



Committee Approver	Board of Management
Stakeholder Consultation	Executive Team and Board of Management
Date Approved	May 2021
Classification	Policy
Title	ICT System Security Policy
Revision Date	May 2021
Revised by	Director of Business Support/ Head of Business Support
Next Revision Date	May 2024
Related Documents	ICT System Security Policy, Remote Access Policy, Data Retention Policy, Privacy Policy and Procedure, Social Media Policy
Location of Electronic Copy	F:\Live Policies\Corporate

## **1. Viewpoint's Values**

Viewpoint is here to help people enjoy their later years. Everything we do is about realising this vision, which is supported by the following straightforward set of values:

- Inspire with positive smiles and words;
- Say 'yes I can and I will';
- Celebrate age, experience and wisdom;
- Do according to our customers' wishes and ambitions;
- Treat people (everyone is a VIP) as we would a "loved one";
- Work hard, have fun and laugh;
- Stay courageous, creative and ahead of the game; and
- Work with those that share our values.

These promises shape us. They are a commitment to our residents, staff and suppliers. They are fundamental to every single plan, decision and project we embark on.

Ensuring that we have systems and processes in place to manage risk effectively will support us to deliver those plans, decisions and projects, in accordance with our vision and values.

## **2. Policy Statement**

We will put in place arrangements to ensure that:

- We use all information and communications technology (ICT) equipment, email, the Internet and data as effectively as possible;
- We have clear rules governing the use of ICT equipment, email and the Internet, and the security of the information held on our computer systems; and
- All individuals who we authorise to use our ICT systems are aware of these rules and the consequences of breaching them.

## **3. Aim (sometimes called Purpose)**

The aim of this policy, and the procedures which support it, is to outline the principles that govern the use of ICT systems and resources provided by us, and to advise Viewpoint employees of their responsibilities when using these facilities.

#### 4. Legislation/related policies

This policy, and the procedures which support it, have taken into account the governance of ICT guidance from International Standards Organisation (ISO) 38500 in particular Principles 1, 5 & 6 below:

- Principle 1: Responsibility  
Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.
- Principle 5: Conformance  
IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.
- Principle 6: Human Behaviour  
IT policies, practices and decisions demonstrate respect for Human Behaviour, including the current and evolving needs of all the 'people in the process'.

The Information Security controls of standard ISO 27002 are also taken into account. ISO 27002 gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s).

This policy, and the procedures which support it, comply with the following legislation:

- Copyright, Designs & Patents Act 1988 (with regard to the copying of software);
- Malicious Communications Act 1988 (with regard to the sending of electronic communications);
- Misuse of Computers Act 1990;
- Data Protection Act 2018 and related guidance; and
- Communications Act 2003 (section 127).

This policy, and the procedures which support it, should be read in conjunction with Viewpoint's Data Retention Policy, Privacy Policy and Procedure, and Social Media Policy.

## **5. Scope**

This policy, and the procedures which support it, applies to all Viewpoint Board Members, employees, and third parties accessing Viewpoint ICT systems.

## **6. Compliance & Support**

Any breach of this policy, and the procedures which support it, will be dealt with in terms of Viewpoint's disciplinary policy and procedures. Serious breaches of this policy and the procedures which support it will be considered gross misconduct in accordance with Viewpoint's disciplinary policy and procedures.

Any member of staff requiring training or clarification on any aspect of this policy and the supporting procedures should contact their line manager.

## **7. Equality Impact Assessment (EIA)**

No potential equalities issues have been identified in relation to the review of this policy, and consequently an EIA has not been completed.

## **8. Privacy Impact Assessment (PIA)**

No data protection implications have been identified in relation to the review of this policy, and consequently a PIA has not been completed.

## **9. Monitoring & Evaluation**

Viewpoint has the right to audit and monitor its Information Systems and reserves the right to access, any computer, mobile device, data file, log file, document, voicemail or email message to maintain and protect ICT provision for the benefit of Viewpoint.

We will ensure that each new employee receives a copy of this policy, the supporting procedures, the Remote Access Policy and the Statement for signature set out in Appendix 2 to the ICT System Security Procedure which supports this policy.

The CEO will ensure that this policy is reviewed at least every three years.