INFORMATION SYSTEMS POLICY & PROCEDURE
V1.0 November 2025

POLICY STATEMENT

ELCAP will use technology and media to help provide high quality services, safely, efficiently, effectively and economically.

The guidelines relating to the use of social media should also be read when using this procedure.

ELCAP wishes to ensure that its Information Systems are used responsibly and safely by all users. ELCAP must ensure that all data relating to individuals is kept confidential and secure. ELCAP therefore requires all users to use information systems including the internet, intranet and e-mail in a way that is legal, secure and confidential. All resources, including hardware, software and data remain the property of ELCAP and may not be changed without permission and must be returned when no longer required. Any loss must be reported immediately.

PROCEDURES

The company reserves the right to access e-mail, Internet/intranet activity and other communications used in ELCAP's work, that may impact on ELCAP's work or that utilises ELCAP resources.

The distribution of any information through the internet, computer-based services, e-mail, and messaging systems (including WhatsApp) is subject to the scrutiny of the company. The company reserves the right to determine the suitability of this information.

Breaches of licensing and copyright agreements is illegal and may result in criminal charges.

Confidentiality

All computer processing of data relating to living individuals must be registered and be undertaken in accordance with the General Data Protection Regulations (2018).

Unauthorised access is an offence under the Computer Misuse Act. If any user has gained access to information which should not be generally available then this should be reported to ELCAP's Business Manager.

Any breaches of confidentiality or loss of data should be reported to ELCAP's Business Manager, Data Protection Officer ASAP. ELCAP under the General Data Protection Regulations (2018) are obliged to report any loss of data.

Security

All ELCAP laptops, desktops and phones will require passwords but any staff using their own mobile with e-mail and intranet access for ELCAP business must also apply a password. A password should be used for any other equipment where this facility is available.

New software should only be installed by an approved IT technician.

Shareware, Freeware, Public Domain and Evaluation software is bound by the same policies and procedures as all software.

All Hardware and Software purchases must be approved by the Chief Executive.

Disposal of Equipment

Any equipment that is disposed of will have confidential information or copyright or licensed material removed, preferably by the removal and total destruction of the Hard Disk Drive and by a qualified technician.

Remote Access (working from home using VPN)

VPN configuration information and security settings must not be divulged to any other person. You must inform the Chief Executive immediately if you believe that another person may have had access to this information.

The user is responsible for selecting an ISP, ensuring that their operating system software supports the VPN connection and for any associated costs or fees in relation to this. The user must ensure that all critical security patches are applied to their operating system software and that this is maintained. The user must ensure that they have a recognised antivirus software solution and that this is kept up to date.

The user will be responsible for the configuration of their PC or laptop to establish the VPN connection. Only approved VPN clients will be used.

Users will be disconnected after five minutes of inactivity. You must re-establish the connection again. Artificial processes must not be used to maintain connection during periods of inactivity.

Only one VPN connection is allowed per PC / laptop.

If you dispose of or transfer a PC / laptop with VPN connection details configured on it, you must ensure that the connection settings are securely removed before hand. You must also notify the Chief Executive that the equipment has been disposed of or transferred. A qualified technician will also advise you with regards the secure removal of ELCAP files from your hard disk drive.

Any company files taken from the server should only be stored temporarily on your local drive while you are working on the file or document. You must ensure that the revised file is then uploaded back on to the server and all copies securely removed from your local drive.

By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of ELCAP's network, and as such are subject to the same rules and regulations that apply to ELCAP owned equipment.