ST. THOMAS AQUINAS CATHOLIC SCHOOLS

STAFF RESPONSIBLE USE AGREEMENT

All staff granted access to STAR Catholic Information Resources must follow the responsible use rules below:

General

- Division information resources are provided for the express purpose of conducting the business and mission of the Division. Resources are not to be used for improper purposes and all laws and existing Division policies apply to conduct while using Division information resources. Improper use or behaviour includes, but is not limited to, the following:
  - creating, displaying, viewing, storing, disseminating or otherwise handling obscene, hateful, pornographic or otherwise illegal materials
  - using the information resources to perpetrate any form of fraud or software, film or music piracy
  - using the information resources to harass others
  - publishing defamatory or knowingly false information about the Division, Division employees or others on any social media or online publishing site
  - circumventing Division security measures
  - undertaking activities which degrade or affect the availability or accessibility of Division information resources
  - deliberately introducing malicious software or code into Division information resources
  - engaging in any illegal activity using Division information resources
- Incidental personal use of electronic mail and internet access is permitted by the Division but it must not interfere with normal performance of duties, must not result in direct costs to the Division, and must not expose the Division to risks.
- If it is anticipated that questionable materials may be accessed in the course of instruction, written, advance approval of a principal or direct supervisor is required.
- Information resources must not be used to conduct any business which is for the exclusive benefit of individuals or for organizations that are not part of the Division.
- All messages, files and documents stored on Division information resources, including personal messages, files and documents, are the property of the Division and are subject to Division review at any time. Employees should have no expectation of privacy with respect to messages, files and documents stored on Division information resources.

Data storage and encryption

- All Confidential Information transmitted over external networks shall be encrypted. **"Confidential information"** means information learned or obtained in the course of employment with the Division that is not a matter of common knowledge, or not readily available to those outside the Division or the unauthorized use or disclosure of which could cause serious damage to the Division, or an individual. It may include, but is not limited to, personal information regarding students, parents or staff.
- Confidential information shall not be sent or forwarded through non-Division email accounts provided by other Internet Service Providers, and shall not be knowingly transmitted via wireless networks to or from a portable computing device unless approved wireless transmission protocols and security techniques are utilized.

Data Protection

- All electronic data utilized or developed to support Division operations shall be saved on Division network servers to ensure backup of the data.
- Any files stored with external storage providers such as Google shall be backed up by the user. Backup or restoration of such data is not the responsibility of the Division.
- Any data stored on servers outside the Division such as Google shall not be considered confidential as it could be accessed by others according to the laws of the host country (where the files are stored).
- Intentionally accessing data or programs contained on systems without appropriate authorization is prohibited.

Virus Protection

- All computing devices, including personally owned devices connecting to the Division network, must run current virus protection software acceptable to the Division. Devices found without acceptable virus protection software or infected with a virus or other malicious code will be disconnected from the Division network until deemed safe by the Technology Department.
- Under no circumstances shall virus protection software be in any way intentionally circumvented or disabled.

Email

- The following email activities are prohibited:
  - Reading another user's email unless authorized to do so by the owner of the email account, or as authorized by the Division for investigation purposes;
  - Posing as anyone other than oneself when sending email;
  - Using email for purposes of political lobbying or campaigning;
  - Sending unsolicited messages to large groups except as required when conducting Division business;
  - Sending excessively large messages or attachments unless in performance of official Division business;
  - Sending or forwarding email that is likely to contain computer viruses;

Storage of Personal data

- Non-Division related information should not be stored on Division network file servers. The Division assumes no responsibility to backup or restore personal data.
- Any files, messages or documents residing on Division computers may be subject to public information requests and may be accessed by the Division. Division email accounts should not be used for personal email correspondence that is confidential in nature.

Division Mobile Device Security	♦ All Division owned mobile devices must be protected against unauthorized access. Reasonable efforts must be made to use passwords, encryption and physical security means wherever reasonable and in accordance with Division policy. ♦ In the event that a Division mobile device is lost, stolen or otherwise misplaced, the Division must be notified as soon as reasonable in order that the Division may take action to protect the content of those devices.
Internet Use	♦ User activity may be subject to logging and review. ♦ Statements or opinions made online shall not imply that such statements or opinions are those of the Division, unless so authorized in writing by the Division. A disclaimer shall be used at all times that states that the statements or opinions expressed are personal and do not represent those of the Division.
Personally Owned Devices	♦ Individuals wishing to use personally owned devices for the purposes of Division business, or wishing to connect personally owned devices to Division networks or servers must agree to the conditions in this Agreement. By using a personally owned device for the purposes of Division business or by connecting a personally owned device to the Division network or server, the user is deemed to have agreed to the conditions in this Agreement. ♦ All personally owned devices accessing Division networks or servers shall be password protected ♦ All personally owned devices shall encrypt all confidential information to ensure that the integrity of the data is not compromised in the event that the device is lost, stolen or otherwise misplaced. ♦ The Division is not responsible for the loss, theft or damage of a personally owned device. ♦ It is a condition of this Agreement that all users of personally owned devices which are used for the purposes of Division business or are connected to Division networks or servers agree that their personally owned device(s) may be subject to access by Division personnel when reasonable grounds exist to believe that there has been a breach of this Agreement, any other Division policy, regulation or rule or any applicable law. ♦ Personally owned devices shall at no time be connected to any Division wired network, and shall only connect to Division wireless networks designated from time to time as appropriate for personally owned devices. ♦ Any device that has been routed or jailbroken will be restricted from access to Division information resources.
Passwords	♦ Every account password, any personal identification numbers (PIN), security token or any other similar information or device used for identification and authorization purposes must not be shared and shall be unique to the individual user. Each user is responsible for all activities conducted using his or her account(s). ♦ Users shall not circumvent password entry through use of auto logon, application “remember password” features, embedded scripts or hard-coded passwords in client software.
Security	♦ Security programs or utilities that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems shall not be downloaded and/or used. The use of password cracking programs, packet sniffers, or port scanners on Division networks is not permitted. ♦ Users must report any identified weaknesses in Division security and any incidents of possible misuse or violation of this agreement to a manager or principal. ♦ Where technically feasible, all laptops or other personal digital devices should be secured with a password-protected screensaver for personal protection.

User Acknowledgment

I acknowledge that I have received and read this Agreement and agree with the terms contained herein. I understand that I must comply with the Agreement when accessing and using Division information resources and my failure to comply with the Agreement may result in appropriate disciplinary action, up to and including termination of employment.

Signature: ______________________________ Date: ______________________________

Print Name: ______________________________