South Gloucestershire and Stroud Academy Trust (SGSAT)

IT Acceptable Use Policy – Mobile Devices

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 147**	**Date of this version:** 07/11/2022 **Review date:** 01/11/2024 (Subject to any legislative changes) **Upload to website?** No **Upload to e-Campus?** No
Approved by:	SGSAT Trust Board
Date:	23/11/2022

IT Acceptable Use Policy – Mobile Devices

1. Policy Intent

1.1. The Digital Era that we now live in means that staff are now using mobile devices to work from home and/or access systems provided by SGS Academy Trust (SGSAT). It is important that SGSAT staff have a good understanding of the complexities and requirements resulting from these working practices. The intent of this policy is to outline the acceptable use of all types of mobile devices that are used in relation to SGSAT business.

2. Scope

2.1. This policy applies to all mobile devices used in conjunction with the business of SGSAT and includes devices such as iPads, Tablets, Laptops, Smartphones and similar 3G and 4G devices, Portable Hard Drives, USB Keys and PDA's are all subject to the "IT Acceptable Use Policy – Users" and present their own unique requirements, but are all covered by this policy.

3. Procedures

3.1. Physical Security

3.1.1. Physical security of any SGSAT mobile device is the responsibility of the staff member it is assigned to. As such, mobile devices should be stored securely at all times, whether at work, in transport or at home.

3.1.2. Mobile devices should not be left in vehicles. If there is no alternative for short periods of time they must be stored out of site in a locked compartment.

3.1.3. In any circumstance, mobile devices must not be left in vehicles overnight.

3.2. Data Security

3.2.1. Microsoft's BitLocker cryptography solution has been adopted for use on all Windows based staff devices providing encryption of all portable media (such as USB keys).

3.2.2. Write access will be denied on all Microsoft Windows based staff machines to all portable media NOT encrypted via BitLocker.

3.2.3. All Microsoft Windows tablets and laptops designated specifically as "Staff Only" will be fully encrypted.

3.2.4. Mobile devices used for SGSAT business MUST be password protected.

3.2.5. Where possible they must use encryption.

3.2.6. Devices must use a fully supported and up-to-date operating system.

3.2.7. All devices in this category capable of sending, receiving and storing ANY business-related data MUST install the “Company Portal” Mobile Device Management (MDM) client from the relevant app store for the device.

3.2.8. Any device not capable of encryption or password protection must not be used to store any data subject to the Data Protection Act 2018 or of a commercial nature.

4. Policy Implementation

4.1. All users of mobile devices used in conjunction with the business of 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:

6.1.1. IT Security Policy
6.1.2. IT Acceptable Use Policy – Users
6.1.3. IT Acceptable Use Policy – Electronic Communication
6.1.4. Data Protection Act 2018

7. Impact

7.1. The impact of this policy is to ensure all business users of mobile devices within SGSAT adhere to this policy and are aware of key requirements for using these devices. 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:	Choose an item. Choose an item. Choose an item.
Which Human Right (HRA) does this policy most protect:	Art. 8 Right to private & family life Choose an item.

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:	☐