NO 34 INFORMATION COMMUNICATION TECHNOLOGY POLICY	
Author	Chief Executive
Division	Chief Executive's Office
For use by	All Age UK Norfolk staff either permanent or temporary, agency staff, consultants/contractors,volunteers and work experience staff who are provided with access to any of Age UK Norfolk's computer system.
Purpose	This policy is to protect individuals and Age UK Norfolk from the consequences of undesirable use of ICT.
Key related Documents	This policy should be read in conjunction with the Organisation's policies on Health and Safety, Confidentiality, Data Protection and Information Governance, Social Media and Disciplinary Procedures
Policy Number	34
Version	1
Revision number	1.5
Approval Date	Q1 2021/22
Review Date	Q1 2023/24

1 Introduction

This policy is to protect individuals and Age UK Norfolk from theconsequences of undesirable use of Information Communication Technology(ICT).

2 Policy Statement

Age UK Norfolk is committed to providing information technology, hardware equipment and software, to enable staff to carry out theirroles and responsibilities as efficiently and effectively as possible.

The Organisation is also committed to providing ICT related training andsupport to all staff and volunteers.

The Organisation has the responsibility to comply with all current legislation, which includes The Computer Misuse Act 1990, The Regulation of Investigatory Powers Act 2000, The Data Protection Act 2018, General Data Protection Regulation (GDPR), software licensing and copyright regulations and the Human Rights Act 1998.

This policy should be read in conjunction with the Organisation's policies on Health and Safety, Confidentiality, Data Protection and Information Governance, Social Media and Disciplinary Procedures and any other policies of relevance.

3 Who this Policy applies to

All Age UK Norfolk staff, either permanent or temporary, agency staff, consultants/contractors, volunteers and work experience staff who are provided with access to any of Age UK Norfolk's computer system are required and expected to adhere tothis policy.

All of Age UK Norfolk's ICT facilities and information resources remain the property of the Organisation and not of particular individuals,teams or departments.

4 Definitions

- ICT: Information Communication Technology
- Information Communication Technology: all devices, applications and systems that allow us to store, manipulate, retrieve, transmit, receive information electronically.

5 Responsibilities

Onyx is responsible for the server administration, implementation, security, and troubleshooting of the whole of the Age UK Norfolk computer network.

6 Responsibilities

Onyx is responsible for the server administration, implementation, security, and troubleshooting of the whole of the Age UK Norfolk computer network.

All those persons referred to within the scope of this policy arerequired to adhere to its terms and conditions.

Individual managers are responsible for ensuring that this policy isapplied within their own team/department. Any queries on the application or interpretation of this policy must be discussed with the Head of Operations or the Chief Executive prior to any action being taken.

All staff have a responsibility to adhere to the terms of the ICT Policy under their contract of employment.

6.1 General Security

It is important to realise that security starts with the individual user. Do not assume it is the responsibility of someone else. The main risks to your computer systems are;

- Processing error
- Theft
- Loss of data
- Hardware failure
- Power failure
- Viruses
- Disclosure of sensitive information

The guidelines issued in this policy are designed to keep theequipment and data as secure as possible.

6.2 Data Protection

Your computer represents a valuable asset, but the information you work with is even more valuable because it is essential to the running of Age UK Norfolk. As part of the services that Age UK Norfolk provides the collection of personal and sensitive data is essential. Age UK Norfolk is registered with the Information Commissioner under the Data Protection Act.

It is the responsibility of every computer user to ensure that all data is kept secure, and is accessed only by appropriate staff, volunteers and contractors in order to carry out their role and to work in accordance with the Data Protection and Information Governance Policy.

6.3 Equipment

All ICT equipment purchased or donated must be approved by Onyx to ensure it is appropriate & compatible according to existingstandards and that it is correctly licensed.

Unauthorised personnel, i.e. family and friends should not use any of Age UK Norfolk's equipment.

All of Age UK Norfolk's laptops will have encryption softwareand multi factor authentication installed in order to protect any data on them.

The System Administrator is responsible for keeping a record of when all equipment is purchased including serial numbers, makes,models, technical specification and warranty information. The Finance and Operational Support Officer is responsible for keeping the asset register and a record of mobile phones.

