POLICY AND CODE OF PRACTICE ON THE
USE OF COMPUTERS, IT AND SOCIAL MEDIA NETWORKS

PURPOSE
Age UK Cambridgeshire & Peterborough (AUKCAP) encourages the use of IT equipment and electronic communications. However equipment and electronic communications must be used in a proper manner and in accordance with this policy or other instructions issued by a senior manager. Misuse could result in disciplinary action. These guidelines apply to all users at AUKCAP. "User" refers to any person working for AUKCAP or associated companies either as employees, contracted persons or recognised volunteers. This Policy applies to the use of IT equipment, email, discussion groups, social media and the internet.

Computers
Information technology including computers, laptops, e-mail and internet are important tools to help Age UK Cambridgeshire & Peterborough (AUKCAP) in its work with older people. This document provides clear rules and guidelines on the use of information technology,

Social Media
Whilst we believe the use of a social networking site is a personal preference and the content personal to the member of staff/volunteer, there are standards of conduct to be observed to protect AUKCAP's legitimate business and its employees/volunteers from the dangers of inappropriate use.

This policy document is set out in four sections as follows:
Section 1 – Computers
1.1   Use of the system
1.2   Back-up
1.3   Virus protection
1.4   Passwords
1.5   Software
1.6   Drives
1.7   Permissions
1.8   Remote Access
1.9   Equipment

Section 2 – E-mail
2.1   Sending E-mail
2.2   Checking messages
2.3   Unsolicited e-mail
2.4   Ownership
2.5   Copyright
2.6   Standard Confidentiality notice
2.7   Representation
2.8   Interference

Section 3 – Internet
3.1   Virus protection
3.2   Excessive use
3.3   Monitoring

3.4 Restrictions and personal use including live television.

Section 4 – Social Media networks
4.1 What is social networking?
4.2 Profile information
4.3 Use of Social Networking Sites

Section 1 – Computers
1.1   Use of the system
All users must use the system in a manner that preserves the privacy of others. Actions which interfere with the integrity of the system are not permitted and may be an offence under the Computer Misuse Act 1990. These include, for example, impersonating others, making unauthorised changes to systems that interfere with other people's computer use, and altering or destroying computer programs belonging to others.

1.2   Back-up
All computers connected to the server based at County Office and The Lindens are backed up daily. Services operating using remote access via the Microsoft remote access portal are also using the server, and their work will be backed up. Anyone NOT using this method should ensure all their work is backed up daily. Seek guidance if necessary. Back up tapes used for this purpose must be stored off-site.

1.3   Virus protection
AUKCAP is protected against known viruses imported by e-mail received at the Lindens office and County Office. This protection is updated regularly by Complete I.T., *(AUKCAP's outsourced IT specialists.)*
If a virus warning is received:
- Do not open or send any e-mails until the system is cleared of all viruses.
- Never forward any virus warnings electronically. Most messages asking to be copied to everyone you know are in fact hoax viruses.
- If you have information about a virus that is attacking us or colleagues, please pass this on to the Finance & IT Manager or the Chief Executive.

1.4   Passwords
AUKCAP do not encourage the use of passwords on individual documents or files and request that confidential documents are filed in secure drives. If there are circumstances where passwords are used you are responsible to ensure that these remain confidential to yourself and your Manager. If you are concerned about any possible breaches of confidentiality you should pass this on to the Finance & IT Manager or the Chief Executive.

1.5   Software
No software may be loaded on any machine by any means, including downloading from the internet, without the written agreement of the Chief Executive or the Finance & IT Manager. Software may only be used in accordance with its licence. All software must be checked for viruses before it is used for the first time.

1.6   Drives
If you open **My Computer,** you will find various drives.
'C' is the hard disk drive which operates your machine. The AUKCAP system server does <u>not</u> back up any files you create, so do not use 'C' to save your work.

'H' and 'P' are Network Drives, which means that all files and folders are held on the server and backed up daily. You should therefore create and hold nearly all your work on the 'H' drive. Use the 'P' drive only if you have confidential work that you do not wish to share with anyone else.

1.7 Permissions
'H' drive folders and files are generally open to all users, within the following rules:
- All staff/volunteers have **Full Access** to their own files, and **Read-only** access to everything else, apart from specific sensitive data such as HR files – which are protected.
- Managers have **Full Access** to all files of their responsibility.
- Chief Executive, System Administrator and Finance Manager have **Full Access** to all files.
- **Full Access** lets you create/change/archive/delete folders and files.
- **Read-only** lets you look at files but not change them in any way.

1.8 Remote Access
Certain employees are granted remote access enabling them to access AUKCAP's servers from any computer anywhere. The policies set out in this document must be observed on all occasions of such use.

1.9 Equipment
Users are expected to take proper care of IT equipment. In the event of a problem the user should contact Complete IT for support.

Purchase of Equipment can only be authorised by a member of the senior management team. It is our policy to re-use and re-cycle equipment where this is appropriate and as such this will always be the first option. Where new equipment is to be purchased, this will be sourced by the Finance & IT Manager. New equipment will need to be added to the asset register.

De-commissioning: When equipment such as printers and monitors are unserviceable they will be disposed of by users in accordance with current legislation and with reference to AUKCAP's environmental policy. Processing units will be returned to the Lindens or County Office for de-commissioning, prior to disposal by Complete IT.

