ESH GROUP
ACCEPTABLE USE OF COMPUTING RESOURCES

Policy Author:	Paul Carmody, Head of IT
Date:	April 2018
Policy Review Date:	2019
Policy Owner:	Mark Sowerby, Group Chief Financial Officer

1 Policy Statement

Esh Group's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to our established culture of openness, trust and integrity. Esh Group balance this with a committment to protecting its employees, partners and itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Esh Group. The investment in these is for business purposes in order to serve the interests of the company, and of our clients in the course of normal operations.

Effective security is a team effort involving the participation and support of every Esh Group employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment at Esh Group. These rules are in place to protect the employee and Esh Group. Inappropriate use exposes Esh Group to IT security risks including virus attacks, compromise of network systems and services, and legal issues.

All employees are required to also read the Group Data Protection Policy and ensure that their IT use is compliant with that policy.

2 Scope

For the purpose of the Policy, the Esh Group includes all its subsidiaries and associated companies.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Esh Group, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Esh Group.

All employees, contractors, consultants, temporaries, volunteers and other workers at Esh Group are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Esh Group

policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 3.2.

3 Policy

3.1 General Use and Ownership

3.1.1 Esh Group information stored on electronic and computing devices whether owned or leased by Esh Group, the employee or a third party, remains the sole property of Esh Group.

3.1.2 Staff have a responsibility to promptly report the theft, loss or unauthorised disclosure of Esh Group proprietary information to their line manager.

3.1.3 In the event that Personal Information is lost or compromised, this must be reported immediately to the Data Protection Officer (see Data Protection Policy).

3.1.4 You may access, use or share Esh Group proprietary information and Personal Information only to the extent it is authorised and necessary to fulfill your assigned job duties.

3.1.5 Use of Esh Group equipment for personal use (e.g. internet access or personal email) is permitted however, staff are responsible for exercising good judgment regarding the reasonableness of personal use to maintain security and levels of productivity. If there is any uncertainty, employees should consult their supervisor or manager.

3.1.6 For security and network improvement purposes, authorised individuals within Esh Group may monitor equipment, systems and network traffic at any time.

3.1.7 Esh Group reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2 Security and Proprietary Information

3.2.1 All mobile and computing devices that connect to the internal network must comply with the standards referred to in the IT Security Policy.

3.2.2 System level and user level passwords must comply with the standards referred to in the IT Security Policy. Providing access to another individual, either deliberately or through failure to adequately secure access, is prohibited.

3.2.3 All computing devices are secured with a password-protected screensaver with the automatic activation feature set to 10 minutes. You must lock the screen or log off when the device is unattended.

3.2.4 Postings by employees from a Esh Group email address to newsgroups or social media should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Esh Group, unless posting is in the course of business duties.

3.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

3.3 Unacceptable Use

3.3.1 The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

- Under no circumstances is an employee of Esh Group authorised to engage in any activity that is illegal while utilising Esh Group-owned resources.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Esh Group.

- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Esh Group or the end user does not have an active license is strictly prohibited.

- Accessing data, a server or an account for any purpose other than conducting Esh Group business, even if you have authorised access, is prohibited.

- Exporting software, technical information, encryption software or technology, in violation of laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. The only exception to this being if IT Services require your password to aid resolution of a support call.

- Using an Esh Group computing asset to actively engage in procuring or transmitting material that is in violation of the law.

- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing,

pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Using tools that scan the IT Network (such as port / security scanning) is expressly prohibited unless prior notification to the Head of IT is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Esh Group network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Extracting and providing information about, or lists of, Esh Group employees to parties outside Esh Group.

3.3.2 Email and Communication Activities - When using company resources to access and use the Internet, users must realise they represent Esh Group. Whenever employees state an affiliation to the Group, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". The following are prohibited.

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Esh Group's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Esh Group or connected via Esh Group's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

3.3.3 Blogging and Social Media - Blogging and any social media activities by employees, whether using Esh Group's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Esh Group's systems to engage in blogging and social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Esh Group's policy, is not detrimental to Esh Group's best interests, and does not interfere with an employee's regular work duties and productivity levels. Blogging or engaging in any social media activities from Esh Group's systems may also be subject to monitoring.

3.3.4 Employees are prohibited from revealing any Esh Group confidential or proprietary information when engaged in blogging or social media activities.

3.3.5 Employees shall not engage in any blogging or social media that may harm or tarnish the image, reputation and/or goodwill of Esh Group and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or posting on social media.

3.3.6 Employees may also not attribute personal statements, opinions or beliefs to Esh Group when engaged in blogging or social media activities. If an employee is expressing his or her beliefs and/or opinions in blogs or on social media platforms, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Esh Group. Employees assume any and all risk associated with this type of activity.

3.3.7 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Esh Group's trademarks, logos and any other Esh Group intellectual property may also not be used in connection with any blogging or social media activity.

4 Policy Compliance

4.1 Compliance Measurement

4.1.1 Esh Group will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

4.2.1 Any exception to the policy must be endorsed by the appropriate Business Director and approved by the Head of IT in advance.

4.3 Non-Compliance

4.3.1 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.