ESH GROUP
IT SECURITY POLICY – STAFF GUIDANCE

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

I.T. Security – practical tips for keeping your data safe and secure

Esh Group have an IT Security Policy which defines what we must all do in order to keep data and IT systems safe and secure. This should be read in conjunction with the Esh Group Acceptable Use Policy which outlines the appropriate use of computer equipment that protects our workers and the Group.

It is necessary to read both documents in full, however here are some key salient points:

Why IT security is important

Whatever role you have in Esh Group, some of the data you use may be sensitive (e.g. commercial pricing) or confidential (e.g. name, address, financial details), and so you must ensure you keep it safe. Legislation to enforce Data Protection has been tightened through GDPR (see also Data Protection Policy), which increases the need for strong IT controls to protect Personal Data.

We also access data using a wide range of devices, mostly owned by Group but sometimes accessed from personal devices. The same standard of security applies to all devices, irrespective of ownership – including the ones that you own yourself.

There are also countless threats to IT security, with phishing emails, malware and viruses and social engineering that look to get hold of data for financial or malicious gains.

In summary, you must treat Esh Group's information as you would wish your own details to be handled.

Passwords

- Any device (desktop, laptop, tablet or smartphone) that connects to the Esh Group network must be protected by a password.
- Use a strong password, 8 characters or more in length. Group IT recommend using three random words but avoiding simple combinations such as "onetwothree" or words that are closely related to you personally, such as the names of family members or pets. In the case of a tablet or smartphone, a minimum of a 6-digit secure PIN is required. Keep it a secret.
- Don't use the same password for work and personal use.
- Never share your login details with anyone, for any reason unless specifically asked to by Group IT to aid in resolving a support issue.
- Never leave your computer left unlocked and unattended. Log out or lock it.

Email

- Always take care before opening attachments or links, especially if you are not expecting them. Before you click on a link, hover your cursor over it to check its true destination.
- Only send sensitive or confidential information electronically if it is encrypted (such as a password protected Microsoft Office document). For advice on encryption, contact Esh Group IT.
- Check the content of emails before 'forwarding' as they may contain sensitive information not intended for the recipient(s).

Phones, tablets and other computing devices.

- If you are using your own device, please be aware of your responsibilities under the Acceptable Use Policy.
- When on the move, computing devices must be locked away securely when not with an individual (for instance in the boot of a car).
- You should report stolen or lost phones as soon as possible to Esh Group IT.

Software

- Do not install software on a company owned device that hasn't been approved by Esh Group IT. Unauthorised software will be removed.
- Ensure you restart your machine to apply the latest software updates when prompted to do so.

Storage

- Do not keep sensitive or confidential data in insecure locations. Always use the Esh Group Network and folders that have appropriate security controls in place. If in doubt, contact Esh Group IT.
- If you need to copy data to a USB device, it must be encrypted. Please speak to IT if you require an encrypted stick.

Web browsing and social media

- Before you log in to a supposedly secure website, check in your browser's address box that you can see the padlock symbol. This indicates that the site is secure. Be extra vigilant if using Public Wifi.
- Consider the consequences carefully before you give out any personal or Esh Group details on websites and social media.

Starters and Leavers and Changes

- Esh Group IT must be informed of every worker starting, changing role or leaving the Group who has access to Esh Group IT systems and services.
- Company owned devices must be returned directly and promptly to Esh Group IT if a worker is either changing role or leaving the Group.

Disposing of equipment

- Esh Group equipment must be securely disposed of through Esh Group IT.

Reporting concerns or security breaches

- Report any IT security incidents or concerns straight away to Esh Group IT.