INFORMATION SECURITY POLICY

Statement of policy and purpose of policy

1. EASY WI-FI LIMITED (the **Employer** or **Supplier**) provides staff with access to a range of communications and information technology equipment and systems (**Resources**) both as a shared resource in the workplace and also through individual allocation of items for use inside or outside the workplace. It is our aim and responsibility to:
    a. provide you with all the Resources necessary for the proper performance of your duties, in a reasonable and economical manner;
    b. ensure the security of Resources against unauthorised access or abuse whilst ensuring their accessibility to authorised and legitimate users.
2. The purpose of this document is to explain to staff the standards we require them to observe in using our Resources and the consequences of not adhering to these as well as to explain our policy in respect of monitoring use of our Resources.
3. This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

Who and what does this policy cover?

4. This policy and the rules contained in it apply to:
    a. All staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (Staff); and
    b. All use of our Resources including but not limited to use (and misuse) of computer servers and other hardware or equipment, desktop or portable computers, laptops and mobile telephones, Blackberries and other smart phones or personal digital assistants (PDAs), networks and systems, software, applications, subscriptions to databases and electronic resources, fax machines, scanners, printers, memory or storage devices, copiers, CCTV, and electronic keys, passes and cards, cloud hosting, laptop, phone, email, the internet and any data sent from, received by, or stored on our computer or communications equipment or systems.
5. The board of directors of the Employer has overall responsibility for this policy and has appointed the security team leader (Paul Devins) as the person with day-to-day responsibility for the Employer's Resources.

6. All Staff have personal responsibility to use our Resources in a professional, ethical and lawful way and ensure compliance with this policy. You are expected to protect our Resources from unauthorised use or access at all times. Managers have special responsibility for leading by example and monitoring and enforcing compliance.
7. Any breach of this policy will be taken seriously and may result in disciplinary action.

Personal use of Resources

8. Our Resources are provided to support Staff in the proper performance of their duties. We allow Staff to make occasional and incidental personal use of Resources, so long as all use complies with this policy and does not interfere with the proper performance of work duties or business use of the Resources. Personal use of Resources must not consume more than a trivial amount of Resources or commit us to any marginal cost. It must take place substantially out of normal working hours or during lunch hours. You should be aware that use of the Resources is monitored by the Employer and so you should have no expectation of privacy as regards any personal or business use of the Resources.
9. Personal use of our resources is a discretionary privilege that we offer and which we may withdraw at any time, either in general or for particular members of Staff. Staff who do not comply with our guidelines for personal use of Resources or who otherwise abuse the privilege may have their right to personal use or to access to certain telephone numbers or internet sites withdrawn and/or disciplinary action may be taken.

   We expect all users to adhere to the acceptable use policy when using equipment and services for business or personal use without exception.

Guidelines for PC and Laptop Use

10. Each employee has responsibility for the appropriate use and day-to-day care of their office computer workstation and any computer equipment provided for use on or off our premises.
11. You may not connect personal equipment or peripherals, for example, flash memory cards and sticks, mp3 players or digital cameras, to our Resources unless this has been authorised in advance by the security team.
12. You will log on your computer using an individual username and password. You must not log on to any computer using someone else's name and password or otherwise use our Resources in a way that would lead us to believe that your activities are somebody else's, unless this has been approved in advance by the security team even if you have the consent of the individual concerned.
13. Do not leave your computer accessible to others when you are not at your computer. Lock your screen or logout whenever you are away from your computer for more than a few minutes.

Using Resources outside work (Remote Access Policy)

14. If you are given authorisation to use any Resources away from our premises, including at home, (Remote Resources) then you must take appropriate care of the any equipment provided to use, ensure it is well-maintained and used in accordance with our rules, including this policy and with specific instructions given to you by the security team. We may inspect Remote Resources without prior notice and, if asked, you must immediately return any equipment to us for inspection or maintenance.

15. Remote Resources provided to you are your responsibility. You must take reasonable steps to ensure the security of any equipment provided to you for use outside the workplace. If you are transporting equipment by car, it should be locked and left out of sight when the vehicle is unattended (e.g. in the boot of a car).

16. We provide equipment and other Resources for use outside the workplace in our absolute discretion and may withdraw this entitlement at any time. You must immediately return any Resources to us if we ask you to and, in any case, when your employment ends. When accessing resources remotely this should only be done using the approved VPN service, credentials and software provided by EASY WI-FI LIMITED and all activities in accordance with our data protection and data security policy.

Email guidelines

17. Email is an efficient and cost-effective means of communication and we encourage its appropriate use for business related purposes. However, inappropriate or negligent use of email carries significant risks.

