Document Control

Policy Title	Internet Content Policy
Policy Number	096
Owner	Information & Communication Technology Manager
Contributors	Information & Communication Technology Team
Version	1.0
Date of Production	28 April 2015
Review date	28 April 2017
Post holder responsible for review	Information & Communication Technology Manager
Primary Circulation List	Shared Drive
Web address	None
Restrictions	n/a

Version Control

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

1.0 POLICY:

The purpose of this Internet Content Filtering Policy is to define the acceptable use of Sunbeam House Services (SHS) internet services and describe which categories of internet content are accessible to SHS employees and service users and which are filtered (blocked).

This policy is mandatory and by accessing internet content from any Information Communication Technology (ICT) resources which are owned or leased by the SHS, users are agreeing to abide by the terms of this policy.

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

3.0 FILTERED INTERNET CONTENT

For the purpose of managing internet access, internet sites are grouped together into a number of categories and subcategories depending on the content that each site offers.

SHS reserves the right to filter and block selected categories of internet content that it considers inappropriate, or where access to such categories could lead to legal, security or operational issues.

The following categories/sub-categories of internet content are currently filtered and blocked by SHS:

- Adult Material
    - Sex
    - Nudity
    - Adult Content
- Peer-To-Peer File Sharing
- Gambling
- Illegal or Questionable
- Hacking
- Proxy Avoidance

- URL Translation
- Web Hosting
- Web and Email Spam
- Military & Extremist
- Productivity PG
- Racism & Hate
- Violence
- Weapons

Though every effort is made to block illegal and inappropriate internet content there is an onus on every user not to access this content whether or not its blocked.

4.0 ROLES & RESPONSIBILITIES:

4.1 Users

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

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

4.1.2 Respecting and protecting the privacy and confidentiality of the information they process at all times.

4.1.3 If a user needs access to a site that is blocked by the internet filtering software that they need access to, they then need to email their Senior Manager seeking approval to gain access to that site.

4.1.4 Complying with instructions issued by the ICT Manager on behalf of SHS.

4.1.5 Reporting all misuse and breaches of this policy to their Senior Manager.

4.2 Senior Managers

In addition to each user's responsibilites, Senior Managers are directly responsible for:-

4.2.1 The implementation of this policy and all other relevant SHS policies within the business areas for which they are responsible.

4.2.2 Ensuring that all SHS employees who report to them are made aware of and are instructed to comply with this policy and all other relevant SHS policies.

4.2.3 When they receive a request from an individual to access a site that is blocked that they consider the request with the ICT Manager, if approved the ICT Manager will provide access to that site.

4.2.4 Consulting with the ICT Manager in relation to the appropriate procedures to follow when a breach of this policy has occurred.

4.3 ICT System Administrators & Developers

Each SHS System Administrator & Developer is responsible for:-

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

4.3.2 Complying with instructions issued by the ICT Manager on behalf of SHS.

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 cancelleation 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.