South Gloucestershire and Stroud Academy Trust (SGSAT)

IT Acceptable Use Policy – Electronic Communication

If you would like this document in an alternate format

Please contact the Human Resources Department

Prepared by:	Tim Hanks
Job Title/Role:	Group IT Director
Ref. No.: **Q/P 146**	**Date of this version:** 07/11/2022 **Review date:** 01/11/2024 (Subject to any legislative changes) **Upload to website?** **Upload to e-Campus?**
Approved by:	SGSAT Trust Board
Date:	23/11/2022

IT Acceptable Use Policy – Electronic Communication

1. Policy Intent

1.1. We live in a digital era that is everchanging and now has enumerable ways of communicating digitally. The intent of this policy is to outline the acceptable use of all forms of electronic communication within SGS Academy Trust (SGSAT), either through Office 365 or any other systems managed by SGSAT.

2. Scope

2.1. This Policy applies to **all** users of electronic communication systems provided within SGSAT.

2.2. Electronic communication systems include but are not limited to:

- Email
- All Microsoft Teams communications, including 'chat' and 'channel' messages
- Communication using SGSAT social media platforms
- Arbor

3. Procedures

3.1. Use of SGSAT systems for personal communication

3.1.1. Personal use of SGSAT communication systems is permitted providing the following points are adhered to and at no point are any other policies contravened.

3.1.2. Personal views must be stated as such.

3.1.3. Wherever possible all personal communications or files should be stored in a folder clearly labelled as personal.

3.1.4. The purpose of any personal use of college communication systems must not be for personal financial gain or that of another organisation.

3.2. Use of Attachments

3.2.1. Use of attachments in any SGSAT system should be considered before sending. Use of 'cloud-sharing' systems are often now much more efficient and effective and staff should use cloud-sharing options wherever possible.

3.2.2. When using email, the maximum size permitted, including attachments, is 32Mb.

3.2.3. Certain attachment types are blocked by the email system such as executable and JavaScript files. A full list is available from SGS IT Services.

3.3. Electronic Communication Security

3.3.1. Not all forms of electronic communication are secure and may be seen by others.

3.3.2. Confidentiality of any electronic communication cannot be assured and as such users should carefully consider the content of any communication prior to sending.

3.3.3. Users must not access or intercept any other users' electronic communications without proper grounds, authorisation and only in accordance with the law.

3.3.4. Any email, or other communication, such as Teams Chat, containing confidential information or information subject to GDPR should be protected accordingly. Attachments may be encrypted using 7Zip while an entire email maybe protected using the "Protect" facility within Office 365. **NOTE: The "Protect" functionality within Office 365 relies on the recipient being correct. If in any doubt the confidential information needs to be encrypted.**

3.4. Monitoring and Access to Electronic Communications

3.4.1. SGSAT may at any time permit the inspection, monitoring, or disclosure of any electronic communication content:

3.4.1.1. When required by and consistent in law.

3.4.1.2. SGSAT does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Freedom of Information Act, Data Protection Act, The Regulation of Investigatory Powers Act, and other laws concerning disclosure and privacy, or other applicable law.

3.4.2. SGSAT reserves the right to monitor electronic communication in order:

3.4.2.1. To comply with the Prevent Strategy, which aims to reduce the threat to the UK from terrorism, by preventing people from being drawn into terrorism, SGSAT carries out appropriate monitoring and filtering of SGSAT systems.

3.4.2.2. To carry out system management, problem resolution, maintenance and capacity planning, to correct addressing problems or for similar reasons related to performance or availability of any electronic system.

3.4.2.3. To address security issues, including virus management and authorised surveillance, including tracking unauthorised access to a system.

3.4.2.4. SGSAT may access, with written authorisation from SGSAT Group Executive, the content of any electronic communication using college systems and to meet time-dependent, critical business or operational needs or to carry out records management responsibilities, e.g.: to conduct business during a crisis if an employee is absent when information is required, or a prolonged absence of an employee when information in the User's electronic systems is required. The User will generally be informed at the earliest opportunity if this form of access is necessary.

