ICT POLICY

1. Introduction

1.1 Our IT and communications systems are intended to promote effective communication and working practice within our organisation. This Policy (Previously named IT Communications and Monitoring Policy Issue 3) outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take if you breach these standards.

1.2 Misuse of IT and communications systems can damage the business and our reputation. Breach of this policy will be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to dismissal.

1.3 This policy covers all employees, officers, consultants, contractors, volunteers, work placement employees, agency workers and anyone who has access to our IT and communication systems.

1.4 This Policy has been created to:

- ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring;
- protect Age UK Surrey and its employees from the risk of financial loss, loss of reputation or libel, and
- ensure that the facilities do not cause harm or damage to any person or the organisation.

1.5 This Policy applies to the use of:

- local, inter-office, national and international, private or public networks (including the Internet) and all systems and services accessed through those networks;
- desktop computers, laptops and applications;
- telephones, mobile telephones, and
- electronic mail and messaging services;
- remote desktop working via Terminal Server.

1.6 Day-to-day responsibility for operating the policy and ensuring its maintenance and review is the manager in charge of IT. All managers have a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for supporting colleagues and ensuring its success.

2. Computer Facilities - Use Of Computer Systems

2.1 Subject to anything to the contrary in this Policy the facilities must be used for business purposes only.

2.2 In order to maintain the confidentiality of information held on or transferred via

Age UK Surrey's facilities, security measures are in place and must be followed at all times. You will be given a username and password for access to Age UK Surrey's computers. Age UK Surrey reserves the right to override your password and obtain access to any part of the facilities.

2.3 You are responsible for keeping your password secure. You must not give it to anyone, including colleagues, except as expressly authorised by Age UK Surrey.

2.4 Passwords giving access to Age UK Surrey's computers, Finance and Charitylog will be changed every six months.

2.5 You are expressly prohibited from using the facilities for the sending, receiving, printing or otherwise disseminating information that is the confidential information of Age UK Surrey or its clients other than carrying out your duties for Age UK Surrey.

2.6 In order to ensure proper use of computers, you must adhere to the following practices:

- anti-virus software must be kept running at all times;
- all forms of media storage must be checked by the IT department before the contents are accessed or stored on Age UK Surrey's servers or hard drives;
- all files, including those stored on laptops, must be stored on the network drive which is backed up regularly to avoid loss of information;
- always log off or lock your computer before leaving your desk.

2.7 Employees' access to company data is limited, based on departmental need.

3. Software

3.1 Software piracy could expose Age UK Surrey and the user to allegations of intellectual property infringement. Age UK Surrey is committed to following the terms of all software licences to which it is a contracting party. This means, in particular, that:

- software must not be installed onto any of Age UK Surrey's computers unless this has been approved in advance by the IT department who will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer facilities
- software should not be removed from any computer nor should it be copied or loaded on to any computer without the prior consent of the IT department.

4. Laptop Computers or Netbooks

4.1 At various times during your employment with Age UK Surrey, you may use a laptop or netbook. These computers, along with related equipment and software, are subject to all of Age UK Surrey's policies and guidelines governing the non-portable computers and software. However, use of a laptop and netbooks creates additional problems, especially in respect of potential breaches of confidentiality. In order to make remote working more

secure you must comply with the following and the requirements of the 'Mobile Equipment Release Agreement' as issued by the IT department:

- You are responsible for all equipment and software until you return it. The laptop must be kept secure at all times.
- You are the only person authorised to use the equipment and software issued to you.
- You must not load or install files from any sources without inspecting such files for viruses.
- You must password protect confidential data on network drives or media storage to protect against theft. All such passwords should be stored with the IT department.
- If you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the attention of the IT department.
- At the request of Age UK Surrey, at any time, for any reason, you will immediately return any laptop, equipment and all software to Age UK Surrey.
- If you are using your own laptop to connect with Age UK Surrey's servers or to transfer data between the laptop and any of Age UK Surrey's computers you must ensure that you have obtained prior consent of the IT department, comply with instructions and ensure that any data downloaded or uploaded is free from viruses.

5. Email (Internal or External Use)

5.1 Internet email is not a secure medium of communication – it can be intercepted and read. E-mails can be used in legal proceedings so do not use them to say anything you would not wish to be made public. If you are sending confidential information by email this should be sent using password protected attachments or the preferred option of EGRESS which is available to all staff – request a licence from ICT.

5.2 Email should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the email.

5.3 Do not forward email messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.

5.4 Your email inbox should be checked on a regular basis.

5.5 As with many other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

5.6 Use of email facilities for personal use is permitted during your lunch break providing that:

- such emails do not contain information or data that could be considered to be obscene, racist, sexist, otherwise offensive and provided that such use is not part of a pyramid or chain letter; and

- such emails are not used for the purpose of trading or carrying out any business activity other than Age UK Surrey business.

5.7 If you are away from the office and use email as an external means of communication you must ensure that the autoreply service is used to inform the sender that you are unavailable. If you have any doubt as to how to use these facilities please contact the IT department.

