Adopted: 25th April 2017

REMOTE WORKING POLICY

INTRODUCTION

AUKCAP & Peterborough (AUKCAP) will where considered appropriate, provide users with the facilities and opportunities to work from remote locations. All users who work remotely must ensure they are aware of the acceptable use of computers and laptops and any other information technology (IT) equipment. In this policy the term "PC" will be used to mean "personal computer" and will include desktop, laptop or any other similar computer equipment as well as "memory sticks".

PURPOSE

The purpose of this document is to state the Remote Working policy of AUKCAP.

PCs are provided to assist users to conduct official AUKCAP business efficiently and effectively. The equipment, and any information stored on it, should be recognised as valuable and sensitive organisational Service User information safeguarded appropriately.

SCOPE

This document applies to all AUKCAP users i.e. employees, trustees, volunteers, and associated partners, contractual third parties and agents who use AUKCAP IT facilities and equipment remotely, or who require remote access to AUKCAP Information Systems or information.

DEFINITION

This policy should be adhered to at all times whenever any user makes use of PCs. This policy applies to all users of AUKCAP IT equipment and personal IT equipment when working on official company business away from AUKCAP premises (i.e. working remotely).

RISKS

AUKCAP recognise that there are risks associated with users accessing and handling information in order to conduct official business. The mobility, technology and information that make portable computing devices so useful to users and organisations also make them valuable prizes for thieves. Securing PROTECTED or RESTRICTED data when users work remotely or beyond the AUKCAP network, is a pressing issue – particularly in relation to AUKCAP's need, as an organisation, to protect data in line with the requirements of the Data Protection Act 1998 and AUKCAP Confidentiality Policy.

This policy aims to mitigate the following risks:

- Unauthorised access to PROTECTED and RESTRICTED information.
- Increased risk of equipment damage, loss or theft.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised introduction of malicious software and viruses.
- Potential sanctions against AUKCAP or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against AUKCAP or individuals as a result of information loss or misuse.
- Damage to AUKCAP's reputation as a result of information loss or misuse.

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

APPLYING THE POLICY

All IT equipment supplied to users remains at all times the property of AUKCAP.

Equipment must be returned at the request of AUKCAP.

All IT equipment will be supplied and programmed by AUKCAP.

Software **must only** be provided by AUKCAP.

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 PCs when moving between office, home and any remote location.

- Users will not install or update software to any company owned PC.

- Users will not install any screen savers on to a company owned portable computer device.

- Users will not change the configuration of any company owned portable computer device.

- Users will not install any hardware to or inside any company owned PC, unless authorised by IT Manager..

- Users will allow the installation and maintenance of AUKCAP's installed Anti Virus updates immediately upon request.

- Users will inform IT Manager of any AUKCAP owned PC message relating to configuration changes.

- Business critical data should be stored on an AUKCAP file and print server wherever possible and not held on the PC.

- All faults must be reported to Complete IT.

- Users must not remove or deface any asset registration number.

- User registration must be requested from IT Manager. Users must state which applications they require access to.

- The Line Manager must approve user requests for upgrades of hardware or software. Equipment and software will be purchased and installed by the appointed IT Service Provider.

- The IT equipment may be used for personal use by staff so long as it is not used in relation to external businesses and use is in line with AUKCAP's IT Policy. Only software supplied and approved by AUKCAP can be used (e.g. Word, Excel, Adobe,etc.)

- The IT equipment is supplied for the user's sole use in the course of their work for AUKCAP and for occasional personal use in line with AUKCAP's IT Policy.

- The user must ensure that reasonable care is taken of the IT equipment supplied. In transit, laptops will be stored in the locked boot of the vehicle if it is necessary to leave unattended.

- AUKCAP may at any time, and without notice, request a software and hardware audit, and may remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

- Any user who is permitted 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 hold any database, or carry out any processing of PROTECTED or RESTRICTED information relating to the AUKCAP, its users, or clients. **Under no circumstances** should PERSONAL or RESTRICTED information be emailed to a private non AUKCAP email address.

- Permission for work at home shall be obtained from the Line Manager.

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. Equipment must be secured whenever it is not in use. If left in an unattended vehicle, equipment will be locked in the boot out of sight.

Users must ensure that personal identification numbers and passwords are kept in a separate location to the portable computer device at all times. All removable media devices and paper documentation must not be stored with the portable computer device. A list of all passwords and user names will be supplied to the IT Manager.

Paper documents are vulnerable to theft, these should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Sensitive documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing PROTECTED or RESTRICTED information must be shredded.

ACCESS CONTROLS

It is essential that access to all PROTECTED or RESTRICTED information is controlled. This can be done through physical controls, such as ensuring that documents and removable media devices are held securely or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls. (see also above)

PCs 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 device must be password protected.

ANTI VIRUS PROTECTION

Anti Virus software will be installed by an AUKCAP approved supplier. No other anti virus software is to be installed unless approved by IT Manager. Users who work remotely must ensure that their PCs are connected to the corporate network at least once every week to enable the anti virus software to be updated.

USER AWARENESS

All users must comply with appropriate codes and policies associated with the use of IT equipment. This includes the following:

- IT Policy
- Record keeping Policy

It is the users' responsibility to ensure their awareness of and compliance with these.

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

POLICY COMPLIANCE

If any user is found to have breached this policy, they may be subject to disciplinary procedures. 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 your line manager.

POLICY GOVERNANCE

The following table identifies who within AUKCAP is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.

- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Board, Chief Executive
Accountable	IT Manager
Consulted	Complete IT/Aldex
Informed	All

REVIEW AND REVISION

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years.

Policy review will be undertaken by the Board.

REFERENCES

The following AUKCAP policy documents are directly relevant to this policy, and are referenced within this document:

- IT Policy
- Record Keeping Policy

The following AUKCAP policy documents are indirectly relevant to this policy:

- Lone Worker
- Risk Management

KEY MESSAGES

- It is the user's responsibility to use computer equipment in an acceptable way. This includes not installing software, taking due care and attention when moving computer devices and not emailing PROTECTED or RESTRICTED information to a non-AUKCAP email addresses.
- 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, if not possible, password protected.

REMOTE ACCESS AND HOME WORKING

The Chief Executive, Senior Management Team and approved project staff will have remote access. This will enable staff to organise time effectively, for example by accessing e-mails from home early in the day prior to a local appointment without the necessity to travel to the office to deal with routine correspondence. However, it is

important to note that this is not permission for ‘home working’ and care must be taken to ensure that offices and centres are staffed during core opening hours.

Requests for remote access and/or home working will be considered on a case by case basis on the merits of each request.

Staff using remote access may use personal equipment or AUKCAP mobile devices and should refer to AUKCAP’s IT and Electronic Comms Policy. Under no circumstances shall sensitive and confidential AUKCAP information be held on personal equipment.

Special care and consideration must be given when files are transported on memory sticks or similar devices.

Reviewed: