IT and Communications Systems and Monitoring Policy

Incorporating
**Internet, Email and Social Media
Acceptable Use Policies**

KEY INFORMATION

Policy prepared, reviewed or amended by:	Bridgette Doyle, Suzanne Hilton – Chief Executive
Policy approved by Board of Trustees on:	24 August 2021
Policy became operational on:	28 July 2015 (IT and Communications Systems and Monitoring Policy adopted 28 August 2018)
Next Review Date	The IT and Communications Systems and Monitoring Policy (incorporating the Internet, Email and Social Media Acceptable Use Policies), and associated guidance and procedures does not form part of staff contracts of employment and may be reviewed and updated at any time. It will be reviewed no less than every three years, or sooner where there are significant changes to guidance or legislation. Minor updates will be made as required.

INTRODUCTION

The Age UK Bolton IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards that you must observe when using these systems; the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.

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.

This policy applies to all permanent and temporary employees, trustees, volunteers, agency staff, job applicants, contractors, consultants who are working for or supplying services to Age UK Bolton or Age UK Bolton Enterprises Limited *(which is a wholy owned subsidiary of Age UK Bolton)* hereafter referred to as "workers" and who use the Age UK Bolton IT and communications systems.

This policy applies to no matter whether the internet access or email and/or social media use takes place on Age UK Bolton's premises, while travelling for work or while working from home, including outside working hours on their own devices and networks or third party networks. It applies to use of the internet on any device that is owned by Age UK Bolton or that is connected to any of the charity's networks or systems. The policy will apply if an Age UK Bolton worker is using the internet at

their desk at work, or if they connect their own personal tablets, smart phones or other electronic devices to the Age UK Bolton wireless networks.

This policy should be read alongside other key policies. In particular, users should also read the charity's Privacy Policy.

POLICY STATEMENT

Age UK Bolton understands the importance of appropriate and acceptable use of IT and communications systems - including internet, email and social media - and owes a duty to their stakeholders to put in place a policy for regulating and monitoring acceptable use of these media.

AGE UK Bolton recognises that all clients and workers have the right to expect that any information imparted by them to us will be used only for the purpose for which it is given and should not be released to any other person, or outside the organisation, without the user's consent.

For the purpose of this policy, 'client' means anyone who uses the service directly or indirectly, whether this be an individual older person, their representative or carer or another organisation.

WHY THIS POLICY EXISTS

This IT and Communications Systems and Monitoring Policy is designed to:

- Reduce the online security and business risks faced by Age UK Bolton
- Let workers know what they can and cannot do online and whilst using email and/or social media sites
- Ensure that workers do not view inappropriate content at work
- Ensure that workers follow good practice and etiquette in their use of the internet, email and social media
- Help Age UK Bolton satisfy its legal obligations regarding internet, data privacy, email and social media use

SCOPE AND RESPONSIBILITY

Age UK Bolton makes internet access available to its employees, volunteers and other workers (hereafter collectively referred to as 'workers') where relevant and useful for their jobs. This policy describes the rules governing internet, email and social media use at Age UK Bolton and sets out how our workers are expected to behave when using the internet, email and social media sites.

This policy applies whether workers use internet and email or access social media services and social networking websites at work, either through Age UK Bolton IT systems or via their own personal equipment. It sets out how Age UK Bolton workers must behave when using the organisation's IT and communications systems, including email and social media accounts. It also explains the rules about

using personal email and/or social media accounts at work and describes what workers may say about Age UK Bolton on their personal accounts.

Everyone who uses the internet at work, operates a charity email or social media account or who uses their personal social media accounts at work has some responsibility for implementing this policy.

The Board of Trustees of Age UK Bolton 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 and the Corporate Services Manager.

The Corporate Services Manager, in conjunction with the Chief Executive, has a responsibility for:

- ensuring that the Age UK Bolton IT and communications systems (including internet, email and social media use) are conducted safely, appropriately and in line with the charity's objectives;

- ensuring that the IT or social media support contractor provides any 'apps' and tools that the Chief Executive advises are required to manage the charity's social media presence and track any key performance indicators;

- proactively monitoring for social media security threats;

- ensuring requests for assistance and support made via social media are followed up

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.

