ICT Acceptable Use Policy - Residents

1. Purpose & Scope

1.1. The purpose of this policy is to outline the acceptable and unacceptable use of computer equipment and online services provided to residents and other service users by Stoll.

1.2. These rules are in place to protect Stoll residents and the organisation. Inappropriate use exposes Stoll and other users to risks including virus attacks, compromise of network systems and services and legal issues. It can also upset other users of the facility.

1.3. This policy applies to all residents and their visitors and other authorised users of the Stoll IT Services. It also applies to all equipment that is owned or leased by Stoll and to all equipment connected to Stoll's networks including residents' own devices.

1.4. Stoll is mindful of the need to ensure proper use and adequate security in order to protect our residents, systems and data, and to comply with legislation such as the Data Protection Act 1998; the Human Rights Act 1998; the Telecommunications Act 1984; the Obscene Publications Act 1959; the Protection of Children Act 1987; the Criminal Justice Act 1988 and the Protection from Harassment Act 1993.

2. Objectives

2.1. This policy will enable Stoll to:

- comply with the law in respect of the access to IT;
- follow good practice;
- protect Stoll's tenants, staff, volunteers, supporters and other individuals;
- protect the organisation from the consequences of a breach of its responsibilities.

2.2. Stoll will:

- comply with both the law and good practice;
- respect individuals' rights;
- provide training and support for residents and other authorised users so that they can act appropriately.

2.3. All authorised users are required to read, understand and accept any policies and procedures that relate to the acceptable use of IT. Residents who contravene this policy may find themselves subject to restrictions to the IT services provided by Stoll. Individuals may also be subject to criminal proceedings.

2.4. Stoll reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

3. Definitions

3.1. Authorised users

Use of Stoll equipment and the Stoll network are limited to Residents, their families and authorised third parties only. Under no circumstances should any person not included in the above list be allowed to access the Stoll network.

3.2. Unacceptable use

Unacceptable use of Stoll computers and network resources may be summarised as, but not restricted to:

- Actions which cause physical damage to any ICT hardware and software, including peripherals (eg mouse, cables, wiring, printers).
- Accessing, creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate.
- Threatening, bullying, intimidating or harassing staff, residents or others.
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights.
- Defamation.
- Unsolicited advertising, often referred to as "spamming".
- Sending emails that purport to come from an individual other than the person actually sending the message using, e.g. a forged address.
- Attempts to break into or damage computer systems or data held thereon.
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, e.g. use of equipment which is inadequately protected against viruses and spyware.
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised.
- Using the Stoll network for unauthenticated access.
- Unauthorised resale of Stoll services or information.
- Using the ICT facilities for carrying out any illegal trading activity.
- Any other conduct which may discredit or harm Stoll, its staff and residents or the ICT facilities.

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy:

- Interfering with data or settings in another person’s network account.
- Users must not deliberately visit, view, download, print, copy, forward or otherwise transmit any unlawful material or that which is likely to cause offence.
- The downloading, distribution or storage of music, video, film or other material for which you do not hold a valid licence or other valid permission from the copyright holder.
- The distribution or storage by any means of pirated software.
- Connecting an unauthorised device to the Stoll network, ie one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, purchasing policy and acceptable use.
- Circumvention of network access control.
- Monitoring or interception of network traffic without permission.
- Probing for the security weaknesses of systems by methods such as port-scanning without permission.
- Associating any device to network Access Points, including wireless, to which you are not authorised.
- The use of portable media for the purpose of copying unlicensed copyright software, music, etc.

If you mistakenly access such material you should notify Stoll. In the event of any use that could be regarded as giving rise to criminal proceedings, Stoll may inform the police or other law enforcement agency. You should be aware that you will be held responsible for any claims brought against Stoll. Other uses may be unacceptable in certain circumstances.

4. Policy Content

4.1. Use of Stoll's IT services is conditional upon acceptance of this Acceptable Use Policy, for which a signature of acceptance is required. The lack of a signature does not exempt an individual from any obligation under this policy.

4.2. All allocated access codes, usernames and passwords are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username should not be divulged to any other person. Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.

4.3. Stoll reserves the right to monitor use of IT services provided. Reasons for such monitoring include the need to:

- Investigate or detect unauthorised use of the Stoll's telecommunications systems and ensure compliance with this policy or other policies.
- Ensure operational effectiveness of services (eg to detect viruses or other threats to the systems).
- Prevent a breach of the law or investigate a suspected breach of the law, Stoll's policies and contracts.
- Monitor standards and ensure effective quality control.

Where abuse is suspected (especially criminal activity), Stoll may conduct a more detailed investigation involving further monitoring and examination of stored data held on servers/disks/drives or other historical/archived data. Where disclosure of information is requested by the police (or another law enforcement authority), the request where possible will be handled by Stoll's Safeguarding Officer or other appropriate senior person.