18. Your communications by email, like all other modes of communication, must not breach our disciplinary or workplace rules or any other policy and procedure and must not cause us to be in breach of obligations we owe to others. See the Misuse of Resources section of this policy, below, for further information.

19. Confidentiality is a particular concern when using email. You must be careful in addressing messages to make sure that communications are not inadvertently sent to unintended recipients. In addition, although we take steps to protect data security, you should be aware that the confidentiality of data (including email messages) sent via the internet cannot be assured. You should only send price sensitive or commercially sensitive information belonging to or relating to us with the prior authority of the security team unless the emails and any attachments are password protected or encrypted in line with our guidelines

20. Delivery of email cannot be guaranteed. If your email is urgent or important, check that it has arrived safely with the intended recipient.

21. In general, you should not:

    a. distribute chain mail, junk mail, jokes or gossip, trivial or unnecessary messages; or.

    b. agree to terms, enter into contractual commitments or make representations by email unless you are authorised to do so.

22. If you are sent an email in error you should delete it and notify the sender. You should disclose or use any confidential information it contains.

23. Bear in mind that viruses may lurk in attachments or links sent by email. While we take measure to protect against viruses, do not open emails or attachments or click on links unless they are from a source that you know and trust. If you see any virus alert or notification on your computer, contact the security team immediately.

24. In using email, you should observe the standards for communication that we expect for other forms of writing, including as to style, content and choice of language.

25. Always consider whether there is a more suitable method of communication, for example, where there is a need to preserve confidentiality or in the case of sensitive issues which should be communicated face to face.

26. Do not use your work email address to register or sign up for online services or otherwise to communicate with any provider of goods or services, since this is likely to increase the amount of spam email that we receive as a business.

27. You must comply with any guidelines that we issue concerning filing, archiving and deletion of emails.

28. If you are out of the office on a working day you must create an automated "out of office" message to alert correspondents to your absence and the arrangements for dealing with any urgent queries.

29. All emails sent using our Resources must include the following disclaimer text: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. .

Guidelines for Internet Use

30. When using the internet, remember that each website that you visit has the ability to detect information about you, including our identity as an organization and, potentially, your identity and who you are, and whom you represent. The information that you input on a website may be accessed by third parties, anywhere in the world. Accordingly, judgement and discretion should be used in determining the websites that you choose to access and your activities on that site.

31. You must read and comply with the terms and conditions of any website that you access using our Resources.

32. Please refer to our acceptable use policy for full details about internet and resource access.

Guidelines for Software Use

33. Most of the software and applications we use are licensed from third parties and our use is subject to terms and conditions. You must always comply with the terms of any software license we hold. You must not copy, download or install any software or application except with the prior approval of the security team.

34. If any computer, phone, Blackberry or other hardware we have provided to you prompts you to update or renew any software or application licensed to us, then you must do so promptly, unless we have told you not to.

35. Only software or applications provided or authorised by the security team may be installed on our Resources including but not limited to on your desk computer or laptop and any Remote Resources. You may not install other computer games, internet files, software, applications or other programs on our Resources.

Monitoring of use of our Resources

36. We may monitor and intercept your use of our Resources, including your internet use and communications sent to you or received by you, by phone, email (including associated files or attachments), fax or any other means, involving our Resources for a number of relevant business reasons, including but not limited to:

    a. ensuring compliance with the terms of this policy;

    b. training and monitoring standards of service;

    c. ensuring compliance with regulatory practices or procedures imposed or recommended by any regulatory body relevant to our business;

    d. ascertaining whether internal or external communications are relevant to our business;

    e. preventing, investigating or detecting unauthorised use of our IT systems or criminal activities;

    f. maintaining the effective operation of our Resources - in particular, all emails received by the Employer are automatically scanned for viruses;

    g. establishing the existence of facts.

37. Where it becomes apparent in the course of monitoring emails or other communications that a particular message is obviously private, we will take reasonable steps to respect your privacy in respect of that message. However, it may not be possible to determine whether that communication is personal or business-related until it is already open and read. You should therefore not have any expectation of privacy as to your use of our Resources, including communications sent to you or received by you, by phone, email (including associated files or attachments), fax or any other. If you wish to maintain the privacy of your communications, you should not use our Resources for personal use.

38. Certain authorised employees involved in administering our Resources may necessarily have access to the contents of email messages in the course of their duties. Any knowledge thus obtained should not be communicated to others, unless necessary for legitimate business reasons.

39. We may also take any action in administering email or other communications that is reasonably necessary to preserve the integrity or functionality of our Resources including as part of a firewall or spam or virus protection arrangements. This could include the deletion or non-transmission of any emails or communications (including any personal communications).

