Document Control

Policy Title	3rd Party Access to Sunbeam House Services Network Data Policy
Policy Number	082
Owner	Information & Communication Technology Manager
Contributors	Information & Communication Technology Team
Version	1.0
Date of Production	01 October 2014
Review date	01 October 2016
Post holder responsible for review	Information & Communication Technology Manager
Primary Circulation List	Shared Drive
Web address	n/a
Restrictions	None

Version Control

Version Number	Owner	Description	Circulation
1.0	Information & Communication Technology Manager	Review	SMT

1.0 POLICY:

This policy defines third party access to Sunbeam House Service's (SHS) Network and Data.

2.0 SCOPE:

This policy represents SHS's position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

- All SHS ICT resources which include equipment, systems, and applications including cloud based applications.
- All users, and uses of SHS ICT resources;
- All connections to (locally or remotely) SHS network (Local Area Network (LAN)/Wide area network (WAN))

3.0 ROLES & RESPONSIBILITIES:

3.1 Users

Each user of SHS's ICT resources is responsible for:-

3.1.1 Complying with the terms of this policy and all other relevant SHS policies procedures, regulations and applicable legislation.

4.0 GUIDELINES:

4.1 Access to the SHS's network will only be granted to external parties for the maintenance of specific systems or services for which they are responsible, or to enable them to utilise or contribute to specific SHS services under specific agreement.

4.2 SHS will restrict access to its network to the specific IP address(es) of the external parties' machine(s) wherever possible.

4.3 Each external party who is granted access to SHS network is responsible for providing the IP address (es) of the machine(s) that they require to access SHS network from, and for notifying SHS of any subsequent changes to these.

4.4 External parties must not access SHS network for any purpose other than that/those for which they have been granted access, and only at times when such access is necessary for the intended purpose.

4.5 All software used by external parties when accessing SHS network or systems or services, or operating upon their own systems that are hosted at SHS, must comply fully with all licensing conditions.

4.6 Whist accessing SHS network external parties must not attempt to navigate systems or services, or areas of the network away from the system or services to which they have been given access.

4.7 Access to SHS network, systems, or services by external parties is restricted to the external parties' employees (or contracted staff working under a formal contract of employment) who are qualified and sufficiently competent to undertake the work.

4.8 Should an external party identify any perceived security risk or vulnerability on SHS's network or whilst accessing SHS systems or services they must not try to prove the weakness or exploit the vulnerability.

4.9 Any identified or perceived security risk or vulnerability that is stumbled upon must be reported to the ICT Manager.

4.10 All external parties who are granted access to SHS network, systems, or services must maintain effective security of the computer(s) they use for such access and ensure that security patches and anti-virus software on them is fully up to date.

4.11 Data that is the intellectual property of SHS must not be copied, deleted, modified, or removed by any third party without the express permission of SHS.

4.12 All access to SHS network or systems or services hosted upon it must be in accordance with the law and must comply fully with all legal requirements.

4.13 All usage of SHS network or systems or services hosted upon it must comply fully with SHS's Acceptable Usage Policy.

4.14 SHS reserves the right to monitor and log all access to its network, systems or services (as allowed by law) by any external party at any time.

4.15 External parties must not install (or have installed) any peer to peer (P2P) software on machines connected to SHS network without first obtaining ICT Manager permission.

4.16 External parties must not use SHS resources for the promotion or enhancement of their systems or services without first obtaining formal SHS consent.

4.17 External parties must not undertake any activity that is detrimental to the performance of SHS network or systems or services attached to it.

5.0 ENFORCEMENT

5.1 SHS reserves the right to take such action as it deems appropriate against users who breach the guidelines of the policy

5.2 Breaches of this policy by a third party, may lead to the withdrawal of SHS information technology resources to that third party and/or the cancellation of any contract(s) between SHS and the third party.

5.3 SHS will refer any user of its ICT resources for illegal activities to the appropriate law enforcement agencies.