All ICT equipment will be disposed of in accordance with the WEEEDirective (Waste Electrical and Electronic Equipment Directive) andappropriate records kept on the asset management system.

The Head of Operations is responsible for ensuring that all ICT equipment, including equipment used by homeor mobile staff and volunteers i.e. phones, laptops and printers, are covered by Age UK Norfolk's insurance policies.

6.4 Back Up of Data

All data saved on the servers is backed up by Onyx. Users should not save any data on the desktop, as this will not be backed up.

Organisation Log is backed up by the Information and Advice team once a week.

6.5 Software Updates and Installation

It is the responsibility of all users to ensure software updates issued by Microsoft, Java and Adobe are installed regularly to maintain thesecurity of the equipment. If individuals are using bespoke software, they are responsible for ensuring it is kept up to date.

In order to ensure that all software is correctly licensed only Onyx is authorised to download and install software onto individual PCs supplied by Age UK Norfolk other than the software mentioned above.

Users must not download commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other suchlicence.

6.6 Passwords

Passwords are an integral part of system security. They are used for identification and authentication purposes. To avoid misuse, passwords should be selected carefully, protected and changed regularly.

Passwords must not be shared with any other person. Users must login with their own username and password and must not share this information with anyone. Users are responsible for their password security and must take all reasonable safeguards to protect it. Users will be held accountable for any misuse recorded under their account details if reasonable care was not demonstrated.

Age UK Norfolk's computer system will prompt users to change their password at regular intervals except in operational circumstances decided by the system administrator. This is critically important as it protects the overall security of the computersystem; sensitive data stored on the computer, helps comply with the Data Protection Act and General Data Protection Regulation (GDPR) ensures the integrity of audit trails of computer use. If this raises operational issues (e.g. someone is unexpectedly away and there is a need to access information on their personal drive or Outlook account) Onyx should be contacted for advice and assistance.

Users are required to follow the following practices to help keep passwords secure:-

- Choose a minimum of 6 characters.
- Choose a random collection of characters, numbers and letters in both upper and lowercase; this makes for the best passwords.
- Ensure your password is robust. The strength of a password (and the level of security it provides) is related to its length and how easy it would be for an attacker to guess it. Avoid choosing passwords based on birthdays, pet names, favourite football teams etc.
- Keep your password confidential. Except for a contractor providing ICT support or a System Administrator, never divulge your password toanyone and never enter passwords when others can see your key strokes.
- If you suspect that someone, other than a contractor providing ICT support or a system administrator, knows your password, change itimmediately or seek advice from Onyx.

6.7 Preventing Unauthorised Use

Your personal identity must not be shared with or used by anyone else.

- Never leave your computer unattended whilst logged on
- Never leave any confidential or personal data open to view.
- Always use a screen saver/auto-locking facility or log offwhen you leave your workstation (Ctrl – Alt – Del)
- For those staff and volunteers sharing a PC – they should always log off when they have finished their shift.
- Never let somebody else use your PC when you are loggedon.

6.8 File Management

All documents relating to the business of Age UK Norfolk must besaved in an appropriate folder on the Server. The saving of data relating to the day to day business of the Organisation, unless highly confidential or personal should not be saved on your One Drive . Drives have been set up for individual sites or teams and allAge UK Norfolk work should be saved in these drives to aid retrieval by other team members.

6.9 Use of USB Sticks, Personal home PCs & Other Devices

Uncontrolled use of ipads, USB sticks, smart phones and other devices which connect to the network via a PC or a personal homePC can lead to data theft, introduction of viruses and malware (malicious software).

For this reason, only authorised devices with adequate up-to-date anti-virus software can be connected to Age UK Norfolk's computer network. Before connecting such a device you are required to seek permission from the Head of Operations or the Chief Executive who will, if necessary, defer to Onyx for advice. This includes the use of USB sticks. If approved, Onyx will then scan the device for viruses and other undesirable malware.

6.10 Antivirus Software

Age UK Norfolk will ensure that appropriate centralised antivirus software is installed on its servers and all PCs and laptops. It is theresponsibility of Onyx to ensure it is up to date.

