IT AND SOCIAL MEDIA CODE OF PRACTICE

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

SCOPE

This Policy applies to the use of mobile or non-mobile IT equipment (including but not limited to laptops, desktop computers, scanners, mobile devices, collectively known as IT Systems) email, Microsoft Office365, discussion groups, social media, and the internet.

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

Social Media
Whilst we believe the use of social networking sites 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, at all times.

Code of Practice

This document is set out in four sections as follows:
Section 1 – Computers and mobile phones & other Devices
Section 2 – Email
Section 3 – Internet
Section 4 – Social Media networks

Section 1 – Computers

1.1   Remote Access
Should a staff member need to access their MS work account from anywhere else other than their place of work set out in their contract or one of our premises, they must inform their line manager immediately. You will be required to use Multi Factor Authentication (MFA) to access any Age UK Cambridgeshire and Peterborough data and systems.

1.2   Equipment
Users are expected to take proper care of IT equipment. In the event of a problem, the user should contact our Office Co-ordinator via email IT@ageukcap.org.uk If the issue cannot be resolved in house, our Office Co-ordinator will contact ICO Solutions for further advice.

Purchase of Equipment can only be authorised by a member of the Leadership Team. It is our policy to re-use and recycle 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 Office Co-ordinator. New equipment will need to be added to the equipment register.

De-commissioning: When equipment such as printers and monitors are unserviceable, they will be returned to Frans House Office and disposed of in accordance with current legislation and with reference to AUKCAP's environmental policy. Processing units, such as external hard drives and servers, will be returned to the Head Office for de-commissioning, prior to disposal by ICO Systems or any other approved IT recycling company.

1.3   Use of Mobile Phones

Use of mobile phones while driving: The use of handheld mobile phones when driving is not permitted. A hands-free mobile phone may be used as a sat-nav only, provided it is connected to the vehicle's screen or placed in a holder or mount and set up prior to setting off. Calls should not be made or received while driving under any circumstances, including via hands-free devices.

Use of Mobile Phones for work purposes: Staff must not use any mobile phone device to record or share identifiable Service User information on text or Whatsapp or other messaging platforms.

Mobile data usage: staff must be mindful of their data use and regularly check allowance. The use of apps which use data must be limited to reduce the risk of going over data limits.

1.4 Use of Personal Devices: The use of personal devices for work purposes is discouraged, however, on the rare occasion this is unavoidable all users are expected to comply with organisational policies including all security and data protection procedures. This can only be authorised by the CEO as Data Controller for the organisation. Any breaches to this could result in disciplinary action.

Section 2 – Email

2.1 Sending Email
Emails 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 a professional "out of office" reply to respond to messages when you are away.

2.3 Unsolicited email & SPAM

Spam and phishing attempts should be captured by Microsoft 365 Security and kept in quarantine. Treat any unsolicited email that has bypassed security 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 Office Co-ordinator or Deputy CEO or Chief Executive.

2.4 Ownership
All email messages sent/received using the AUKCAP email system and all the addresses on that system are the property of AUKCAP. AUKCAP will monitor the use of email 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-, as follows:
"Age UK Cambridgeshire and Peterborough is a Charitable Incorporated Organisation (CIO) registered with the Charity Commission for England and Wales with registered charity No. 1165856.
This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you receive a message in error, please advise the sender and delete immediately."

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 organisation 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 should be sent to recipients via BCC to prevent large number of all staff replies and breaching GDPR legislation.
- Chain letters.

Section 3 - Internet

3.1 Virus protection
Do not download or transmit information from the internet, which is known to, 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 line 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
Email and the internet are to be used primarily for the business purposes of AUKCAP. As with telephone calls, personal use is not prohibited, unless for safe personal use during breaks. Any such use **must not:**
o Interfere with the user's employment or other obligations to AUKCAP
o Involve sending or saving messages that could bring AUKCAP into disrepute.
o Involve sending or saving messages or other material that does not observe personal and professional courtesies.
o 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 websites 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 service users, 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, unless sharing an AUKCAP post

- 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 regards 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.

REVIEW OF THIS POLICY
This policy will be reviewed every 36 months.

Use of computers, IT & Social Media policy approved: May 2024

Signed by Chair of Trustees: