REMOTE WORKING POLICY

1. POLICY STATEMENT

Streetlight UK provides users with the facilities and opportunities to work remotely as appropriate. Streetlight UK will ensure that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.

2. PURPOSE

The purpose of this document is to state the Remote Working and working from home policy of Streetlight UK.

In some cases Portable computing devices are provided to assist users to conduct official Streetlight UK business efficiently and effectively. This equipment, and any information stored on portable computing devices, should be recognised as valuable organisational information assets and safeguarded appropriately.

3. SCOPE

This document applies to all Employees, volunteers and Trustees of Streetlight UK, contractual third parties and agents of Kingdom Faith who use Streetlight UK IT facilities and equipment remotely, or who require remote access to Streetlight UK Information Systems or information.

4. DEFINITION

This policy should be adhered to at all times whenever any user makes use of portable computing devices. This policy applies to all users' use of Streetlight UK IT equipment and personal IT equipment when working on official Streetlight UK l business away from Streetlight UK premises (i.e. working remotely).

Portable computing devices include, but are not restricted to, the following:

- Laptop computers.
- Tablet PCs.
- PDAs.
- Mobile phones.
- Text pagers.
- Wireless technologies

5. RISKS

Streetlight UK recognises that there are risks associated with users accessing and handling information in order to conduct official Streetlight UK business. The mobility, technology and information that make

portable computing devices so useful to employees and organisations also make them valuable prizes for thieves. Securing PROTECT or RESTRICTED data when users work remotely or beyond Streetlight UK network is a pressing issue – particularly in relation to the Streetlight UK's need as an organisation to protect data in line with the requirements of the Data Protection Act 1998.

This policy aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to PROTECT and RESTRICTED information.
- Unauthorised introduction of malicious software and viruses.

Non-compliance with this policy could have a significant effect on the efficient operation of Streetlight UK and may result in financial loss and an inability to provide necessary services to our service users.

6. APPLYING THE POLICY

All IT equipment (including portable computer devices) supplied to users is the property of Streetlight UK. It must be returned upon the request of Streetlight UK. Access for ICT Services staff shall be given to allow essential maintenance security work removal or retrieval of documents, upon request.

All IT equipment will be supplied and installed by Wessex IT Service staff. Hardware and software must only be provided by them.

7. USER RESPONSIBILITY

It is the user's responsibility to ensure that the following points are adhered to at all times:

- Users must take due care and attention of portable computer devices when moving between home and another business site.
- Users will not install or update any software on to Streetlight UK owned portable computer device.
- Users will not install any screen savers on to a Streetlight UK owned portable computer device.
- Users will not change the configuration of any Streetlight UK owned portable computer device.
- Users will not install any hardware to or inside any Streetlight UK owned portable computer device, unless authorised by Wessex ICT department.
- Users will allow the installation and maintenance of Wessex installed Anti-Virus updates immediately.
- Users will inform the IT Helpdesk of any Streetlight owned portable computer device message relating to configuration changes.
- Business critical data should be stored on a Streetlight UK file.
- All faults must be reported to the IT Helpdesk.
- The IT equipment can be used for personal use by staff so long as it is not used in relation to an external business. Only software supplied and approved by Streetlight UK can be used (e.g. Word, Excel, Adobe, etc.)
- No family members may use the IT equipment. The IT equipment is supplied for the staff members' sole use.
- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, Streetlight UK may recover the costs of repair.
- Streetlight UK may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

- Any authorized user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to copy or hold any Streetlight UK files on personal laptops, tablets, mobile devices and non-streetlight UK equipment. Including information of, or from the database, or carry out any processing of information, all of which is PROTECTED and RESTRICTED information relating to Streetlight UK, its employees, volunteers, trustees or service users.

8. REMOTE AND MOBILE WORKING ARRANGEMENTS

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use.

Users must ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times. All removable media devices and paper documentation must also not be stored with the portable computer device.

Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read.

9. ACCESS CONTROLS

It is essential that access to all PROTECTED or RESTRICTED information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all PROTECTED or RESTRICTED data held on the portable device must be encrypted.

10. ANTI VIRUS PROTECTION

Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least once every two weeks to enable the Anti-Virus software to be updated.

11. USER AWARENESS

The user shall ensure that appropriate security measures are taken to stop unauthorized access to PROTECTED or RESTRICTED information, either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as Streetlight UK itself.

12. POLICY COMPLIANCE

If any user is found to have breached this policy, they may be subject to Streetlight UK disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the CEO of Streetlight UK Helena Croft.

13. REVIEW AND REVISION

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Key Messages:

- It is the user's responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention when moving portable computer devices.
- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- It is the user's responsibility to ensure that access to all PROTECTED or RESTRICTED information is controlled – e.g. through password controls.
- All PROTECTED or RESTRICTED data held on portable computer devices must be encrypted.