Individuals are responsible for monitoring any prompts or error messages and following the instructions issued by the antivirus software. If in any doubt as to whether the error message or prompt is genuine, staff must alert their line manager before following the instructions, who if necessary will seek advice from Onyx.

The antivirus should not be switched off or disabled by anyindividual without seeking guidance from Onyx first.

6.11 Using your own device

Age UK Norfolk recognises the benefits that can be achieved by allowing staff and volunteers to use their own electronic devices when working at home or when travelling. However, Age UK Norfolk must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing.

A 'Bring Your Own Device Policy' is appended to this IT Policy at Appendix 1. All staff and volunteers using their own devices for Age UK Norfolk purposes must read this policy and comply with it.

6.12 New Users and Leavers

It is the responsibility of line managers to inform Onyx of a newuser by using the new starter forms with as much notice as possible, but at least 7 working days notice so that the user can beset up on the server. The line manager will then set up a suitable time and day to carry out the induction, which should include a copy of the ICT Policy.

As part of the induction process, those members of staff/volunteerswho have been identified as needing access to the Age UK Norfolk computer system will be provided with a logon, appropriate training by the line manager in the use of the network, where to store documents, acceptable use of email and internet.

When a member of staff or volunteer leaves, an IT Leaver Form must be completed by the line manager and emailed to the Helpdesk. The line manager must also discuss with the individual about clearing out their Personal drive of any personal/private documents. Any Age UK Norfolk documents saved on this drive must be transferred to another appropriate drive.

The Helpdesk will ensure that emails are forwarded as instructedand that the account is disabled and subsequently deleted at an appropriate time.

6.13 Troubleshooting

Staff/volunteers are encouraged to solve day to day problems withspecific packages themselves in the first instance by using the “help” facility, using ICT guidance on the internet or speaking to colleagues. Problems with the network, or error messages should be emailed to helpdesk@ageuknorfolk.org.uk .

6.14 Contacting the Helpdesk

The preferred method of contact is via email tohelpdesk@ageuknorfolk.org.uk.

This email will then be forwarded and dealt with as detailed below.If an enquiry is very urgent and/or there is no email access staff and volunteers should contact their line manager.

Onyx will arrange repairs or replacements as soon as possible.

6.15 Use of Internet

Use of the Internet by staff or volunteers of Age UK Norfolkis permitted and encouraged where such use supports the goals and objectives of the Organisation. Personal use of the internet is permitted only outside of the employee’s or volunteer’s normal working hours and in accordance with this policy.

Filtering software is set up on Age UK Norfolk’s internet access across all sites. This software will deny access to a range of sites deemed unacceptable.

Users must ensure that they:

- Comply with current legislation.
- Use the Internet in an acceptable way.
- Do not create unnecessary business risk to the Organisation bytheir misuse of the internet.

6.16 Unacceptable behaviour

In particular, the following is deemed as unacceptable use or behaviour by users of Age UK Norfolk ICTequipment and networks:

- Visiting Internet sites that contain obscene, hateful orpornographic material.
- Visiting gambling sites and those containing racist, sexist,ageist or extreme political views.
- Using the computer to perpetrate any form of fraud, orsoftware or music piracy.
- Using the Internet to send offensive or harassing material tootherusers.
- Downloading commercial software or any copyrighted materials belonging to third parties unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Creating or transmitting defamatory material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus into the corporate network.
- The streaming of audio (i.e. music or radio) or video otherthan for work purposes.

If you mistakenly access an inappropriate site, as detailed above, make a note of the full website address you accessed, the date andtime and report it with this information to your line manager. Your line manager will make a log so that when an audit is carried out onthe PC in question an investigation will not have to be carried out.

6.17 Email Acceptable Use

Use of email by staff or volunteers of Age UK Norfolk is permitted and encouraged where such use supports the goals and objectives of the Organisation.

Personal use of email is permitted only outside of the staff or volunteer's normal working hours and in accordance with this policy.

Age UK Norfolk has a policy for the use of email whereby users must ensure that they:

- Comply with current legislation.
- Use email in an acceptable way.
- Do not create unnecessary business risk to the Organisation by their misuse of the Internet.

