IT and Communications Systemsand 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 approvedby 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 notform 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. Next review date – June 2027

1. INTRODUCTION

1.1 The Age UK Bolton IT and communications systems are intended to promote effective communication and working practices within our organisation. This policyoutlines 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.

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

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

1.4 This policy applies 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, andnetworks 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.

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

2. POLICY STATEMENT

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

2.2 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.

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

3. WHY THIS POLICY EXISTS

3.1 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.

4. SCOPE AND RESPONSIBILITY

4.1 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 tobehave when using the internet, email and social media sites.

4.2 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 workersmust 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.

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

4.4 The Board of Trustees of Age UK Bolton has overall responsibility for the effectiveoperation 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.

4.5 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

4.6 All managers have a specific responsibility to ensure the fair application of this policyand all members of staff are responsible for supporting colleagues and ensuring its success.

4.7 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 certainstandards of equipment or procedures to ensure security and compatibility.

5. AUTHORISED USERS

5.1 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.

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

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

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

6. IT EQUIPMENT SECURITY AND PASSWORDS

6.1 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 ofthe office. You should keep your passwords confidential and change them regularly.

6.2 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 useterminals under supervision.

6.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the Corporate Services Manager orthe Chief Executive.

6.4 You must not use another person's username and password, or make available to orallow 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 ofemployment *(for any reason)* you must provide details of your passwords to the Corporate Services Manager and/or the Chief Executive and

return any equipment.

6.5 If you have been issued with a mobile phone, laptop, tablet, you must ensure that it iskept 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.

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

7. SYSTEMS AND DATA SECURITY

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

7.2 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 programmes, instant messaging programmes, 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.

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

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

7.5 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 reservesthe 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.

7.6 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.

7.7 If you use laptops or Wi-Fi enabled equipment, you must be particularly vigilant abouttheir 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/orwhich is subject to data protection legislation; such information must be treated with extreme care and in accordance with our Privacy Policy.

GENERAL USE GUIDELINES

8. Business Email Use

8.1 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by email. You should also include our standard email signature and disclaimer.

8.2 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.

8.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails.

8.4 You should not:

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

8.4.2 send or forward chain mail, junk mail, cartoons, jokes or gossip;

8.4.3 contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to others who do not have a real need to receive them; or

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

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

9. Business internet use

9.1 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 theirwork 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.
- facilitate general communication.

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

10. Personal Email and Internet Use

10.1 We permit the incidental use of our systems to send personal email, browse the internet and make personal telephone calls, subject to certain conditions. 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.

10.2 Personal use must meet the following conditions:

10.2.1 it must be minimal and take place substantially outside of normal working hours (that is, during your lunch break, and before or after work);

10.2.2 personal emails should be labelled "personal" in the subject header;

10.2.3 it must not affect your work or interfere with the business;

10.2.4 it must not commit us to any marginal costs; and

10.2.5 it must comply with our policies, including this policy, the Diversity, Equity and Inclusion (DEI) Policy, Anti-harassment and Bullying Policy, Data Protection Policy, and Disciplinary and Capability Procedure.

11. The Power of Social Media

11.1 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 potentialclients, 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 encourage workers to use social media to make useful connections, share ideas and good practice and to shape discussions to help achieve the organisation’s aims and objectives.

11.2 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 , thereby minimizing the likelihood of exposing the organisation to any risk or detriment.

11.3 Users should:

- Know the social network. Spend time becoming familiar with the social networkbefore 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 theirbreaks, unless it is part of their role.
- Not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.
- Avoid making any social media communications that could damage our business interests or reputation, even indirectly
- Not express opinions on our behalf via social media, unless expressly authorised to do so by your manager. You may be required to undergo training in order to obtain such authorisation
- Not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.
- Don't make promises without checking. Some social networks are very public, so it is very important that workers should not make any commitments or promises 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 ChiefExecutive.
- 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, workersshould 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 statusupdate and then regret it. Workers should always take the time to think before responding, and hold back if they are in any doubt at all.

- If you see social media content that disparages or reflects poorly on Age UK Bolton you should contact the Corporate Services Manager

11.4 If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues. Similarly, on leaving the organisation you should update your personal profiles to reflect that you no longer work for Age UK Bolton.

12. Copyright and Intellectual Property

12.1 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, nor 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.

12.2 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.

12.3 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.

12.4 With regard 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 alwayscheck licences, including creative commons licences used on social media, to facilitate legal and appropriate sharing of content.

13. Contracts and liability to third parties

13.1 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 aletter.

14. Email Marketing and Bulk Emails

14.1 Age UK Bolton may use email to market to existing and potential customers. Thereis 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).

15. Monitoring

15.1 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 (including any personal use), may be continually monitored by automated software or otherwise.

15.2 We reserve the right to retrieve the contents of email messages or to 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):

15.2.1 to monitor whether use of the email system or the internet is legitimate and in accordance with this policy;

15.2.2 to find lost messages or to retrieve messages lost due to computer failure;

15.2.3 to assist in the investigation of alleged wrongdoing; and

15.2.4 to comply with any legal obligation.

16. Prohibited use of our systems

16.1 Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

16.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

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

16.2.2 offensive, obscene or criminal material or material which is liable to cause embarrassment to us or to our clients or customers;

16.2.3 a false and defamatory statement about any person or organisation;

16.2.4 material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Diversity, Equity and Inclusion Policy or our Anti-harassment and Bullying Policy);

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

16.2.6 unauthorised software;

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

16.2.8 music or video files or other material in breach of copyright.

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

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 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 couldbe considered confidential or sensitive.
- Share or link to any content or information owned by another charity or personthat could be considered confidential or sensitive.
- Share or link to data in any way that could breach the Age UK Bolton PrivacyStandard.

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 therefore reserve the right 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. As a result, users 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 ……