3.5. **SPAM**

3.5.1. SPAM is defined as unsolicited bulk email communications including internal communications not authorised by the SGSAT Group Executive.

3.5.2. Users are strictly prohibited from the sending of SPAM internally and externally.

3.6. **Access using mobile clients and apps**

3.6.1. All mobile devices accessing any SGSAT digital system using any application or "app" other than a web browser MUST configure and install the "Company Portal" application from the relevant app store.

3.7. **Email retention**

3.7.1. Default email retention should set to 365 days with the option to create folders with longer retention periods if required in line with the organisations Data Privacy & Protection Policy.

3.7.2. "Junk Mail" and "Deleted Items" will have a 30-day retention prior to permanent deletion.

4. Policy <u>Implementation</u>

4.1. All users of electronic communication facilities provided by SGSAT.

5. Enforcement

5.1. Failure to adhere to the requirements, advice or guidance outlined in this document may result in disciplinary action in accordance with the SGSAT's disciplinary policy and procedure.

6. Related Policies, Procedures, Charters, Plans, Guidance and Legislation

6.1. Related SGSAT policies, procedures and guidance can be found on SharePoint and include:

- IT Security Policy
- IT Acceptable Use Policy – Users
- IT Acceptable Use Policy – Mobile Devices
- Freedom of Information Act
- Data Protection Act 2018
- The Regulation of Investigatory Powers Act
- Data Privacy & Protection Policy
- Other laws concerning disclosure and privacy, or other applicable law

7. Impact

7.1. The impact of this policy is to ensure all users of electronic communication systems within SGSAT adhere to this policy and are aware of key requirements for using these systems. This in turn ensures the overall integrity of systems and ensures the ongoing positive reputation of SGSAT.

8. Additional useful information

8.1. The Group IT Director will review and monitor the policy and procedures and will recommend and implement approved changes where necessary.

9. MANDATORY INITIAL IMPACT SCREENING

Completed by:		
Tim Hanks	Group IT Director	07/11/2022

I have read the guidance document: Completing a Policy Impact Assessment?	✓
If this policy has been up-dated, please tick to confirm that the initial impact screening has also been reviewed:	✓

EQUALITY AND DIVERSITY IMPACT ASSESSMENT				
Characteristic	This policy seeks to:			
Age	Choose an item.			
Disability	Choose an item.			
Faith or Belief	Choose an item.			
Gender	Choose an item.			
Race or Ethnicity	Choose an item.			
Orientation	Choose an item.			
Gender reassignment	Choose an item.			
Economic disadvantage	Choose an item.			
Rural isolation	Choose an item.			
Marriage	Choose an item.			
Pregnancy & maternity	Choose an item.			
Carers & care leavers	Choose an item.			
Vulnerable persons	Choose an item.			
Please identify any sections of the policy that specifically seek to maximise opportunities to improve diversity within any of the Trust's stakeholder groups:		NA		
Please identify any sections of the policy that specifically seek to improve equality of opportunity within any of the Trust's stakeholder groups:		NA		
Is there any possibility that this policy could operate in a discriminatory way?	☐	×	If you have ticked yes (red), which characteristic will be most affected? Choose an item.	
If yes please confirm that the Policy has been sent for a full Equality & Diversity Impact Assessment, and note the date:	☐	Click or tap to enter a date.		

Note: if the policy does not seek to increase diversity or improve equality you should go back and review it before submitting it for approval.

MAPPING OF FUNDAMENTAL RIGHTS	
Which United Nations Convention on the Rights of the Child (UNCRC), Right does this policy most protect:	Art. 12 Respect for personal views Atr. 16 Right to privacy Choose an item.
Which Human Right (HRA) does this policy most protect:	Art. 8 Right to private & family life Art. 7 No punishment without law

DATA PROTECTION & PRIVACY BY DESIGN SCREENING	
Tick to confirm that you have considered any data protection issues as part of the design and implementation of this policy; and, that implementing this policy will not result in the collection, storage or processing of personal data outside of official Trust systems:	✓
Tick to indicated that this policy has or requires a Data Privacy Impact Assessment:	☐