### ***EXAMPLE***

### **IT and Internet Use Policy**

#### **1. Policy Statement**

This policy outlines the rules for the proper and responsible use of the company’s IT resources, including computers, mobile devices, email, and internet access. The purpose of this policy is to ensure the protection of company data, maintain productivity, and safeguard against security threats. All employees, contractors, and third-party workers are expected to adhere to this policy to ensure compliance with UK data protection laws, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

#### **2. Scope**

This policy applies to all employees, contractors, and temporary staff who use the company’s IT systems, internet, and email services. It covers the use of company-owned devices, networks, and IT systems, as well as any personal devices that access company systems or data.

#### **3. Acceptable Use of IT Resources**

The company provides IT resources, including computers, mobile devices, email, and internet access, for business-related purposes. Employees are expected to use these resources responsibly and in a manner that supports the company’s goals. Acceptable uses include:

* Conducting business-related research and communications.
* Accessing and using business-related software and applications.
* Sharing information and collaborating with colleagues and clients.

Limited personal use of company IT resources is permitted, provided it does not interfere with job performance, violate any laws or policies, or expose the company to security risks. Personal use should be restricted to break times and should not involve significant use of company bandwidth or resources.

#### **4. Unacceptable Use of IT Resources**

The following activities are prohibited while using company IT resources:

* **Accessing inappropriate content**: Viewing, downloading, or sharing offensive, illegal, or inappropriate materials, including content that is discriminatory, pornographic, or related to hate speech.
* **Illegal activities**: Engaging in any activities that violate UK law, such as software piracy, hacking, or unauthorised access to systems.
* **Unauthorised software**: Installing unapproved software or applications on company devices without IT department authorisation.
* **Misuse of company data**: Accessing, modifying, or sharing sensitive company information, including client data, intellectual property, or confidential documents, without authorisation.
* **Personal business activities**: Conducting personal business or profit-making activities using company resources.
* **Excessive personal use**: Using company devices or internet excessively for personal activities, such as online shopping, social media, gaming, or streaming media.

#### **5. Internet and Email Usage**

The company’s internet and email systems are provided for professional use. Employees must use these systems responsibly and in accordance with the following guidelines:

* **Professional communication**: Company email accounts should be used for professional purposes only. Personal email accounts should not be used for conducting company business.
* **Security**: Employees should avoid opening unsolicited or suspicious emails, clicking on unknown links, or downloading attachments from untrusted sources to prevent phishing attacks, malware, or other security breaches.
* **Confidentiality**: Emails containing confidential or sensitive information should be encrypted or sent using secure communication methods. Employees must comply with the company’s data protection policies when sharing personal data via email.
* **Monitoring**: Employees should be aware that the company reserves the right to monitor internet and email usage in line with UK employment law to ensure compliance with this policy and protect against data breaches or misuse.

#### **6. Remote Access and Use of Personal Devices**

Employees working remotely or using personal devices to access company systems must adhere to the following rules:

* **Secure connections**: Remote work should be conducted using secure and encrypted connections, such as Virtual Private Networks (VPNs), to protect company data from unauthorised access.
* **Approved devices**: Personal devices used for work purposes must be approved by the IT department and comply with the company’s security standards, including up-to-date antivirus software and password protection.
* **Data protection**: Employees must ensure that any company data stored on personal devices is secure and compliant with data protection laws. Company data should not be stored on personal devices unless necessary for work purposes, and it should be deleted as soon as it is no longer required.

#### **7. Data Security**

The company takes data security seriously and expects employees to follow all guidelines to protect company and client information. Key security measures include:

* **Passwords**: Employees must use strong, unique passwords for all company systems and devices. Passwords should not be shared with colleagues or written down in insecure locations.
* **Data storage**: Sensitive data must be stored in secure locations, such as encrypted drives or password-protected folders. Cloud storage solutions should only be used if they are approved by the company.
* **Backups**: Employees are responsible for ensuring that work-related data is regularly backed up to company-approved storage systems to prevent data loss.
* **Reporting security incidents**: Any suspected data breaches, security incidents, or suspicious activities must be reported to the IT department immediately to prevent further harm.

#### **8. Social Media Use**

Employees are expected to use social media responsibly while using company IT resources. Personal social media use should be restricted to break times and must not interfere with work duties. Employees must not:

* Share confidential or proprietary company information on social media platforms.
* Use social media to make defamatory, discriminatory, or inappropriate remarks about the company, colleagues, or clients.
* Engage in activities that could damage the company’s reputation online.

#### **9. Consequences of Misuse**

Misuse of company IT resources, internet, or email systems will be treated as a disciplinary matter and may result in disciplinary action, which could include:

* **Verbal or written warnings**: For minor breaches of this policy.
* **Suspension or dismissal**: For more serious or repeated violations, especially those involving illegal activity, breaches of confidentiality, or security incidents.
* **Legal action**: Employees may be held personally liable for illegal activities conducted using company IT resources.

#### **10. IT Monitoring and Privacy**

To ensure compliance with this policy and protect company data, the company may monitor employee activity on its IT systems. Monitoring will be conducted in line with the company’s privacy policy and relevant UK employment laws. Monitoring may include:

* Internet usage, including websites visited and time spent online.
* Email communications, including email content and attachments.
* Use of company devices, including software installed and files accessed.

The company will ensure that all monitoring activities are conducted lawfully and transparently, with employees being informed of any routine monitoring practices.

#### **11. Training and Awareness**

All employees will receive training on IT security, acceptable use, and data protection during onboarding. Regular refresher training will be provided to ensure employees are aware of changes to policies, technologies, and security risks. Employees are encouraged to seek guidance from the IT department if they are unsure about acceptable use or security measures.

#### **12. Review of Policy**

This policy will be reviewed regularly to ensure it reflects the latest developments in technology, data security practices, and UK laws. Any updates will be communicated to all employees, and they will be required to confirm their understanding and agreement with the revised policy.