Vale of Glamorgan Council (VoG)
ICT Code of Conduct & Statement

All Library Volunteers will be expected to act in a reasonable manner when using the ICT Systems provided and to abide by the principles outlined below.

There are a number of legislative conditions that apply as follows:-

- **Data Protection Act 1998 (DPA).** In general this Act requires that all personal data relating to other living persons with the exception of personal data held by an individual for domestic and recreational purposes should not be stored by any person on a computer system unless the data is suitably registered.

- **Obscene Publications Act, 1959.** Placing material on the Council's computing facilities in such a way that several people can access it constitutes its publication. Under the Obscene Publications Act and the Criminal Justice Act, it is a criminal offence to publish material that is obscene. Material is defined as obscene if its effect is to deprave and/or corrupt individuals.

- All use of Council ICT systems, networks and devices is monitored and audit trails and logs kept. This includes use of email, the internet, all ICT services and removable media such as USB memory ‘sticks’.

- Authorised Officers of the Council may carry out audit checks at any time on any ICT service or device.

- ICT services must not be used for personal use or any activity not authorised as part of a volunteer’s job description. Computer services, including processing time; network capacity; email; printing capacity etc.; must not be wasted by unnecessary activity.

Emails

- Email messages, both internal and external, are a form of written communication and the use of email is subject to the same legal obligations. Volunteers must not use email to:
- Advocate any political or religious cause
- Make comments against any race, religion or sex
- Make comments which could be construed as sexual harassment
- Make comments which could be considered derogatory or defamatory
- Make comments that could misrepresent the Council or the Community Library
- Make personal comments that could be interpreted as libellous
- Email may be legally binding; volunteers must make sure they have gone through the proper channels before making any commitments on behalf of the Library.

System Access VSMART (and any other IT library management software systems)

- All authorised volunteers will be provided with a generic network logon and other system access as required specifically for their job role.

- Volunteers must not divulge their user logon account details, including user IDs and passwords to anyone else.

- Workstations must be locked when being left unattended even for a few minutes. Press CTRL, ALT and DEL and select Lock, or press the Windows Flag key and letter ‘L’.

Network Security

- To maintain the security, integrity and availability of the Corporate network, all users must comply with the following mandatory requirements.
- Personal or non-Council provided equipment MUST NOT be plugged into the Corporate network under any circumstances. This includes, but is not limited to: PCs, Laptops, tablets, smartphones, CD/DVD writers, USB pens/sticks/dongles, cameras, scanners, printers or other hardware not requested and procured through ICT Services.
- The Council has implemented a USB monitoring system which records all USB activity and can block access to unauthorised USB devices.
- Users must not attempt to download and install software onto any corporate device or attempt to install software using removable media such as USB memory sticks, CDs or DVDs. This includes games, music, screen savers, programs, magazine CDs/DVDs, obscene, pornographic material or any material which may contain improper language or any distasteful content and images from the Internet or illegal copies of software.
- Users must not try to circumvent, bypass, reconfigure or otherwise disable the security settings, anti-virus or other software installed on Corporate devices including PCs, laptops and tablets.
- Users must not try to circumvent, bypass, reconfigure or otherwise change the set up or installation of any corporate device.

Information Security

- Users must not remove Council information from the network and copy it to personal or non-Council owned equipment. This introduces a serious information loss and malware risk.
- Users must not copy Council information to removable media.
- Users must not disconnect, move or otherwise tamper with corporate devices or peripherals.
- Licensed software will be installed by ICT Services. Volunteers must not attempt to install or re-install licensed software.
- All original software licences and media will be held by ICT Services.

I agree to abide by the VoG ICT Code of Conduct as described above.

Signed…………………………………………… Date……………………………………..