# 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version: | 1 | | | |
| Date Created: | 01st February 2024 | | | |
| Author: | Timothy Van Zyl | | | |
| Ratified by: |  | | | |
| Date Ratified: |  | | | |
| Review Date: |  | | | |
|  |  |  |  |  |
| Revision History: | | | | |
|  |  |  |  |  |
| Version | Date Created | Date Ratified | Author | Summary of Changes |
| 1.0 |  |  |  |  |
| 2.0 |  |  |  |  |
| 3.0 |  |  |  |  |
| 4.0 |  |  |  |  |
| 5.0 |  |  |  |  |

**Introduction**

Habbibi’s electronic communications systems and equipment are intended to promote effective communication and working practices within our organisation, and are critical to the success of our business. This policy outlines the standards we require users of these systems to observe, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards.

This policy applies to all workers, full and part-time employees, agency workers, volunteers and contractors (collectively referred to as staff in this policy).

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

**Policy scope and purpose**

This policy deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones, smartphones, personal digital assistants (PDAs) and voicemail, but it applies equally to the use of fax machines, copiers, scanners and CCTV.

All staff are expected to comply with this policy at all times to protect our electronic communications systems and equipment from unauthorised access and harm. Breach of this policy may be dealt with under our Disciplinary Policy and, in serious cases, may be treated as gross misconduct leading to dismissal.

The Chief Technical Officer will deal with requests for permission or assistance under any provisions of this policy, subject to their primary tasks of maintaining our core systems, and may specify certain standards of equipment or procedures to ensure security and compatibility.

All managers have a specific responsibility to operate within the boundaries of this policy and ensure that all staff understand the standards of behaviour expected of them, and to take action when behaviour falls below its requirements.

**Equipment security and passwords**

Staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy. If given access to the e-mail system or to the internet, staff are responsible for the security of their terminals.

If leaving a terminal unattended or on leaving the office (depending on their role), the terminal must be locked, logged or switched off to prevent unauthorised users accessing the system in their absence. Staff without authorisation should only be allowed to use terminals under supervision. Desktop terminals, PCs and EPOS systems and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the manager on duty.

Passwords are unique to each user and must be changed regularly to ensure confidentiality.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the HR Department. For the avoidance of doubt, on the termination of employment (for any reason) staff must provide details of their passwords to their Line Manager or a member of HR department and return any equipment.

Staff who have been issued with a laptop, tablet, mobile phone or any other electronic device must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

**Systems and data security**

Staff should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

Staff should not download or install software from external sources without authorisation from their Line Manager or the Chief Technical Officer. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be viruschecked by the IT team before they are downloaded. If in doubt, staff should seek advice from the Chief Technical Officer or their Line Manager.

Employees are permitted and expected to use discretion when using the internet on the basis that it is for business or professional study/ research use only.

The organisation’s intranet services provide the organisation with an internal infrastructure that gives employees and Line Managers access to local network Web services, and ability to manage and obtain appropriate documentation throughout their employment with the organisation.

Employees are expected to ensure that personal use is not excessive; does not have a negative impact on their work, colleagues or environment; does not appear to have been sent on behalf of Habbibi for personal use, does not bring the user, co-workers and the organisation into disrepute, and does not contravene any other guidelines or policies.

Any employee found to deviate from this policy may be subject to disciplinary action in line with the organisation’s disciplinary procedures.

No device or equipment should be attached to our systems without the prior approval of the line manager. This includes any USB flash drive, MP3 or similar device or telephone. It also includes use of the USB port, infra-red connection port or any other port.

We monitor all e-mails passing through our system for viruses. Workers should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .ex). The Chief Technical Officer should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to e-mails for the purpose of effective use of the system and for compliance with this policy. We also reserve the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network, or to any password protected information, unless specifically authorised.

Staff using laptops or Wi-Fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by the Chief Technical Officer from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

**E-mail etiquette and content**

E-mail is a vital business tool, but an informal means of communication, and should be used with great care and discipline. Staff should always consider if e-mail is the appropriate means for a particular communication and correspondence sent by e-mail should be written as professionally as a letter or fax. Messages should be concise and directed only to relevant individuals. A standard disclaimer should always be included.

Staff should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory emails. Anyone who feels that they have been harassed or bullied, or are offended by material received from another staff member via e-mail should inform their Line Manager a member of HR department.

Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable.

In general, staff should not:

* send or forward private e-mails at work which they would not want a third party to read
* send or forward chain mail, junk mail, cartoons, jokes or gossip
* contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them
* sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals
* agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter
* download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this
* send messages from another worker's computer or under an assumed name unless specifically authorised
* send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure
* Staff who receives a wrongly-delivered e-mail should return it to the sender. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

**Use of the internet**

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. Such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

Staff should therefore not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. Whilst content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in their own time, unless authorised to do so.

The organisation understands that there may be a need for its employees to use the internet as a platform to build and develop business relationships, and for that purpose, the organisation recognises that Linkedin is the appropriate social networking site.

Any employee associating themselves with Habbibi or associated business of the Organisation must be linked to the appropriate Habbibi organisation profile.

**Social Media**

Employee are not permitted to use any social networking sites e.g. facebook, twitter etc. during the working day. This is to reduce the risk of potential exposure to cyber threats and viruses in addition to putting a drain on network resources.

Employees are reminded that when visiting social network outside of normal working hours, to ensure that they use discretion, and are explicitly instructed not to associate themselves with the organisation should they belong to any particular online group or site. In addition, employees must also be aware that they have an obligation to ensure that they do not bring either themselves, the Organisation and/or its employees into disrepute, and any comments posted in public domain are subject to this obligation. Any Employee found to divert away from this instruction will be the subject of disciplinary proceedings.

**Personal use of systems**

We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

The following conditions must be met for personal usage to continue:

* use must be minimal and take place substantially out of normal working hours
* personal e-mails must be labelled "personal" in the subject header
* use must not interfere with business or office commitments
* use must not commit us to any marginal costs
* use must comply with our policies including the Equality, Diversity and Inclusion Policy, Bullying and Harassment Policy, GDPR Policy and Disciplinary Procedure

Staff should be aware that personal use of our systems may be monitored and, where breaches of this policy are found, action may be taken under the disciplinary procedure.

We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

**Monitoring of use of systems**

Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our 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 purposes.

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

* to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy
* to find lost messages or to retrieve messages lost due to computer failure
* to assist in the investigation of wrongful acts
* to comply with any legal obligation

**Inappropriate use of equipment and systems**

Access is granted to the internet, telephones and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with our rules, policies and procedures (including this policy, the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure).

Misuse or excessive use or abuse of our telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be dealt with under our Disciplinary Procedure.

Misuse of the internet can in certain circumstances constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

* pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature)
* offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our customers
* a false or defamatory statement about any person or organisation
* material which is discriminatory, offensive, derogatory or may cause embarrassment to others or the Organisation
* confidential information about us or any of our staff, patients, or service users (which you do not have authority to access)
* any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us)
* material in breach of copyright

Any such action will be treated very seriously and is likely to result in dismissal.

Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.