5.8 Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the facilities is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

6. Internet

6.1 Use of the internet, or internet services, by unauthorised users is strictly prohibited. You are responsible for ensuring that you are the only person using your authorised internet account and services. You must not share your password with anyone, including our IT team – passwords can be reset if needed.

6.2 Downloading files which are not work related from the internet using the computer facilities is not permitted.

6.3 Viewing, downloading, storing (including data held in RAM or cache) displaying or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

6.4 Posting information on the Internet, whether on a newsgroup, via a chat room or via email is no different from publishing information in the newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the employee making the posting and Age UK Surrey could face legal claims for monetary damages.

6.5 Using the internet for the purpose of trading or carrying out any business activity other than Age UK Surrey business is strictly prohibited.

6.6 Subject to the above you are allowed to use the internet for personal use during your lunch break. Use of the internet for personal use at any other time is strictly prohibited.

6.7 For the avoidance of doubt the matters set out above include use of mobile phones on personal business other than emergency matters.

7. Monitoring Policy

7.1 There should be no assumption of privacy when using a work computer network that you do not own.

7.2 Age UK Surrey reserves the right to monitor employees' use of the facilities. We may adopt at any time a number of methods including:

- recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones) - such recording may include details of length, date and content.
- recording and logging the activities by individual users of the facilities - this may include opening emails and their attachments, monitoring internet usage including time spent on the internet and web sites visited
- physical inspections of individual users' computers, software and telephone messaging services
- physical inspection of an individual's post
- archiving of any information obtained from the above including emails, telephone call logs and internet downloads.

7.3 Age UK Surrey considers that valid reasons for checking an employee's usage of the facilities include suspicions that the employee has:

- been spending an excessive amount of time on personal telephone calls, sending emails or viewing websites that are not work related, or
- acted in a way that damages the reputation of Age UK Surrey and/or breaches commercial confidentiality.

7.4 Age UK Surrey will not (unless required by law):

- disclose information obtained by such monitoring of the facilities to third parties.

8. Telephones

8.1 Telephones are supplied for business use. If a member of staff or volunteer needs to make an urgent telephone call for personal reasons it is expected that they will pay for the call. A box is held for this purpose by Finance.

9. General Guidance

9.1 Never leave any equipment or data (including client files, laptops, computer equipment, mobile phones etc) unattended on public transport or in an unattended vehicle. Unless securely left in a covered boot area out of sight.

10. Social Networking

10.1 Employees are prohibited from downloading or saving music on Age UK Surrey's computer systems.

10.2 Your business email address must not be used:

- to register an account on any website being used for personal reasons, or to receive communications from such websites e.g. social networking sites such as Facebook and eBay, shopping sites, or similar sites, message boards or any blog sites
- to receive communications relating to any personal businesses
- to subscribe to regular update emails for social activities such as cinema or theatre listings or other non-business purposes.

10.3 Use of social networking sites for good-natured personal contacts is allowed when on a break using your own credentials in a browser "private tab" - for example checking family photos on Facebook.

If you use social networking sites at home or outside of work any comments you make may still have an impact on your work and your colleagues. Please note that you may still be subject to Age UK Surrey's Disciplinary Procedures if you make any defamatory, inappropriate and/or offensive comments about Age UK Surrey, its clients or your colleagues when online.

10.4 Should you come across any article or comments on-line that you feel Age UK Surrey may wish to respond to, you should bring this to the attention of the Chief Executive so that it can be dealt with in an appropriate manner. Under no circumstances should you attempt to respond yourself.

10.5 Please ensure therefore that you do not use systems like Facebook or Twitter to:

- gossip about colleagues in relation to work issues;
- gossip or complain about management or management policies;
- give out any information in relation to your workplace;
- directly communicate with or harass a colleague in relation to an issue of dispute.

Such comments are capable of amounting to gross misconduct and may therefore result in the termination of your employment.

11. Bring your own device

11.1 This section of the policy is intended to protect the security and integrity of Age UK Surrey's data and technology infrastructure.

11.2 Employees must not use their own device to access work data unless signed off by ICT and their department manager. Connection of any device to either the domain or the internal Wi-Fi access point must be authorised and implemented by the IT department.

11.3 Devices may not be used at any time to:

- Store or transmit illicit materials

- Store or transmit proprietary information belonging to another company
- Harass others
- Engage in outside business activities

11.4 Age UK Surrey has a zero tolerance policy for texting or emailing while driving.

11.5 Playing of music is not generally permitted in working hours.

11.6 Security:

- In order to prevent unauthorised access, devices must be password protected using the features of the device.
- The public Wi-Fi code will be changed when considered necessary by the IT department.
- The charity reserves the right to disconnect devices or disable services without notification.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the charity's policies in this respect at all times.
- The employee is personally liable for all damages occurring from his or her personal device interaction with any part of the IT infrastructure.

Review

This policy will be reviewed every three years.
(Was named: IT Communications and Monitoring Policy for Issue 1-3)

Issue	Date agreed by Board of Age UK Surrey	Reviewed
1		November 2013
2	25th November 2013	July 2016
3	27th July 2016	Feb 2020
4	July 2020	