- Clear out old messages. These take up valuable disk space. When you have read something either save it by using “save as”, or delete it.
- Remember you need to delete from both your In, Sent and Deleted boxes.
- Don’t print messages unnecessarily. Don’t automatically print off everything, only those messages you wish to keep/take somewhere.
- Set up an autoreply message if out of the office for whatever reason for more than a day.
- All sent emails must include the name, title and direct dialtelephone number.

6.18 Preview Panes (Auto Preview and Reading Panes)

Preview panes allow you see part of an email before opening it. This can save time, it also shows the recipient the email If the emailis not recognised and is not expected then this is the time that the email needs to be deleted.

6.19 Housekeeping

It is the responsibility of all staff and volunteers to delete unwanted emails on a regular basis.

6.20 Viruses and Junk Mail

Many virus warnings sent by email are hoaxes and it can take up a lot of staff/volunteer time dealing with all the traffic caused by forwarding virus warnings. DO NOT forward these on to everyone, simply notify Onyx who will look into the virus warning and send out any necessary emails to all users.

Unsolicited emails should be treated with caution and must not, without good reason, be transmitted on to other users. Any message with no relevance to Age UK Norfolk’s work should be considered “junk mail” and deleted.

6.21 Unacceptable use of the Organisation’s communications systems

- Use of Organisation’s communication systems to set up personal businesses or send chain letters.
- Forwarding of Organisation confidential messages to external locations unless for valid business purposes connected to theday to day running of the organisation.
- Distributing, disseminating or storing images, text or materialsthat might be considered indecent, pornographic, obscene or illegal.
- Distributing, disseminating or storing images, text or materialsthat might be considered offensive or abusive, in that the context is a personal attack, sexist, ageist or racist.
- Accessing copyrighted information in a way that violates thecopyright.
- Breaking into the system or unauthorised use of apassword/mailbox.
- Broadcasting unsolicited personal views on social, political,religious or other non-business related matters.
- Transmitting unsolicited commercial or advertising material.
- Undertaking deliberate activities that waste staff effort or networked

resources.

- Introducing any form of computer virus into thecorporate network.

6.22 Monitoring

Age UK Norfolk accepts that the use of email and the internet is a valuable business tool. However, misuse of this facility can have anegative impact upon employee productivity and the reputation of the Organisation.

Staff and volunteers should be aware that no e-mail sent or received using the organisation's systems, and no web session, can be considered totally private. All activity on the system, including deleted files, leaves an audit trail and may potentially berecovered.

Age UK Norfolk currently uses automated systems to block and filter out unacceptable emails where possible.

Where there is apparent excessive use of the internet for personalreasons, access to inappropriate websites or any other apparent breach of this policy, the organisation reserves the right to investigate further. This investigation may involve more detailed monitoring of the content of the internet use, including material identified as personal if this is appropriate in all the circumstances. The line manager and Onyx will carry out such investigation only with authorisation from the Chief Executive or a Trustee, who must be satisfied that the case for investigation has been made, and that the type of investigation being proposed is proportionate to the apparent breach of policy.

Staff/volunteers will normally be informed that they are being investigated or monitored. In exceptional cases covert monitoring will be authorised where it is the only reasonable way of obtaining evidence of criminal activity or continuing gross misconduct, and it is necessary to avoid alerting the employee/volunteer.

Emails and files held under an employee or volunteer's name on the organisation's IT systems may be accessed when an employee is away from the office if it is necessary for the business of the organisation. This action will only be taken by Onyx at the requestof the absent employee's line manager, and where the absence iseither unplanned or likely to be lengthy, or in an emergency.

When access is obtained for this purpose, care will be taken not to open or read any email or other file which is clearly personal.

6.23 Use of Social Media including Twitter, Facebook and What's App

Refer to the separate Social Media Policy.

6.24 Use of Mobile Phones

If staff need to accept calls on their personal mobile they should do so at appropriate breaks and not during normal working hours. However, if there is a need to take an urgent call, where possible you should seek approval from your line manager

beforehand.

6.25 Working From Home

Staff formally recognised by Age UK Norfolk as working from home will be provided with sufficient ICT equipment to enable them to carry out their role, including, but not limited to, mobile phone, laptop andappropriate printer.

All equipment provided will remain the property of Age UK Norfolk and will be maintained accordingly.

Age UK Norfolk will reimburse any reasonable costs associated with setting up of a home worker. The home worker is responsible for providing an internet connection sufficient to support remote connection to Age UK Norfolk's servers. Age UK Norfolk are not responsible for the maintaining or setting up of any home workers wireless network they may choose to use.

6.26 Mobile Working

Mobile computing and telecommunications devices make it easy to work from different locations but they expose Age UK Norfolk's information to increased security risks.

Staff and volunteers using portable devices remotely must be aware of the risk of connecting to open, unsecured wireless networks, and configure mobile devices not to connect automatically to unknown networks.

Portable devices are also prone to loss or theft. In order to minimise the risk to unauthorised access to data if the device was to be lost or stolen, mobile devices must have passwords, passcodes, passkeys or biometric equivalents set up. These must be of sufficient length and complexity for the particular type of device.

Remote wipe facilities (for portable devices) if available, must also be set up and remote wipe activated, if the device is lost or stolen.

6.27 Sanction

Failure to comply with these guidelines may result in sanctions ranging from disciplinary procedures such as verbal and writtenwarnings, through to dismissal.

7. Training

All staff and volunteers are expected to implement this policy. Any member of staff or volunteer unsure of their responsibilities with regard to this policy must alert their line manager who will ensure they are fully appraised on the policy and its implementation.

8. Review

This policy will be reviewed two-yearly.

HILARY MACDONALD
Chief Executive

Appendix 1.

Bring Your Own Device Policy

1. Introduction

Age UK Norfolk recognises the benefits that can be achieved by allowing staff and volunteers to use their own electronic devices when working, whether that is at home or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as ‘bring your own device’.

The use of such devices to create and process Age UK Norfolk information and data creates issues that need to be addressed, particularly in the area of information security.

Age UK Norfolk must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing.

2. Information Security Policies

This policy must be read in conjunction with the organisation’s Data Protection and Information Governance Policy.

3. Responsibilities of Staff and Volunteers using their own devices

Individuals who make use of this ‘bring your own device’ policy’ must take responsibility for their own device and how they use it. They must:

- Ensure that others do not have access to or see Age UK Norfolk information.
- Familiarise themselves with their device and its security features so that they can ensure the safety of Age UK Norfolk information, including personal information relating to client information.
- Ensure security controls are adequate for secure handling of confidential information, including up-to-date anti-virus and malware.
- Take responsibility for any software they download onto their device.
- Ensure that the device is not used for any purpose that would be at odds with the Organisation’s IT Policy.
- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device.
- Set up remote wipe facilities (for portable devices), if available and implement a remote wipe if they lose the device.
- Not hold any information that is sensitive, personal or confidential.

- Where it is essential that information belonging to Age UK Norfolk is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails.
- Report the loss of any device containing Age UK Norfolk data (including email) to their line manager.
- Be aware of any Data Protection and ensure all personal data is handled appropriately.
- Report any security breach immediately in accordance with the Data Protection and Information Governance Policy, where personal data is involved.

Age UK Norfolk cannot take responsibility for supporting devices it does not provide. Therefore, staff and volunteers using their own devices to access Age UK Norfolk related data must take all reasonable steps to:

- Prevent theft and loss of data.
- Keep information confidential.
- Maintain the integrity of data and information.

Particular care to delete all Age UK Norfolk information must also be taken if a device is disposed of/sold/transferred to a third party.

5. Data Protection

Age UK Norfolk must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 1998. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

Therefore, staff must follow the guidance in this document and in the Data Protection and Information Guidance Policy when considering using their own devices to process personal data.

9.0 Document Control

Version	Revision	Action	Author	Date
1	1.5	General updates, addition of 'bring your own device' policy and mobile device section.	HM	May 2021
1	1.4	General updates	HM	June 2019
1	1.3	Rebrand of front page and addition of contents page and page numbers, Change Human Resources to People and Development, Removal of need to sign sanction	CA/KE	30/10/17
1	1.2	Item 4.9 revised	SB	November 2016
1	1.1	Reviewed and revised	SB	July 2016