Section 2 – E-mail
2.1 Sending E-mail
E-mails must be written and sent with the same care as a letter or memo that may be kept and read by persons other than the addressee.

2.2 Checking messages
Check your email inbox frequently (twice a day when possible) and answer queries promptly. Initiate an "out of office" reply to respond to messages when you are away.

2.3 Unsolicited e-mail & SPAM
Treat unsolicited e-mail with caution, and do not without good reason transmit to another person. Delete, without opening any attachments, any messages with no relevance to AUKCAP. If in doubt consult with the Finance & IT Manager or Chief Executive.

2.4 Ownership
All e-mail messages sent/received using the AUKCAP e-mail system and all the

addresses on that system are the property of AUKCAP. AUKCAP will monitor the use of e-mail if there is reason to believe there has been a breach of its policies, unlawful activities or to safeguard AUKCAP's interests.

2.5   Copyright
Do not copy, download or transmit to a third party any copyright materials without the owner's consent. Limitations in the use of materials should be confirmed in writing when work is passed on.

2.6   Standard Confidentiality notice
A standard confidentiality notice must be attached to all outgoing e-mails, as follows:
"This message is confidential. It may not be disclosed to, or used by, anyone other than the addressee, without the consent of the sender. If you receive this message in error, please advise the sender immediately.
Age UK Cambridgeshire & Peterborough is a Registered Charity No. 1165856"

2.7   Representation
Users shall not give the impression that they are representing or otherwise making statements on behalf of AUKCAP or entering into agreements on its behalf unless appropriately authorised (explicitly or implicitly) to do so. All emails shall contain, as a footnote, the company information and authorised disclaimer.

2.8   Interference
Electronic communications shall not be used in ways that could reasonably be expected to cause directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with other's use of electronic communications. Examples include:
- Global emails i.e. indiscriminately mailing large numbers of people. Note that global Emails must only be used in exceptional situations and must be authorised by the Chief Executive.
- Chain letters.

Section 3 - Internet
3.1   Virus protection
Do not download or transmit information from the internet which is known, or can reasonably be expected to have a virus.

3.2   Excessive use
Excessive use of the internet may be considered an unproductive use of time and could result in a warning from your Manager, followed by further action under the disciplinary procedures.

3.3   Monitoring
AUKCAP will monitor the use of the internet.

3.4   Restrictions and personal use
E-mail and the internet are to be used primarily for the business purposes of AUKCAP. As with telephone calls, personal use is not prohibited, but must be kept within reasonable limits. Any such use **must not:**
- Interfere with the user's employment or other obligations to AUKCAP
- Involve sending or saving messages that could bring AUKCAP into disrepute
- Involve sending or saving messages or other material that does not observe personal and professional courtesies.
- Watch live television on the internet. AUKCAP does not possess a television

licence and if fined AUKCAP would expect the individual to pay that fine.

Section 4 – Social Media Networks *(owing to the nature of social media and networking, this policy applies both inside and outside the workplace.)*

4.1 What is social networking?
Social networking web-sites allow registered users to upload profiles, post comments, join "networks" and add "friends." They give registered users the opportunity to form "links" between each other based on friendships, hobbies, personal interests, and business sector or academic affiliations. Social networking sites can be used both personally, to contact friends and find old classmates, and professionally, to look for employment or find someone with whom to collaborate. Most social networking systems are available to all users.

4.2 Profile information
Many social networking sites allow for profile information to be added, such as your marital status, education and employment.
If you choose to include AUKCAP as your employer, you must provide a disclaimer that states "this content reflects my own personal views and does not necessarily reflect the views of AUKCAP." If AUKCAP is referred to then the information posted would need to comply with the conditions outlined in section 4.3.

4.3
- **Use of Social Networking Sites**
- If an employee/volunteer using a social networking site brings the charity into disrepute through comments or actions displayed on the site, it may constitute misconduct or gross misconduct and disciplinary action will be applied.
- An employee/volunteer should not disclose confidential information relating to his/her employment at the charity, its clients or suppliers.
- Employees/volunteers must not post entries or comments on social media and networking sites which are offensive, defamatory, discriminatory, derogatory or otherwise deemed inappropriate or which could bring the charity into disrepute.
- Sites should not be used to verbally abuse other staff/volunteers. Privacy and feelings of others should be respected at all times. You should obtain the permission of colleagues before posting pictures and care should be taken to avoid using language which could be deemed as offensive to others.
- Viewing and updating personal sites should not take place during working hours.
- Sites should not be used for accessing, promoting or sharing illegal content.
- Any misuse of social networking sites that has a negative impact on the charity may be regarded as a disciplinary offence.
- If information on the site raises a cause for concern with regard to conflict of interest or a conflict with the mission and vision of the charity, the issue will be raised by your line manager.
- The charity will monitor its IT systems as is deemed necessary in order to prevent inappropriate usage. Hard copies of any content and social media and networking posts may be used in any disciplinary proceedings.

This policy is designed to work in conjunction and taking account of AUKCAP's Safeguarding policy and procedures.

This policy will be reviewed in 24 months from the date of adoption.