eltegroup.im

Elite Group

Acceptable Use Policy

Sponsors	Elite	Board of Directors	
Approvers	Elite	Board of Directors	
Owner	Elite	Director	Alex Cliffe
Authors	ISMS Team		
Audit	Annual		
Every 3 years: Elite Internal Audit			
Review Period	Annual		
Issue Date	19th February 2020		
Next Review	19th February 2021		
Document Name	Acceptable Use Policy		
Document Version	1.1		

Related Documents

Type	Name	Version
Policy Manual	Information Security Management System Policy Manual	1.0
Internal Publication	Employee Handbook	
Process	Induction Process	
Document	Access Control Matrix	
Policy	Acceptable Use Policy	

Document History

Version	Author	Notes	Date
1.0	ISMS Team	Final Document for publication	07/02/2019
1.1	ISMS Team	Extension to Scope for Wrexham Office	19/02/2020

Contents

1 Purpose

Its purpose is to outline the principles for acceptable use of Elite's IT facilities and services, for the mutual benefit of Elite and users of Elite's IT facilities.

2 Scope

This Policy applies to all Elite's IT facilities, whether they are located on Elite premises or elsewhere and regardless of the source of funds used to procure them. For the purpose of this Policy, Elite IT facilities include all:

- physical or virtual computers, whether servers, desktops, terminals or mobile devices;
- peripherals such as monitors, keyboards and printers;
- computer networks, including wireless and telecommunications networks;
- software and data on Elite IT facilities;
- computer-based information systems provided for any purpose; and
- devices not owned by the Elite which are connected to the Elite network.

This Policy applies to all members of staff, as well as individuals conducting work at or for Elite and/or its subsidiaries, who are authorised to have access to Elite's IT facilities ("users").   In this Policy, any reference to the Head of IT also includes reference to an authorised deputy ("Head of IT").

3 Responsibilities & Compliance Framework

3.1 Responsibilities

The Head of IT is responsible for defining, reviewing and publishing this Policy and for providing policies, procedures, guidance, advice and training in support of it, and taking action pursuant to this Policy. Heads of Departments, Directors or equivalent are responsible for ensuring that all staff within their area act in accordance with this Policy and established procedures. Each user is responsible for ensuring that their use of Elite's IT facilities is acceptable and is accountable for all actions undertaken using their Elite login credentials (username, password and other authentication tokens).

3.2 Acceptable use

Elite's IT facilities are provided to staff and contractors for Elite-related activities. However, subject to paragraph 3.3 below, reasonable personal use (i.e. use not related to Elite's activities) is permitted, provided this does not interfere, either by its timing or extent, with the availability of Elite's IT facilities for Elite-related activities or the performance of a member of staff's duties. Elite does not provide any guarantees regarding the privacy or security of any personal use of Elite's IT facilities and users do so at their own risk. Any material and information for personal use which is stored on Elite's IT facilities can be accessed by Elite in the same way as it can access other material and information (see 4 below).

3.3 Unacceptable use

Unacceptable use of Elite IT facilities includes using Elite's IT facilities to download, creation, manipulation, transmission or storage of:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
- unsolicited "nuisance" emails;
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of Elite staff or a third party;
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
- material with the intent to defraud or which is likely to deceive a third party;
- material which advocates or promotes any unlawful act;
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
- material that brings Elite into disrepute.

Elite's Network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

- intentionally wasting staff effort or other Elite resources;

- corrupting, altering or destroying another User's data without their consent;
- disrupting the work of other Users; or
- denying access to the Elite's Network and its services to other users.
- pursuance of personal commercial activities (even if in support of Elite's business).

Where the Elite's Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the Elite Network.

Users shall not:

- introduce data-interception, password-detecting or similar software or devices to Elite's Network;
- seek to gain unauthorised access to restricted areas of the Elite's Network;
- access or try to access data where the user knows or ought to know that they should have no access;
- carry out any hacking activities; or
- intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

3.4 Exceptions

Where use of Elite's IT facilities for what would be considered unacceptable use is required for Elite-related activities, the user must seek the prior written permission of a Director.

4 Monitoring Compliance

Non-compliance with this Policy must be reported to the Head of IT who will determine the action to be taken, which may include disciplinary proceedings. Any breach of this Policy may lead to removal of access to Elite's IT facilities. No member of staff is permitted, as a matter of routine, to monitor or investigate an individual's use of Elite's IT facilities. However, where, for example, there are reasonable grounds to suspect an instance of unacceptable use of any Elite's IT facilities, or where a legitimate request is made by the police or other authority, permission may be granted by a Director of Elite for the monitoring or investigation of an individual's use of Elite's IT facilities. This may include the monitoring of email and use of the internet (for example, use of social media websites).

5 Further Information

Further information and guidance on this policy can be obtained from the Information Security Officer.

This Policy forms part of a series of documents on Information Security and acceptable use and should be read in conjunction with them.