

Computer, Internet & Email Acceptable Usage Policy (AUP)

**Introduction**

It is the intention of Sigmar Recruitment Consultants Ltd. (Sigmar) to provide a pleasant working environment for its entire staff and to mitigate risk and protect its resources. This Acceptable Usage Policy (**AUP**) is valid for all companies under the Sigmar umbrella.

This AUP forms part of the terms and conditions of your employment with Sigmar, under which employees may use the company’s computer and communications equipment and networks. **Any** **breaches of the policies included in this document may result in disciplinary action, up to and including dismissal, or appropriate legal action being taken against you.**

It is the responsibility of any person using a Sigmar resource to read, understand, and follow these guidelines. In addition, users are expected to exercise reasonable judgment in interpreting these guidelines and in making decisions about the appropriate use of Sigmar resources. Any person with questions regarding the application or meaning of these guidelines should seek clarification from their IT administrator. Use of Sigmar resources shall constitute acceptance of the terms of these guidelines. Upon terminating employment, a user is required to notify their IT administrator.

Each employee has the responsibility to maintain Sigmar Group’s established culture of openness, trust and integrity and this document is a reflection of its policy to protect its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly, and to use all resources in a productive manner and avoid placing our businesses at risk.

**No Expectation of Privacy**

* Sigmar resources remain the property of Sigmar Group and are to be used in conformance with these guidelines. Sigmar retains the right to inspect any user’s Hard & Network Drives and any files they may contain. Sigmar also has the right to give permission to management & IT administrators to review the use of Sigmar resources of any user.
* Users are advised that all mail & file transfers, including deleted mails/files, are automatically archived and can be retrieved. In addition, an Internet firewall automatically checks all data moving between the local area network and the Internet and logs the sending and receiving destinations. Use of Sigmar technology resources constitutes consent that Sigmar staff can monitor and/or inspect any files you create, any messages you post or receive, and any web sites you access. Key logging software can be installed at any time to monitor user inputs.
* In order to ensure compliance with the General Data Protection Regulation (GDPR) the Company reserves the right to scan all devices, emails, telephone recordings, CCTV, storage, backups and anywhere or means where personal data may be stored. This is to ensure that we are able to comply with the Data Subject rights and entitlements under GDPR. Consequently, please do not assume privacy in relation to any means of data either email, telephone message or CCTV where related to work. Data howsoever occurring, in order to comply with GDPR may need to be scanned to ensure full access and processing accounts of data subject personal data, therefore any data cannot be deemed private.

All employees are expected to be fully compliant with their obligations under the Data Protection Policy.

**General PC & File use**

* It is not permissible to install or remove any hardware/software on the computer or the network without first consulting your IT department. All software should be licensed appropriately.
* Sigmar respects the rights of copyright holders and requires all employees to likewise respect and adhere to the rights of the copyright holders. There should be no storage or transmission of copyright material on company systems, networks, equipment or storage media without permission of the copyright holder.
* Copyright is the legal right granted to an author, composer, playwright, publisher, or distributor to exclusive publication, production, sale, or distribution of a literary, musical, dramatic, or artistic work. Things which may be considered copyright material include: music, movies, pictures, software and any item which displays the © symbol.
* Third party and personal hardware should not be connected to company devices without authorization from the IT Administrator.
* It is not permissible to install games, screensavers, peer-to-peer software, or any sort of file sharing programs under any circumstances.
* Viruses & Trojans are a huge threat to the Data and the PC’s sitting on the Sigmar network. It is not permissible to download files from the Internet or use disks from non-company sources without first having them scanned by the IT department unless the download is for business purposes or from a secure site.
* The company reserves the right to restrict access to files & servers. Any attempt to circumvent these restrictions is a breach of this policy.
* The “C:\ Drive” is the local drive on the computer and should never be used for saving documents. Any documents saved to the C:\ drive will NOT be backed up and are **not** the responsibility of the IT department. Your “My Documents” folder can be used for saving confidential documents that can only be accessed by the user and IT administrators.
* All programs need to be closed and PC’s completely shut down before leaving the office unless with prior approval/direction by the IT department.