The Corporate Services Manager and/or Chief Executive 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.

AUTHORISED USERS

Only people who are authorised to use Age UK Bolton IT and communications systems *(including use of internet, email and social media)* may do so.

Authorisation is usually provided by a worker's line manager or the charity IT support contractor. It is typically granted when a new worker joins Age UK Bolton and is assigned their login details for the charity IT systems.

Unauthorised use of the charity's IT and communications systems is prohibited.

Workers who use charity's IT and communications systems without authorisation (or who provide access to unauthorised people) may be subject to disciplinary procedures, as appropriate in the circumstances.

IT 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 that you take out of the office. You should keep your passwords confidential and change them regularly.

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, so as 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 Corporate Services Manager or the Chief Executive.

You must not use another person's username and password or make available to or allow your own username and password to be used by anyone else to log on unless authorised by Corporate Services Manager or the Chief Executive. On termination of employment *(for any reason)* you must provide details of your passwords to the Corporate Services Manager and/or the Chief Executive and return any equipment.

If you have been issued with a mobile phone, laptop, tablet, you must ensure that it is kept secure at all times, especially when travelling. Passwords <u>must be used</u> 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.

SYSTEMS AND DATA SECURITY

You should not delete, destroy or modify existing systems, programs, 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 Corporate Services Manager or the Chief Executive. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware. This provision includes software programs,

instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked before they are downloaded. If in doubt, you should seek advice from the Corporate Services Manager or the Chief Executive.

You must not attach any device or equipment to our systems without authorisation from Corporate Services Manager or the Chief Executive. This includes any external hard drive, USB stick or mobile, whether connected via the USB port, or in any other way.

The use of USB memory sticks, pen drives or similar data storage devices is strictly prohibited.

We will monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or any email which appears suspicious (for example, if it contains a file whose name ends **'.exe'**). Inform the Corporate Services Manager or Chief Executive immediately if you suspect your computer may have a virus. Age UK Bolton reserves 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, from time to time, require against importing viruses or compromising system security. The Age UK Bolton data network 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 Policy.

GENERAL USE GUIDELINES

Business Email Use

Age UK Bolton recognises that email is a key communication tool and workers are encouraged to use email whenever appropriate for example to:

- Communicate with customers or suppliers;

- Distribute information to colleagues, volunteers, trustees and partners;

- Market the Charity's products and services.

Notwithstanding, however, its relevance as a vital business tool, you should always consider whether email is the appropriate method for a particular communication.

Correspondence with third parties by email should be written as professionally as you would a letter. Messages should be concise and directed only to relevant individuals and, where appropriate, hard-copies of emails should be kept on the appropriate file. You should adopt a professional tone and observe appropriate etiquette when communicating with third parties by email.

Email Disclaimers

The standard Age UK Bolton email template includes an email disclaimer. Users must ensure this appears on all their emails and must not remove or change this when they send messages.

In the event any user thinks they do not have this disclaimer they should contact the Corporate Services Manager immediately for support in ensuring the correct disclaimer appears on all future emails.

Business internet use

Age UK Bolton recognises that the internet is now an integral part of doing business and workers are encouraged to use the internet wherever appropriate as part of their work to support the charity's aims and objectives, for example to:

- Identify potential partners, customers or suppliers

- Purchase supplies or book business travel as part of their authorised role

- Research for Age UK Bolton

- General communication

- Market Age UK Bolton products and services as part of their role or to do market research

Personal Email and Internet Use

Age UK Bolton also recognises that email and the internet have become important tools in many people's daily lives and, accordingly, allows workers to use their charity email account and the charity's internet connections for personal purposes, with the following stipulations:

- Personal email and internet use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch.

- All rules described in this policy apply equally to personal email/internet use. For instance, **inappropriate content is <u>always</u> inappropriate, no matter whether it is being sent or received for business or personal reasons**.

- Use of email or the internet for personal purposes must not affect the service available to other users. For instance, sending exceptionally large files by email or downloading exceptionally large files via the internet could slow access for other workers who need access as part of their role.

- Users may access the internet at work, if they can do so via our internet connection but only in accordance with these policy guidelines. For instance, a staff member may, <u>during a break period</u>, look something up on the internet, such as if they are looking at holiday prices or searching on *Ebay* or *Amazon* to purchase a gift for someone.

