AGE UK EXETER

Controlled Document

Document Name: IT and Communication Systems Policy
Document Version Number: 4
Approved by Board of Trustees: 4 March 2022
Review Schedule: Every three years
Next review due: March 2025
Owner (Responsibility): Chief Executive Officer
Revision History: See end of document.
Document Location: www.ageuk.org.uk/exeter/about-us/policiesandguidelines/

Document Description
Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy 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.

Implementation & Quality Assurance
Implementation is immediate and this framework shall stay in force until any alterations are agreed.

All aspects of this document shall be open to review at any time. If you have any comments or suggestions on its content, please contact Chief Executive Officer at info@ageukexeter.org.uk or at Age UK Exeter, The Sycamores, Mount Pleasant Road, Exeter, EX4 7AE, 01392 202092.

IT and Communication Systems Policy

1. About this policy

Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy 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.

The Board of Trustees has overall responsibility for this policy, including keeping it under review.

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

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

This policy does not form part of any employee's contract of employment, and we may amend it at any time.

2. Personnel responsible for the policy

Our Board of Trustees (the Board) has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to The Chief Executive Officer.

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.

The Operations Manager will deal with requests for permission or assistance under any provisions of this policy and may specify certain standards of equipment or procedures to ensure security and compatibility.

3. Equipment security and passwords

You are responsible for the security of the equipment allocated to or used by you and must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items you take out of the office. You should keep your passwords confidential.

You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision.

Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the Operations Manager.

You must not use another person's username and password or allow anyone else to log on using your username and password unless authorised by the Operations Manager. On termination of employment (for any reason) you must provide details of your passwords to the Operations Manager and return any equipment, key fobs or cards.

Passwords should not be saved to any device at any time.

If you have been issued with a laptop, PDA or mobile phone, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

You must log out and shut down your computer at the end of each working day.

4. Systems and Data Security

You should not delete, destroy, or modify existing systems, programmes, information, or data (except as authorised in the proper performance of your duties).

You must not download or install software from external sources without authorisation from the Operations Manager. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware. This includes software programmes, instant messaging programmes, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by the Operations Manager before they are downloaded. If in doubt, staff should seek advice from the Operations Manager.

You must not attach any device or equipment to our systems without authorisation from the Operations Manager. This includes any USB flash drive, MP3 or similar device, PDA or telephone, whether connected via the USB port, infra-red connection port or in any other way.

We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources. If an email appears suspicious (for example, if it contains a file whose name ends in .exe), do not reply to it, open any attachments, or click any links to it. Inform the Operations Manager

immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

If you use laptops or Wi-Fi enabled equipment, you must be particularly vigilant about its use outside the office and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Privacy Standard.

5. Email

Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard footer should always be included. Hard copies of emails should be kept on the relevant file as appropriate.

Remember that emails can be used in legal proceedings and that even deleted emails may remain on the system and be capable of being retrieved.

You should access your emails at least once every working day, stay in touch by remote access when travelling in connection with our business, and use an out of office response when away from the office for more than a day. You should endeavour to respond to emails marked “high priority” within 24 hours.

You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic, or otherwise inappropriate emails. Anyone who feels that they have been harassed or bullied or are offended by material received from a colleague via email should inform their line manager.

You should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that email messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user’s inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

To minimise the possibility of a data breach any emails which are being sent to two or more external recipients should have their addresses listed in **bcc** so that they are not visible to other recipients.

In general, you should not:

(a) send or forward private emails at work which you would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them;

(d) sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

(e) agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;

(f) download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

(g) send messages from another person's email address (unless authorised) or under an assumed name; or

(h) send confidential messages via email or the internet, or by other means of external communication which are known not to be secure.

You should return any wrongly delivered email received to the sender.

Do not use your own personal email account to send or receive email for the purposes of our business. Only use the email account we have provided for you.

We do not permit access to web based personal email such as Gmail or Hotmail on our computer systems at any time due to additional security risks.

6. Using the internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in section 9, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored, or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

Internet access is provided for business purposes. Occasional personal use may be permitted as set out in section 7. You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

You should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time.

The following may only be accessed from the network in the course of your work and not for personal use online radio, audio and video streaming, instant messaging and webmail (such as Hotmail, Gmail or Yahoo) and social networking sites (such as Facebook, Meta, Instagram, YouTube, Twitter, Snapchat). This list may be modified from time to time.

We may block or restrict access to some websites at our discretion.

7. Personal use of our systems

We permit the incidental use of our internet (using your own device), and telephone systems to browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

Personal use must meet the following conditions:

(i) use must be minimal and take place substantially outside of normal working hours (that is during lunch breaks or before or after work);

(j) use must not affect your work or interfere with business or office commitments.

(k) use must not commit us to any marginal costs; and

(l) use must comply with our policies including the Equal Opportunities Policy, Anti-harassment Policy, Privacy Standard and Disciplinary Procedure.

You should be aware that personal use of our systems may be monitored and, where breaches of this policy are found, action may be taken under the disciplinary procedure. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

8. Monitoring

Our systems enable us to monitor telephone, email, voicemail, internet, and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

We reserve the right to retrieve the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

(m) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy.

(n) to find lost messages or to retrieve messages lost due to computer failure;

(o) to assist in the investigation of alleged wrongdoing; or

(p) to comply with any legal obligation.

9. Prohibited use of our systems

Access is granted to the internet, telephones, and other electronic systems for legitimate business purposes only.

Misuse or excessive personal use of our telephone system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, misuse of the email system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

(q) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(r) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

(s) a false and defamatory statement about any person or organisation;

(t) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

(u) confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);

(v) unauthorised software;

(w) any other statement which is likely to create any criminal or civil liability (for you or us); or

(x) music or video files or other material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

10. Bring your own device

In order to comply with GDPR you are prohibited from using your own device for any work-related activities, including taking of photographs which are intended to be for business use by AUKE.

If you have not been supplied with a work device(s) and consider this to be necessary, you should first discuss this with your line manager.

Revision History

Revision date	Summary of Changes	Other Comments
27.1.2022	New document using HR Express template	Approved by trustees 4 March 2022. Next review due March 2025