**Passwords**

* Each person is responsible for safeguarding their passwords to allow them access to the Sigmar systems. Passwords should not be printed or stored online. A staff member’s password is to be kept secret and should not be shared with anyone else, except if explicitly asked by a member of your IT department. Each person is responsible for all transactions made with their password. Users will be forced by the systems to change their passwords periodically and to use “strong passwords”. Strong passwords are passwords of more than 6 characters, which must include 3 of each of the following:

A capital letter, a small letter, a number or a “special” character (£, $, %, & etc.,)

For Example: **dUblin07**, **Cred1t%**, **F4nta5y**, **DogName$1** etc.

**Email usage**

* E-mail is a powerful communication tool which gives us the potential to reach our clients and service their needs more quickly and efficiently than the more traditional media of post and fax. E-mail is an electronic document and is often treated more informally and less seriously than “hard copy” communications. “However, it is important that we treat e-mail in the same way as we would our letters”.
* The company reserves the right to monitor emails and other communications originating in, transmitted from or stored on company assets (for example, communication on phones, email servers, disk storage).
* If “Joke” mails or chain e-mails are received they must be deleted immediately. It is not permissible to send or forward any such E-mails to any other person or organisation. If a “Joke” mail is opened by accident, close the mail and delete it.
* As a general rule, if any of the following attachments are received, they must be deleted immediately.
* Non Business related Program files (EXE’s)
* Non Business related PowerPoint/Word documents, movie files (mov, avi, MPEG), picture files (jpg, jpeg, bmp).
* The company does not condone defamation or libel of any party at any time. At no time should an employee make (verbally or in written communication) a false statement of fact that injures any individual or company’s reputation.
* At no time should any communication from an employee of this company contain inappropriate terminology or statements. This includes usage of terms which may be considered swear words and statements which are racial, sexually explicit, religiously offensive or other potentially offensive or menacing material. All will be dealt with as a serious breach of this policy.
* Personal usage of email or other communications devices is not allowed in any Sigmar companies, other than at lunch time & at Management’s discretion. The company reserves the right to restrict access to certain websites, internet servers, phone numbers and other external services. Any attempt to circumvent these restrictions is a breach of this policy.
* Employees shall promptly disclose to their manager or IT Administrator, any message they receive that is inappropriate or makes them feel uncomfortable.
* If you receive “Spam” or any other form of inappropriate or undesired communication via email or any other communications method, you should immediately contact your IT administrator. Do not forward or copy any communication containing inappropriate or undesirable material to other parties.
* The company has a standard disclaimer of liability which is automatically attached to all emails sent through the company email server. Circumventing this disclaimer or preventing it from being attached to the email is a breach of this policy.

**Viruses:**

The IT department has implemented centralised, automated virus detection and virus software updates within the Company. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

* Remove or disable anti-virus software.
* Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Company anti-virus software and procedures.

**Internet usage**

* An Internet firewall automatically checks all data moving between the local area network and the Internet and logs the sending and receiving destinations.
* Deliberate attempts to gain access to sites containing material of pornographic, racially or religiously offensive, illegal or offensive material will be dealt with as a serious breach of this policy.
* Personal Internet usage is not allowed in any Sigmar companies, other than at lunch time & at Management’s discretion. The company reserves the right to restrict access to certain websites, internet servers, phone numbers and other external services. Any attempt to circumvent these restrictions is a breach of this policy.
* Access to online chat, dating, social networking, gambling & auction sites is prohibited at all times.

**Data Protection**

It is the responsibility of the employee to be aware of data protection and privacy legislation which may relate to information or data in a communication, in particular the General Data Protection Regulation which came into effect 25th May 2018. At no time should an employee breach any relevant data protection or privacy laws. Information on data protection can be obtained at the website for the Data Protection Commissioner: <http://www.dataprotection.ie>. This website contains information on your legal obligations concerning access to and usage of data pertaining to other parties.