- Unauthorised use of the charity's internet connection is strictly prohibited and workers who use the internet without permission or provide access to unauthorised people may be subject to disciplinary procedures which, for employees, could result in dismissal in the case of very serious breaches.

The Power of Social Media

Age UK Bolton recognises that social media offers a platform for the organisation to stay connected with customers and build its profile online, including driving potential clients, supporters, donors and volunteers to the website. Age UK Bolton also acknowledges that there may be occasions where staff could be involved in appropriate professional conversations on social networks which would benefit the organisation and, in such circumstances, may encourages workers to use social media to make useful connections, share ideas and good practice and to shape discussions to help achieve the organisations' aims and objectives.

Regardless of which social networks Age UK Bolton workers are using, or whether they are using business or personal accounts, Age UK Bolton expects workers to follow some basic rules to help avoid the most common pitfalls and, thereby, minimise the likelihood of exposing the organisation to any risk or detriment.

Users <u>should</u>:

- Know the social network. Spend time becoming familiar with the social network before contributing.

- Err on the side of caution. If unsure, don't post it to social networks. If a worker feels an update or message might cause complaints or offence - or be otherwise unsuitable - they should not post it. Age UK Bolton workers can always consult the Corporate Services Manager for advice.

- Be thoughtful and polite. Many social media users have got into trouble simply by failing to observe basic good manners online. Workers should adopt the same level of courtesy used when communicating via email.

- Look out for security threats. Be on guard for social engineering and 'phishing' attempts. Social networks are also used to distribute 'spam' and 'malware'. (Further details are set out below).

- Keep personal use reasonable. Although the charity believes that having workers who are active on social media can be valuable both to those workers and to the organisation, workers should exercise restraint in how much personal use of social media they make during working hours and should keep this to their breaks unless it is part of their role.

- Don't make promises without checking. Some social networks are very public, so <u>it is very important that workers should not make any commitments or promises</u> on behalf of Age UK Bolton without checking that the charity can deliver on the promises. Direct any enquiries to your line manager or in their absence the Chief Executive.

- Handle complex queries via other channels. Social networks are not a good place to resolve complicated enquiries and customer issues. If a customer/service user/potential volunteer has made contact via social media, workers should handle further communications via the most appropriate channel — usually email or telephone.

- Don't escalate things. It is easy to post a quick response to a contentious status update and then regret it. <u>Workers should always take the time to think before responding, and hold back if they are in any doubt at all.</u>

When you include your link to Age UK Bolton in a personal profile (e.g a 'bio' on Twitter, 'workplace' on Facebook, or LinkedIn) there should be extra attention to personal posts that may affect the reputation of the organisation. Similarly on leaving the organisation you should update your personal profiles to reflect that you no longer work for Age UK Bolton.

KEY POLICY AREAS

Email and Internet Security

Used inappropriately, both email and the internet can be a source of security problems which could do significant damage to the organisation's reputation and data.

Users of the charity's email system and internet connections <u>must not</u>:

- Knowingly introduce any form of computer virus, Trojan, spyware or other malware into the charity's IT and communications systems or open email attachments from unknown sources lest these contain such a virus/malware.

- Disable security or email scanning software: these tools are essential to protect the business from security problems.

- Send confidential charity data via email: the IT support contractor can advise on appropriate tools to use instead, if in doubt staff should consult the Corporate Services Manager or the Chief Executive.

- Steal, use or disclose someone else's login or password without authorisation.

- Access another user's charity email account. If access is required to a specific message *(for instance, while an employee is off sick)*, the line manager, the Corporate Services Manager or the Chief Executive should be approached prior to consulting the IT support contractor.

- Allow Age UK Bolton data to be uploaded and/or be shared other than via approved services. The Corporate Services Manager can advise on appropriate tools for sending and sharing large amounts of data.

- Gain access to websites or systems for which they do not have authorisation, either within the business or outside of it.

Staff members must always consider the security of the charity's systems and data when using email and/or the internet. If required, help and guidance is available from line managers, the Corporate Services Manager and the charity's IT support contractor.

Users should note, particularly, that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception. Although such interceptions are rare, it is best to regard email as an open communication system which is not suitable for confidential messages and information.

