Device and its use, including technical support.
* You must cooperate with us and allow us to inspect your Device at any time on request. You will provide any necessary passwords or login details to enable us to have full access.

You must report any loss of the Device immediately to our IT Department.

* If you leave our employment or propose to sell or transfer your Device to someone else, then you agree to present your Device to us prior to transfer/termination to allow us to remove all business software and data from it.
  1. Any breach of these rules may result in us revoking your permission to use your Device for work purposes. It may also result in disciplinary action up to and including dismissal or, in the case of a contractor or agency worker, the termination of your engagement.

1. Breaches of this Policy
   1. Any breaches of this Policy will be handled under our Disciplinary Policy. In the case of agency workers, contractors, casual workers and interns, we reserve the right to terminate your engagement in the event of a breach or an alleged breach of this Policy.
   2. Certain behaviours in breach of this Policy may give rise to a criminal offence or other public concern. We may pass any evidence collated to the police or other relevant authority.
   3. If you become aware of conduct of others which may be in breach of this Policy, you should report your concern immediately to your line manager. Our Whistleblowing Policy provides further guidance.
2. Useful links and contacts
   1. The following internal policies are referred to in this Policy and contain additional information and guidance:

* Disciplinary Policy
* Social Media Policy
* Grievance Policy
* Data Protection Policy

1. Administration of the Computers, Email and Internet Policy
   1. Name1 is responsible for the administration of this Policy. Should you have any queries or feedback, please email to Email1.

|  |  |
| --- | --- |
| Organisation Name: | ABC Ltd |
| Policy Adopted Date: | 1st January 2024 |
| Due for Review Date: | 1st January 2026 |
| Person Responsible for Policy: | Name1 |
| Email: | Email1 |