# South Bank Multi Academy Trust

# Communications Acceptable Use Policy

| | |
|---|---|
| Approved by Trustees: | January 2022 |
| Version: | 2.0 |
| Review Timetable: | 3 years |
| Renewal Date: | January 2025 |

## 1. INTRODUCTION

1.1 As part of South Bank Multi Academy Trust's (SBMAT) programme to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), it has a suite of information governance policies.

1.2 The Communications Acceptable Use policy governs the use of the SBMAT's communications network that the schools and individuals use on a daily basis in order to carry out business functions.

1.3 This policy should be read in conjunction with the other policies in SBMAT's Information Governance policy framework.

## 2. SCOPE

2.1 All policies in SBMAT's Information Governance policy framework apply to all Trust employees, any authorised agents working on behalf of the Trust, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly breach any of the points outlined in this and other Information Governance policies may face disciplinary action.

2.2 The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,

- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

## 3. EMAIL AND INSTANT MESSAGING USE

3.1 The Trust provides email accounts to employees to assist with performance of their duties. There is also the facility to use instant messages on some systems in schools. For the benefit of doubt instant messages are classed as email communications in this policy.

3.2 **Personal Use:** Whilst email accounts should primarily be used for business functions, incidental and occasional use of the email account in a personal capacity may be permitted so long as:

- Personal messages do not tarnish the reputation of SBMAT or any of its schools,
- Employees understand that emails sent to and from corporate accounts are the property of the Trust,
- Employees understand that Trust management may have access to their email account and any personal messages contained within,
- Employees understand that the emails sent to / from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation,
- Employees understand that the Trust reserves the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network,
- Use of corporate email accounts for personal use does not infringe on business functions.

3.3 **Copyright:** The Trust does not permit individuals to attach photos, pictures or images to their email profile or within their email signature as these may breach copyright law.

3.4 **Inappropriate Use:** The Trust does not permit individuals to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files,
- Unwelcome propositions,
- Profanity, obscenity, slander, or libel,
- Ethnic, religious, or racial slurs,
- Political beliefs or commentary,

- Any messages that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

3.5 **Other Business Use:** Users are not permitted to use emails to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of Trust / School Leadership Team.

3.6 **Email Security:** Users will take care to use their email accounts in accordance with SBMAT's Information Security policy. In particular users will:

- Not click on links in emails from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise the Trust's / School's IT network,
- Not send excessively large email attachments without authorisation from Trust / School management and the Trust's IT provider.

3.7 **Group Email Accounts:** Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These generic email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of generic email accounts could lead to suspension of an individual's email rights. The School Business/Finance Manager will have overall responsibility for authorising access to generic email accounts but this responsibility may be devolved to other individuals.

3.8 The Trust may monitor and review all email traffic that comes to and from individual generic email accounts.

## 4. INTERNET USE

4.1 The Trust provides internet access to employees to assist with performance of their duties.

4.2 **Personal Use:** Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of SBMAT or any of its schools,
- Employees understand that Designated Senior Leaders may have access to their internet browsers and browsing history contained within,
- Employees understand that the Trust / School reserves the right to suspend internet access at any time,
- Use of the internet for personal use does not infringe on business functions.

4.3 **Inappropriate Use:** The Trust does not permit individuals to use the internet in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files,
- Images, cartoons, jokes or movie files containing ethnic, religious, or racial slurs,
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.
- Individuals are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

4.4 **Copyright:** The Trust does not permit individuals to download any content from the internet including photos, pictures or images and use them within the Trust without seeking advice about copyright infringement from the School Business Manager.

4.5 **Other Business Use:** Users are not permitted to use the internet to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of the Senior Leadership Team.

4.6 **Internet Security:** Users will take care to use the internet in accordance with SBMAT's Information Security policy. In particular users will not click on links on un-trusted or unverified Web Pages.

## 5. SOCIAL MEDIA USE

5.1 The Trust recognises and embraces the benefits and opportunities that social media can contribute to an organisation. The Trust also recognises that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

5.2 **Corporate Accounts:** Schools within SBMAT may have social media accounts operating on different platforms. Where schools have these accounts in place only nominated employees will have access to these accounts. Only these nominated employees will be permitted to post information about the School. Authorised employees will not disclose the usernames and passwords to these accounts to any other individual within or external to the organisation The School Business/Finance Manager will have overall responsibility for allowing access to social media accounts. Corporate Social Media Accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of SBMAT's Information Governance policies and data protection legislation.

Corporate Social Media Accounts must not be used in a way which could:

- Tarnish the reputation of SBMAT or any of its schools,
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.
- Be construed as sexually explicit,
- Construed as political beliefs or commentary.

5.3 **Personal Accounts:** The Trust understands that many employees will use or have access to Personal Social Media Accounts. Employees must not use these accounts:

- During working hours,
- Using corporate equipment,
- To conduct corporate business,
- To contact or approach students, customers, or partners of the Trust / School.

## 6. TELEPHONE AND VIDEO CONFERENCING USE

6.1 The Trust provides email accounts to employees to assist with performance of their duties. The Trust also allows employees to use video conferencing platforms for business use. For the benefit of doubt these platforms are classed as telephone calls in this policy.

6.2 **Personal Use:** Whilst the telephone should primarily be used for business functions, incidental and occasional use of the telephone in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of SBMAT or any of its schools,
- Employees understand that the Senior Leadership Team may have access to call history,
- Employees understand that the Trust reserves the right to suspend telephone usage at any time,
- Use of the telephone for personal use does not infringe on business functions.

**6.3** **Inappropriate Use:** The Trust does not permit individuals to use the telephone in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

6.4 **Other Business Use:** Users are not permitted to use the telephone to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of the Senior Leadership Team.

6.5 **Telephone / Mobile Phone Conduct:** Members of staff dealing with telephone enquiries should be careful about disclosing any personal data held by the Trust in particular they should:

  - Check the caller's identity to make sure that information is only given to a person who is entitled to it.
  - Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
  - Refer to their line manager or the DPO for assistance in difficult situations.
  - No-one should feel pressurised into disclosing personal information.
- Any telephone call where sensitive information is being discussed should take place in an appropriately private place, where personal information cannot be overheard.
- Mobile phones should not be used in front of pupils, unless on a school trip (in which case the circumstances should be explained to those present) or in relation to out of hours clubs / activities when communicating with parents.
- Mobiles can be used in the building outside of lessons (where a member of staff is not directly supervising pupils) with sensitivity towards other staff.
- Mobiles should not be switched on during professional meetings, unless exceptional circumstances have been discussed and agreed with the Senior Leader / Headteacher in advance.
- Mobile devices should not be used to take images or videos of pupils or staff, unless specifically authorised by the Headteacher, with the consent of all parties and with a school owned mobile device.
- Mobile devices should not be used to send inappropriate messages, images or recordings.