Data Protection

40. Monitoring of our Resources use will be conducted in accordance with an impact assessment that we've carried out to ensure that monitoring is necessary and proportionate. Monitoring our Resources is in our legitimate interests and ensures this policy is being complied with. For the purposes of the law on data protection, the Employer is a data controller of the personal information in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal information is processed. The person responsible for data protection compliance is our Data Protection Officer.

41. Monitoring will normally be carried out by our Security team.

42. Information obtained through monitoring may be shared internally, including with members of the HR team, your line manager, managers in the business area in which you work and IT staff, if access to the information is necessary for performance of their roles. Information is only shared internally if we have reasonable grounds to believe that there has been a breach of this policy. We will not share information gathered from monitoring with third parties, unless we have a duty to report matters to a regulatory authority or law enforcement agency. Personal information gathered through monitoring will not be transferred outside of the European Economic Area (EEA).

43. You have a number of rights in relation to your personal information, including the right to make a subject access request and the right to have your information rectified or erased in some circumstances. You can find out more about these rights and how to access them in our Data protection policy, which you can find here: https://easy-wifi.co.uk/legal-and-policy-reference/. If you believe that we have not complied with your data protection rights, you can complain to the Information Commissioner.

Password policy

44. Appropriate passwords are vital to maintaining the security of our Resources.

45. In general, to access certain Resources such as computers, mobile phones or other devices or certain information sources or accounts, it will be necessary to enter a password or personal identification code. Passwords should be kept private and are the direct responsibility of the person to whom the account or device is allocated. Where access to any device or equipment that we provide to you can be secured by a password or code, you must use that facility.

Password standards

46. Passwords used on our Resources should adhere to the following standards, where permitted by the device or account in question:

    a. they must contain at least 8 characters in total and at least one of each of the following:

        i. uppercase character

        ii. lowercase character

        iii. numeric character

    b. they should not be a dictionary word in any language, slang, dialect, jargon, etc.

    c. they should not be based on readily available information about you like your date of birth, spouse's or child's name, telephone numbers or address.

    d. they should not be the same as or contain your name or username.

    e. you must not use the same password on our Resources as you do for your personal accounts or devices.

    f. they must differ materially from previous passwords.

Password security

47. You are personally responsible for maintaining the security of your passwords used on our Resources. You must not disclose your password to anyone else, inside or outside the Employer, except as directed by the security team. You may not keep a written record of your passwords anywhere on our premises or any device unless it has been encrypted.

48. You must not attempt to access any restricted area of our Resources or to guess or determine the password of any other user.

49. You must change your main computer log in password when prompted to do so either automatically or by contacting the security team.

50. If you become aware or suspect that your password has become known to another person then you must immediately change it and notify the security team of the situation.

51. On termination of your employment, however arising, or if requested to do so by the security team, you must provide details of all passwords used on our Resources to the security team.

Misuse of Resources

52. The same principles apply to your use of Resources for communication including through email, telephone and the internet as apply to any means of communication and you must not use these for any purpose or in any way which could be subject to disciplinary or legal action in any other context. In particular, you must not use our Resources in any way that:

    a. breaches obligations of confidentiality which you owe to us or to any third party or which causes us to breach duties of confidence which we owe to any third party.

    b. breaches the rights of any other Staff member to privacy, data protection and confidentiality or which amounts to bullying or harassment;

    c. is offensive, insulting, immoral, discriminatory, obscene, pornographic or sexually explicit;

    d. poses a threat to our confidential information and intellectual property;

    e. infringes the intellectual property rights of any other person or entity;

    f. defames or disparages us or our associated companies or to any party with whom we have a business relationship, such as suppliers or customers;

    g. breaches or causes us to breach any law or the rules or guidelines of any regulatory authority relevant to our business;

    h. breaches data protection rules;

    i. breaches our rules, policies or procedures for the use of our IT Systems or other equipment or resources;

    j. is dishonest, improper, unethical or deceptive (eg pretending to be someone or attempting to access another employee's computer, computer account, email, files, or other data);

    k. is likely to damage your reputation or our reputation;

    l. breaches any of our other policies and procedures, including

        i. Acceptable use Policy

    m. wastes Resources or use them excessively or to the exclusion of others;

n. interferes with the work of others or our computer, technology or communications systems.

53. Further, you must not:

a. delete, destroy or attempt to modify our Resources or any information contained on them except in line with this policy or instructions given to you by the security team;

b. use our resources to conduct any business other than our business.

54. You should also note that the following activities are criminal offences:

a. unauthorised access to computer material (hacking); and

b. unauthorised modification of computer material.

Other relevant policies

55. Staff are referred to other Employer policies and procedures which may be relevant to the issues covered in this policy including policies concerning:

a. data protection and data security

b. Acceptable use Policy