1. ABOUT THIS POLICY

1.1 We offer two distinct internet access services to our residents, which together are called "**Internet Access**". They are:

1.1.1 Use of our fixed computer terminals ("**Terminal**") provided by us (such use being "**Terminal Use**"); and

1.1.2 Use of your own device(s) on our Wifi network (such use being "**Device Use**").

Each time you use Internet Access, whether by Terminal Use or Device Use, you are deemed to have agreed to comply with this policy during such use. It is therefore important that you read this policy carefully to ensure that you fully understand it.

1.2 This policy outlines the standards you must observe when using Internet Access, when we will monitor such use, and the action we will take if you breach this policy.

1.3 The Senior Management Team has overall responsibility for this policy, including keeping it under review. Please contact them if you have any questions or concerns regarding this policy.

1.4 Breach of this policy may lead to restrictions on, or removal of, your Internet Access, as we in our sole discretion deem appropriate. Clause 7 deals with this topic in additional detail.

2. REGISTERED DEVICES, SECURITY AND PASSWORDS

2.1 Where you wish to use your own device for Device Use, you should notify the Registered Manager. They will review the request, and provided they deem it appropriate, will issue you with a code to access the Wifi system using that device (which shall be known as a "**Registered Device**").

2.2 You are responsible for the security of each Registered Device that you own or possess, and you must not allow it to be used for Internet Access by

anyone else except under your direct supervision. You will be responsible for all such use as if you were using the Registered Device yourself.

2.3 You should use passwords on all Registered Devices. You should keep your passwords confidential and change them regularly.

2.4 You must only engage in Device Use using your own Registered Device. You must not use another resident's Registered Device or allow another resident to use your Registered Device.

2.5 You must not connect (or attempt to connect) to our Wifi with any device unless it has become a Registered Device.

2.6 When you first express an interest in Terminal Use, you will be provided with a password to do so ("**Password**"), so long as we do not feel that there is a legitimate reason to restrict or prevent your Internet Access. This Password is personal to you, and must not be shared with or disclosed to another resident, or any other third party.

2.7 If another resident or a third party engages in Terminal Use using your Password, then you will be responsible for their actions during such Terminal Use. It is therefore important that, if you leave the Terminal even for a short time, you log out from it.

3. SYSTEMS AND DATA SECURITY

3.1 You must not move or tamper with a Terminal, or any associated equipment, cabling etc. This could cause serious injury to you or another person, or significant damage to property.

3.2 You should not delete, destroy or modify existing systems, programs, information or data on or relating to a Terminal.

3.3 You must not download or install software from external sources to a Terminal under any circumstances. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

3.4 You must not attach any device or equipment, including mobile phones, tablet computers or USB storage devices to a Terminal. Any attempt to do so will constitute a breach of this policy.

3.5 We monitor all e-mails passing through our system. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an email looks suspicious do not reply to it, open any attachments or click any links in it.

3.6 Inform the Registered Manager immediately if you suspect that a Registered Device or Terminal may have a virus.

3.7 You must not attempt to gain access to any restricted areas of our networks or Terminals.

4. EMAIL

4.1 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails. By engaging in Internet Access, you irrevocably consent to us sharing any information which we may have with the police or other appropriate bodies with reference to conduct of this nature.

4.2 You must not:

4.2.1 download or email text, music or other content on the internet which is subject to copyright protection, unless it is clear that the owner of such work allows this;

4.2.2 engage in any illegal or unethical activity whatsoever via Internet Access; or

4.2.3 send messages from another person's email address or under an assumed name.

4.3 It is common for criminals to send emails in which they purport to be someone whom they are not. For example, they may pretend to be a

representative of your bank or building society, and request that you confirm your account details to them. If you receive any email which you are suspicious about, or which asks you for account details, passwords or other private information, then please do not reply to it. If you give out private details or information whilst engaging in Internet Access, then we will not accept any liability whatsoever under any legal theory (including without limitation negligence) for your resulting losses (or those of any third party).

5. USING THE INTERNET

5.1 Internet Access is provided at our discretion as a benefit to residents, and does not form part of your contractual entitlement as a resident. Internet Access is not part of the consideration from us for the payment of any fees applicable to your status as a resident.

5.2 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

5.3 We may block or restrict access to some websites at our discretion.

6. MONITORING

6.1 Our systems enable us to monitor email, internet and other communications. For legal reasons, and in order to carry out legal obligations in our role as a service provider, your Internet Access may be continually monitored by automated software or otherwise.

6.2 We reserve the right to retrieve the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

6.2.1 to monitor whether the Internet Access is legitimate and in accordance with this policy;

6.2.2 to find lost messages or to retrieve messages lost due to computer failure;

6.2.3 to assist in the investigation of alleged wrongdoing; or

6.2.4 to comply with any legal obligation.

6.3 We do not accept any duty of care to actively monitor Internet Access to protect residents or third parties. You engage in Internet Access at your own risk.

7. PROHIBITED USE OF OUR SYSTEMS

7.1 Misuse or excessive/inappropriate use of Internet Access (together, "**Misuse**") will be dealt with at the discretion of the Registered Manager and/or the Senior Management Team. Misuse can in some cases be a criminal offence.

7.2 In the event of any Misuse, or any other breach of this policy, at our discretion we may do one or more of the following:

7.2.1 issue you with advice and/or a warning regarding your future use of Internet Access;

7.2.2 temporarily suspend your Internet Access; or

7.2.3 permanently terminate your Internet Access.

7.3 For the avoidance of doubt, the above is not a “three strikes” or cumulative system of sanctions. In any event of Misuse, we may at our discretion elect to take any of the actions specified in clauses 7.2.1 to 7.2.3 inclusive.