
EMAIL, INTERNET AND COMPUTER SYSTEM POLICY

1. This policy contains the Business' expectations in relation to the operation and use of its internet, email and computer systems.
 - 1.1 This policy may be changed from time to time. The policy does not form part of any contract.
 - 1.2 In certain cases, the Business chooses to give staff and others access to information and communication systems and devices. Those persons who are given access are expected to act responsibly and follow this policy.
2. **EMAIL, INTERNET, COMPUTER EQUIPMENT AND OTHER DEVICES**
 - 2.1 You are expected to take a professional and courteous approach to everything you do in connection with work, during and outside working hours, that includes:
 - sending emails;
 - accessing and searching the internet (including Facebook, Twitter, Instagram and any other social network, blogging or method of communicating via the internet); and/or
 - using computer equipment issued or paid for by the Business.
 - 2.2 You should **not** expect that any email or other activity conducted over the Business' computer network(s) will be private or otherwise confidential.
 - 2.3 You are allowed personal use that is reasonable and limited so as not to get in the way of you doing your job.
 - 2.4 You must not say or type things about the Business unless you have been told you can do so.
 - 2.5 You must respect the equipment, treating it carefully.
 - 2.6 Passwords must be kept confidential, except where you need to provide your password to IT.
 - 2.7 You must not engage in use that involves conduct or material that is inappropriate or otherwise obscene or offensive such as accessing or distributing content of a sexual, pornographic, discriminatory, sexist or racist nature.
 - 2.8 You must not engage in use that includes conduct or material that has the risk of defaming, or of causing damage to, the Business or any of its officers or employees.
 - 2.9 You must not engage in use that includes unlawful activities that are illegal or otherwise inappropriate.

-
- 2.10 You must not engage in use that impacts the performance of the network(s), computers or other equipment owned or operated by or on behalf of the Business.
- 2.11 An email may be blocked by the Business if it is in breach of this policy. You will usually receive a 'bounce back' or other email to let you know this has happened.

3. SURVEILLANCE

- 3.1 The law requires us to let you know that the Business conducts:
- computer surveillance of all its information technology systems, including email usage, internet usage and any other usage of information technology supplied by the Business. This surveillance is be carried out on an intermittent but ongoing basis and will effectively start upon commencement of this policy;
 - camera surveillance by way of closed circuit television cameras. The surveillance will be continuous and ongoing and will effectively start upon commencement of this policy. Access to the recorded material will be strictly limited to authorised personnel; and
 - tracking surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device). The surveillance will be continuous and ongoing and will effectively start upon commencement of this policy. Access to the recorded material will be strictly limited to authorised personnel.

4. CONFIDENTIALITY AND PRIVACY

- 4.1 You are not allowed to take or otherwise release any confidential information or intellectual property owned by the Business unless you have been told to do so for work purposes.

5. FAILING TO FOLLOW THIS POLICY

- 5.1 The outcomes of failing to follow this policy can include a warning, a final warning or in the worst cases, the termination of your employment.