Inappropriate Email, Internet or Social Media Content and Use

The charity's IT and communications systems must not be used to send or store inappropriate content or materials.

It is important employees understand that viewing or distributing inappropriate content via email, internet, social media or other means <u>is not acceptable under any circumstances</u>.

Users <u>must not</u>:
- Write, create, send, post or otherwise transmit - whether by email, internet or social media - any message, status update or material (or link to other

material) that might be regarded as defamatory or incur any liability for Age UK Bolton.

- Create or distribute any inappropriate content or material via email, internet or social media.

  (For the avoidance of doubt, 'inappropriate content' includes (but is not limited to): pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs. This definition of inappropriate content or material also covers any text, image or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation or any other characteristic protected by law.)

- Use email, internet or social media for any illegal or criminal activities.

- Sell or advertise using our email system or broadcast messages about lost property, sponsorship or charitable appeals unless you have received proper authorisation to do so.

- Broadcast, using our email system or internet/social media, any unsolicited views on social, political, religious or other non-business related matters.

- Interact with the charity's stakeholders in any ways that could be interpreted as being offensive, disrespectful or rude.

- Discuss on social media other workers, colleagues, customers/clients, partners or suppliers without their approval.

- Post, upload, forward or provide a link to spam, junk emails or chain emails and messages.

- Send, post, distribute or otherwise transmit any abusive, obscene, discriminatory, racist, offensive, harassing, derogatory or defamatory material to others.

- Send any message or material or take part in any internet/social media activities that could damage the name, image or reputation of Age UK Bolton.

Any user who receives an email or is aware of any internet/social media/Microsoft Teams chat content that they consider to be inappropriate should report this to their line manager/supervisor, Corporate Services Manager or the Chief Executive.

Generally, you should take care with the content of any *(and every)* email message or internet/social media/Teams chat contributions that you send or interact with, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should work on the presumption that messages or material on social media may be read/viewed by others and take care not to include anything which would offend or embarrass any reader/viewer, themselves or the organisation, if it found its way into the public domain.

Copyright and Intellectual Property

Age UK Bolton respects and operates within copyright and intellectual property laws. Users may not use the charity's email or internet to share any copyrighted software, media or materials owned by, or licensed to, third parties, unless permitted by that third party or use any of the charity's equipment, software or internet connection to perform any tasks which might involve, create or constitute a breach of copyright or other intellectual property rights.

Workers must not use the charity's email or internet system to perform any tasks that may involve breach of copyright law, including *(but not limited to)* downloading illegal copies of music, films, games or other software, whether via file-sharing services or other technologies.

Users should keep in mind that the copyright in letters, files and other documents attached to an email or on social media may be owned by the sender or a third party. Forwarding or otherwise distributing such emails/social media to other people may, therefore, breach this copyright and care should be taken accordingly.

With respect to internet/social media and providing that they are confident that it is not illegal, workers may share content published on another website, provided that the website has obvious 'sharing' buttons or functions on it. Workers should always check licences, including creative commons licences used on social media to facilitate legal and appropriate sharing of content.

Contracts and liability to third parties

Users must be careful about making commitments or agreeing to purchases, particularly via email. This is important because an email message may form a legally-binding contract between Age UK Bolton and the recipient even if the user has not obtained proper authorisation within the charity, as a name typed at the end of an email constitutes a signature in the same way as a name written at the end of a letter.

Email Marketing and Bulk Emails

Age UK Bolton may use email to market to existing and potential customers. There is significant legislation covering the practice of bulk emailing and use of email for marketing. In this context, workers should ensure that they aware of the requirements and controls established by the Data Protection Act 2018 and the General Data Protection Regulations (GDPR).

All email campaigns must be authorised by the Chief Executive and implemented using the charity's email marketing tools, if applicable. Users must not send bulk emails using the standard business email system.

BEST PRACTICE FOR EMAIL

Email etiquette

Email is often used to communicate with clients, customers, partners and other important contacts. Although a relatively informal medium, staff should be aware that each email they send does affect the charity's image and reputation.

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

Age UK Bolton expects all workers using email to follow rules of good email etiquette.
Users <u>must</u>:

- Not forward on chain emails or 'humorous' messages. These clog up people's 'in-boxes' and some topics are not appropriate for the workplace.