**Confidentiality & Intellectual Property**

* The employee shall keep confidential all information which is disclosed (by whatever means, directly or indirectly) by the company whether before or after this Agreement and which is either marked “confidential” or is by its nature confidential, including without limitation confidential information relating to the company or Group companies, Work Results and the company’s actual or proposed business activities, financial offers (including, for the avoidance of doubt, the fees and Gross Margin), products, systems, operations, processes, plans, intentions, developments, trade secrets, customers and/or suppliers (the “Confidential Information”);
* For the avoidance of doubt, employees shall not without the Company’s express permission remove from the Company’s premises any material containing any Confidential Information (including without limitation Client and Candidate contact information); and on request, return to the Company (or as the company may direct) all materials in its or their possession or control and belonging to the Company and/or containing Confidential Information.
* Intellectual Property Rights created by the employee during their employment with the company shall vest in and belong to the company with a full title guarantee by the employee
* “Intellectual property rights” means any and all present and future copyrights, registered designs, patents, trademarks, service marks, design rights (whether registered or unregistered), applications for any of the above, rights to extract or re-utilise data, know how, database rights, trade secrets, rights of confidence and all other similar rights recognised in any part of the world.

**Remote Access**

* Where a person has access to the company systems (including but not limited to VPN, Citrix, Remote Desktop) at an external source, they are responsible to ensure that such access is not abused and does not compromise the security of the company’s computer systems. It is the responsibility of employees with VPN/remote privileges to ensure that unauthorized users are not allowed access to Sigmar resources & internal networks.
* Connections from non-owned Sigmar resources must ensure that the equipment is configured to comply with the Sigmar computer & network policies outlined above.

**Working Off-site**

* It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:
* Working away from the office must be in line with **Company remote working policy**.
* Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
* Laptops must be carried as hand luggage when travelling.
* Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
* Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

**Clear Desk and Clear Screen Policy**

* In order to reduce the risk of unauthorised access or loss of information and in compliance with GDPR, the Company enforces a clear desk and screen policy as follows:
* Personal or confidential business information must be protected using security features provided for example secure print on printers.
* Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
* Care must be taken to not leave confidential material on printers or photocopiers.
* All business-related printed matter must be disposed of using confidential waste bins or shredders.

**Telephony (Voice) Equipment Conditions of Use**

Use of Company voice equipment is intended for business use. Individuals must not use Company’s voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual’s own expense using alternative means of communications.

Individuals must not:

* Use Company’s voice for conducting private business.
* Make hoax or threatening calls to internal or external destinations.
* Accept reverse charge calls from domestic or International operators, unless it is for business use.

**Actions upon Termination of Contract**

* All Company equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Company at termination of contract.
* All Company data or intellectual property developed or gained during the period of employment remains the property of Company and must not be retained beyond termination or reused for any other purpose.

**Monitoring and Filtering**

* All data that is created and stored on Company computers is the property of Company and there is no official provision for individual data privacy, however wherever possible the Company will avoid opening personal emails.
* IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Company has the right (under certain conditions) to monitor activity on its systems, including Internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.
* Any monitoring will be carried out in accordance with audited, controlled internal processes,
* It is your responsibility to report suspected breaches of security policy without delay to your line management, the IT department or the Admin department.
* All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Company disciplinary procedures.

**Conclusion**

All users are obliged to comply with the outlined Acceptable Usage Policies in a responsible, ethical and lawful manner. **Any** **breaches of the policies included in this document may result in disciplinary action, up to and including dismissal, or appropriate legal action being taken against you.**

Confirmation of Acceptable Usage Policy

BY SIGNING THIS ACCEPTABLE USAGE POLICY (AUP), YOU CONFIRM THAT YOU HAVE READ, UNDERSTOOD AND AGREE TO COMPLY WITH THE TERMS AND CONDITIONS OUTLINED IN THE POLICIES AS DESCRIBED.

|  |  |  |  |
| --- | --- | --- | --- |
| Signed: |  | Witness: |  |
| Block Letters: |  | Position: |  |
| Date: |  |  |  |