

**Main/Registered Office: Signposts, 58 Regent Road, Morecambe, LA3 1TE**

**Telephone : (01524) 419021**

**Fax : (01524) 411541**

Community  
Legal Service



Help Point



E-mail: [signpostsmarc@signposts.org.uk](mailto:signpostsmarc@signposts.org.uk)

Website: [www.signposts.org.uk](http://www.signposts.org.uk)

**“Working to Empower the Community”  
in Lancashire and Cumbria**

**Pamela Beswick - Chief Executive Officer**

## Remote ICT Access Policy

### What is Remote Access?

Remote Access refers to any technology that enables you to connect users in geographically dispersed locations. This access is typically over some kind of dial-up connection, although it can include WAN connections.

### 1. Purpose of Policy

Remote access by staff is a method of accessing files and systems that is becoming more common. Often, critical business processes such as Casework Databasing and access to corporate communication rely on easy and reliable access to corporate information systems. In practice, the benefits of securing remote access are considerable – business can be conducted remotely with confidence and sensitive corporate information remains confidential. This document sets out the policy for remote access and includes a set of common controls, which can be applied to reduce the risks associated with a remote access service.

Willful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.

### 2. Scope

This policy covers all types of remote access, whether fixed or ‘roving’ including:

- 2.1. Travelling users (e.g. Staff working across sites or are temporarily based at other locations)
- 2.2. Home workers (including IT support)

### 3. Objectives

The objectives of the policy on remote access by staff are:

- 3.1. To provide secure and resilient remote access to Signposts information systems.
- 3.2. To preserve the integrity, availability and confidentiality of Signposts information and information systems.
- 3.3. To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security.

Charity Registration Number: 1117645

Member of AdviceUK (previously FIAC)

Company Limited by Guarantee: 5990592

Registered in England and Wales



North Lancashire  
Teaching Primary Care Trust



INVESTOR IN PEOPLE

Additional major funding from Preston City Council, the FC Scott Charitable Trust and Tudor Trust

- 3.4. To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that Signposts is adequately protected under computer misuse legislation.

#### 4. Principles

In providing remote access to staff, the following high-level principles will be applied:

- 4.1. The CEO will be appointed to have overall responsibility for each remote access connection to ensure that Signposts's policy and standards are applied.
- 4.2. A formal risk analysis process will be conducted for each application to which remote access is granted to assess risks and identify controls needed to reduce risks to an acceptable level.
- 4.3. Remote users will be restricted to the minimum services and functions necessary to carry out their role.

#### 5. Responsibilities

- 5.1. Signposts **Board** is ultimately responsible for ensuring that remote access by staff is managed securely.
- 5.2. The **CEO** will maintain policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks.
- 5.3. **The CEO** is responsible for providing clear authorisation for all remote access users and the level of access provided and for confirming whether remote access to business applications and systems is permitted.
- 5.4. **The ICT Support Providers** will ensure that user profiles and logical access controls are implemented in accordance with agreed access levels.
- 5.5. **The ICT Support Providers** will provide assistance on implementing controls.
- 5.6. All **remote access users** are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources, notify Signposts immediately of any security incidents and breaches.
- 5.7. Users must return all relevant equipment on termination of the connection.
- 5.8. **Senior Managers** are responsible for assessing risks and ensuring that controls are being applied effectively.

#### 6. Risks

Signposts recognises that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:

- 6.1. unavailability of network, systems or target information
- 6.2. degraded performance of remote connections
- 6.3. loss or corruption of sensitive data
- 6.4. breach of confidentiality
- 6.5. loss of or damage to equipment
- 6.6. breach of legislation or non-compliance with regulatory or ethical standards.

#### 7. Security Architecture

The security architecture is typically integrated into the existing network and is dependent on the IT services that are offered through the network infrastructure. Typical services include:

- 7.1. Password authentication, authorisation, and accounting
- 7.2. Strong authentication
- 7.3. Security monitoring by intrusion detection systems

## 8. Security Technologies

To ensure the most comprehensive level of protection possible, every network should include security components that address the following five aspects of network security.

### 8.1. User Identity

All remote users must be registered and authorised by the Deputy CEO. User identity will be confirmed by strong authentication and User ID and password authentication. **The ICT Support Providers is responsible for ensuring a log is kept of all user remote access.**

### 8.2. Perimeter Security

The **ICT Support Providers** will be responsible for ensuring perimeter security devices are in place and operating properly. Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. Routers and switches handle this access control with access control lists and by dedicated firewall appliances. Remote Access Systems with strong authentication software control remote dial in users to the network. A firewall provides a barrier to traffic crossing a network's "perimeter" and permits only authorised traffic to pass, according to a predefined security policy. Complementary tools, including virus scanners and content filters, also help control network perimeters. Firewalls are generally the first security products that organisations deploy to improve their security postures.

### 8.3. Secure Connectivity

Signposts will protect confidential information from eavesdropping or tampering during transmission.

### 8.4. Security Monitoring

Network vulnerability scanners will be used to identify areas of weakness, and intrusion detection systems to monitor and reactively respond to security events as they occur.

### 8.5. Remote diagnostic services and 3rd parties

8.5.1. Suppliers of central systems/software expect to have dial up access to such systems on request to investigate/fix faults. Signposts will permit such access subject to it being initiated by the computer system and all activity monitored.

8.5.2. Each supplier or Signposts user requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified representatives.

8.5.3. Each request for dial up access will be authorised by approved computer services staff, who will only make the connection when satisfied of the need. The connection will be physically broken when the fault is fixed/supplier ends his session.

### 8.6. User Responsibilities, Awareness & Training

Signposts will ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. Irresponsible or improper actions may result in disciplinary action(s).

## 9. System Change Control

All changes to systems must be authorised by the **ICT Support Providers**.

## **10. Reporting Security Incidents & Weaknesses**

All security weaknesses and incidents must be reported to the **ICT Support Providers** through the IT Helpdesk – **01524 732807**

## **11. Guidelines and training**

The **ICT Support Providers** will produce written guidance and training materials for all remote access users.

## **12. Validity of this Policy**

This policy should be reviewed annually under the authority of the Chief Executive. Associated information security standards should be subject to an on going development and review programme.

Chief Executive  
September 2011