

541: St. George Academy Technology Security Policy

1. Purpose:

1.1 The purpose of this policy is to ensure the secure use and handling of all data, computer systems and computer equipment by St. George Academy students, patrons, and employees.

2. Policy:

2.1. It is the policy of the St. George Academy to support secure network systems, including security for all personally identifiable information that is stored on paper or stored digitally on school-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the school, its students, or its employees.

2.2 The school will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.

2.3 All persons who are granted access to network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of devices and the network.

2.4 When an employee or other user becomes aware of suspicious activity, they are to immediately contact the school's Information Security Officer with the relevant information.

2.5 This policy and procedure also covers third party vendors/contractors that contain or have access to St. George Academy critically sensitive data. All third-party entities will be required to sign the SGA Employee Non-Disclosure Agreement before accessing our systems or receiving information.

2.6. It is the policy of St. George Academy to fully conform with all federal and state privacy and data governance laws, including the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.

2.7. Professional development for staff and students regarding the importance of network security and best practices will be conducted each year.

2.8. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network and the Utah State Office of Education.

2.9. St. George Academy supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect St. George Academy's data, users, and electronic assets.

3. Definitions:

3.1. "Access" means direct or indirect use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

3.2 "Authorization" means having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

3.3. "Computer" means any electronic device or communication facility that stores, retrieves, processes, or transmits data.

3.4. "Computer system" means a set of related, connected or unconnected, devices, software, or other related computer equipment.

3.5. "Computer network" means the interconnection of communication or telecommunication lines between computers; or computers and remote terminals; or the interconnection by wireless technology between computers; or computers and remote terminals.

3.6. "Confidential data" means data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it is not available to others without the owner's or custodian's permission.

3.7. "Encryption or encrypted data" means the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

3.8. "Personally Identifiable Information (PII)" means any data that could potentially identify a specific individual.

3.7. "Security system" means a computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

4. Procedures:

4.1. St. George Academy shall appoint an IT Security Officer (ISO) responsible for overseeing school wide IT security, to include development of policies and adherence to the standards

**Policy Adapted from Washington County
Board Approved 2/9/23*

defined in this document subject to approval by the Executive Director and the St. George Academy Governing Board.

4.2. St. George Academy, led by the ISO, shall ensure that all employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information. Training resources will be provided to all employees.

4.3. St. George Academy, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.

4.4. St. George Academy shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. Automatic log off, locks and password screen savers should be used to enforce this requirement.

4.5. St. George Academy shall ensure that all equipment that contains sensitive information will be secured to deter theft.

4.6. Telecommunication rooms/closets must remain locked when not in use by a school employee or technician.

4.7. Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor will need to present a company issued identification card, and his/her access will need to be confirmed directly by the authorized employee who issued the service request or by St. George Academy's Technology Department.

4.8. At present there are no servers on the premises. SGA houses data via Google Cloud and USBE services.

4.9. Network perimeter controls will be implemented to regulate traffic moving between trusted internal resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

4.10. St. George Academy shall ensure that all student access computer networks are separated from employee computer networks and utilize security policies to ensure the integrity of those computer networks.

4.11. St. George Academy will utilize industry standards and current best practices to segment internal computer networks based on the data they contain.

4.12. No wireless access point shall be installed on St. George Academy's computer network that does not conform with current network standards.

4.13. St. George Academy shall scan for and remove or disable any rogue wireless devices on a regular basis.

****Policy Adapted from Washington County
Board Approved 2/9/23***

4.14. All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections.

4.15. St. George Academy shall ensure that any remote access with connectivity to the school's internal network is achieved using a centralized VPN service that is protected by multiple factor authentication systems.

4.15.1. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the Information Security Officer.

5. Access Control

5.1. System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

5.2. St. George Academy shall encourage strong password management for employees, students, and contractors.

5.3. All server system-level passwords must conform to best practices password construction guidelines.

5.4. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.

5.5. St. George Academy shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs.

5.6. St. George Academy shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.

5.7. St. George Academy shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.

5.8. St. George Academy shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

5.9 Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

6. Continuity

6.1 To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of school IT operations.

**Policy Adapted from Washington County
Board Approved 2/9/23*

6.2 The continuity plan should include procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities.

7. Malicious Software

7.1 Workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

7.2 St. George Academy shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e., chromebooks, workstations, and laptops.

7.3 St. George Academy shall ensure that malicious software protection will include frequent update downloads, frequent scanning, and that malicious software protection is in active state (real time) on all operating servers/workstations.

7.4 St. George Academy shall ensure that all security-relevant software patches are applied within thirty days and critical patches shall be applied as soon as possible.

7.5 All computers must use the school approved anti-virus solution.

7.6. Any exceptions must be approved by the Information Security Officer.

8. Internet Content Filtering

8.1. In accordance with Federal and State Law, St. George Academy shall filter internet traffic for content defined in law that is deemed harmful to minors.

8.2. St. George Academy acknowledges that technology-based filters are not always effective at eliminating harmful content and due to this, St. George Academy uses a combination of technological means and supervisory means to protect students from harmful online content.

8.3. In the event that students take devices home, St. George Academy will provide a technology-based filtering solution for those devices. However, the school will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content.

8.4. Students shall be supervised when accessing the internet and using school owned devices on school property.

9. Data Privacy

9.1. St. George Academy considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

**Policy Adapted from Washington County
Board Approved 2/9/23*

9.2. St. George Academy protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (“FERPA”), the Government Records and Management Act U.C.A. §62G-2 (“GRAMA”), U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 (“COPPA”) and Utah Administrative Code R277-487 (“Student Data Protection Act”).

9.3. St. George Academy shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs.

9.4 All data privacy and security measures will adhere to SGA policy 552: SGA Data Governance Policy.

10. Security Audit and Remediation

10.1. St. George Academy shall perform routine security and privacy audits.

10.2. School personnel shall develop remediation plans to address identified lapses.

10.3. Employee disciplinary actions shall be in accordance with applicable laws, regulations and SGA policies. Any employee found to be in violation of this policy may be subject to disciplinary action up to and including termination of employment with St. George Academy.