- Always use a meaningful 'subject' line rather than leaving it blank or using a single word like 'hello' so that the subject is clear.

- Only use the 'important message' setting sparingly, i.e. for messages that really are important.

- Never ask recipients to send a 'message read' receipt. Many people find these annoying and not all email services support them.

- Not use ALL CAPITAL LETTERS in messages or subject lines as this can be perceived as impolite.

- Be sparing with group messages, only adding recipients who will find the message genuinely relevant and useful.

- Use the 'CC' (carbon copy) field sparingly. If someone really needs to receive a message, they should be included in the 'To' field.

- Use the 'BCC' (blind carbon copy) field to send group messages where appropriate. It stops an email recipient seeing who else was on the email.

- Return any wrongly-delivered email received to the sender.

Internal Email

Email is a valid way to communicate with colleagues. However, we do not wish for it to be over-used for internal communication.

When emailing colleagues users should consider whether the issue could be better addressed via a face-to-face discussion or telephone call? Also whether email is really the best way to send a document out for discussion? Often, it becomes very hard to keep track of feedback and versions.

It is rarely necessary to 'Reply All'. Usually, it is better to reply and then manually add other people who need to see a message.

BEST PRACTICE FOR SOCIAL MEDIA USE, SECURITY AND DATA PROTECTION

Age UK Bolton workers should be aware of the security and data protection issues that can arise from using social networks.

Maintaining confidentiality

Users must not**:
- Share or link to any content or information owned by the organisation that could be considered confidential or sensitive.

- Share or link to any content or information owned by another charity or person that could be considered confidential or sensitive.

- Share or link to data in any way that could breach the Age UK Bolton Privacy Standard.

Protection of Social Media Accounts

All Age UK Bolton social media accounts should be protected by strong passwords that are changed regularly and shared only with authorised users.

Age UK Bolton workers must not use a new piece of software, app or service with any of the charity's social media accounts without receiving approval from the Chief Executive.

With the rise in staff users on Facebook to administer groups, the Communications Officer and Corporate Services Manager should monitor the number of users, terms of access and review posts to ensure consistency.

Avoiding Social 'Scams'

Workers should watch for 'phishing' attempts, where 'scammers' may attempt to use deception to obtain information relating to either the charity or its clients.

Workers should never reveal sensitive details through social media channels. Provider or supplier identities must always be verified in the usual way before any account information is shared or discussed.

Workers should avoid clicking links in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague-sounding direct messages.

MONITORING AND BREACH OF THE POLICY

Monitoring of Email Use

The Age UK Bolton email system and software are provided for legitimate business use and we reserve the right, therefore, to monitor employee use of email but can reassure users that any such examinations or monitoring will only be carried out by authorised staff.

Users should also be aware that all emails sent or received through Age UK Bolton's email system are part of official Age UK Bolton records and that we could be legally compelled to show that information to law enforcement agencies or other parties.

It is our policy, therefore, that users should always ensure that all business information sent via email is accurate, appropriate, ethical, and legal. 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; consequently, all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

Monitoring of Internet and Social Media Use

Age UK Bolton IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate business use. Age UK Bolton reserves the right, therefore, to monitor use of the internet, to examine systems and review how data is stored on these systems and how social networks are used and accessed through these resources. Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all internet data written and data relating to social networks written, sent or received through the organisation's computer systems is part of official Age UK Bolton records and the charity can be legally compelled to show that information to law enforcement agencies or other parties. Users therefore have a duty to always ensure that all Age UK Bolton information sent over or uploaded to the internet or posted or shared via social media is accurate, appropriate, ethical, legal and not in breach of this policy.

Potential Sanctions for Breach of Policy

Knowingly breaching this email use policy is a serious matter and may result in disciplinary procedures being taken.

Workers, trustees, volunteers, contractors and other users may also be held personally liable for their violation of this policy.

EMPLOYEE/VOLUNTEER CONSENT STATEMENT

I …………….....................……….. (name of employee/volunteer) hereby confirm that I have read, understood and will comply with the attached Age UK Bolton IT and Communications Systems monitoring policy.

Signed……………………………………………………….………………..

Date …………………………………………