Approved by Management Committee 25/03/21

Policy Document

ELHA POLICY

Date Issued	**February 2021**
Department	Corporate Services - IT
Title	**ICT SECURITY POLICY**
Objective	Provide Staff with suitable Information Communication Technology (ICT) for their working needs and to prevent unauthorised access to the Group's IT Network
Responsible	Director of Finance
Review Date	February 2026

1.0 Introduction

We ensure that we provide our staff with the access to the Information and Communications Technology (ICT) systems they require to undertake their duties, whilst maintaining strict security to prevent unauthorised access to these systems. We are committed to maintaining the highest standards of ICT Security and protection of our data.

1.1 The aims of this policy are to:

- Protect the Group's network from unauthorised access, cyber-attacks, theft of data, fire and other risks
- Provide staff with suitable ICT for their working needs, including access to the programs and data they require
- Deny access to all programs, data and hardware to unauthorised users
- Comply with all legal requirements in relation to GDPR
- Require a high level of anti-virus protection to be in place
- Require multi-factor authentication to be installed for remote working
- Minimise the risk of introduction to our ICT systems of unauthorised programs, data, viruses or other risks
- Maintain procedures related to our ICT systems

1.2 Cyber Essentials Certification

Cyber Essentials is a UK Government information assurance scheme that is operated by the National Cyber Security Centre (NCSC). It encourages organisations to adopt good practice in information security. Cyber Essentials also includes an assurance framework and a simple set of security controls to protect information from threats coming from the internet.

There are two levels of assurance. The Group currently holds Cyber Essentials, but is working towards the higher level, Cyber Essentials Plus.

1.3 Related Policies / Procedures

The ICT Security Policy is supported by:

- Cyber Essentials Certification
- The ICT Strategy
- The Use of Information Technology Procedure
- The Working Away from the Office Policy
- The Emergency Working from Home Policy
- The Information Technology Systems Policy

2.0 Responsibility for ICT Security

2.1 The Director of Finance has overall responsibility for ensuring the security of our ICT Systems and data. The Director of Finance and Corporate Services Manager will work with the Group's IT Managed Services provider to make sure all systems and data are secure.

2.2 Conflicting duties and areas of responsibility shall be segregated where possible to minimise the risk of accidental or misuse of the Group's assets.

2.3 The Group's IT Managed Services provider will maintain all security and passwords relating to the network and applications.

3.0 Network / Application and Data Security

3.1 Our infrastructure will be protected by firewalls and virus protections managed by our IT Support provider.

3.2 IT Support staff will have separate system administrator logins.

3.3 All staff are provided with a unique user identity which allows access to the system and which is further protected by passwords. Staff are required to keep these passwords confidential and change them at least once every 90 days.

3.4 All staff are given access to the areas of the Network and applications relevant to their role. Access requirements are supported by authority from a line manager.

3.5 All staff must log out of the network at the end of their working day.

3.6 Staff leaving the Group will have their system access rights terminated on their leaving date.

3.7 The Group's IT Support provider:

- Is responsible for ensuring a daily back-up of our network is undertaken and for confirming success to the Group's IT Support staff.
- Will alert us of any data security breaches, and of any unusual / unauthorised access attempts or other suspicious activity
- Will carry out patching to our network at regular intervals to meet our security requirements (for example "Cyber Essentials" certifications)
- Provide regular reports detailing any potential security breaches, network issues requiring attention and actions to be taken
- In conjunction with our Corporate Services Manager and IT Support Staff, will ensure multi-factor authentication (MFA) is required for all users working remotely
- Manage and maintain all network and administration passwords securely

3.8 All staff are required to adhere to their own department's controls and procedures for data entry, processing and reporting.

3.9 The use of memory sticks will be kept to a minimum and tightly controlled. IT Support will maintain a register of memory sticks held and staff are required to return these to IT Support after use for the removal of any data.

4.0 Document Security

4.1 Users will have access to drives on our network, depending on their operational requirements. The drives provided for users are as follows:

- "H" Drive as home directory for users to store private files
- "J" Drive, ELHA's shared drive for user access by department (this drive contains all policies and procedures for Group and ELHA operations)
- "K" Drive – R3 Repairs' shared drive for user access by R3 staff and relevant ELHA staff (this drive contains all policies and procedures for R3's operations)
- "Q" Drive – Secure drive, accessible to Senior Management Team only

4.2 In addition to the above, there are other drives that are provided for individual software packages to support our applications, e.g. SDM.

5.0 Procedures

5.1 We maintain a suite of IT procedures including critical network operating procedures (password protected as required).

5.2 We review procedures regularly and update them to reflect current processes.

5.3 We issue the "Use of Information Technology" procedure to all staff and provide regular updates.

5.4 The Corporate Service Manager / IT Support staff will report any breaches of network or data security to the Senior Management Team.

5.5 All breaches of the network or our data will be recorded in line with GDPR requirements.

6.0 Monitoring and Review:

6.1 This policy will be reviewed every five years by the Director of Finance.